# International CIIP Handbook 2008/2009

## An Inventory of 25 National and 7 International Critical Information Infrastructure Protection Policies

**Edited Volume**

**Author(s):**
Brunner, Elgin M.; Suter, Manuel

**Publication date:**
2008

**Permanent link:**
https://doi.org/10.3929/ethz-b-000009792

**Originally published in:**
International CIIP Handbook

*Elgin M. Brunner and Manuel Suter*

# INTERNATIONAL
# **CIIP HANDBOOK** 2008 / 2009

## AN INVENTORY OF 25 NATIONAL AND 7 INTERNATIONAL CRITICAL INFORMATION INFRASTRUCTURE PROTECTION POLICIES

***Series Editors***
*Andreas Wenger, Victor Mauer and Myriam Dunn Cavelty*

*Center for Security Studies, ETH Zurich*

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

CSS
ETH Zurich

*Elgin M. Brunner and Manuel Suter*

# INTERNATIONAL
# **CIIP HANDBOOK** 2008 / 2009

AN INVENTORY OF 25 NATIONAL AND 7 INTERNATIONAL
CRITICAL INFORMATION INFRASTRUCTURE PROTECTION POLICIES

***Series Editors***
*Andreas Wenger, Victor Mauer and Myriam Dunn Cavelty*

*Center for Security Studies, ETH Zurich*

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

# Contents

# Preface

The nature of risks and vulnerabilities in modern societies is becoming more and more transnational today. An open, non-hierarchical dialog on newly recognized vulnerabilities at the physical, virtual, and psychological levels is needed to create new knowledge and a better understanding of new risks and of their causes, interactions, probabilities, and costs.

It was on the basis of these premises that the "Crisis and Risk Network" (CRN; www.crn.ethz.ch) was launched in the year 2000 as a joint Swiss-Swedish initiative. CRN is an initiative for international dialog on security risks and vulnerabilities, risk analysis and management, emergency preparedness, and crisis management. Through the interchange of views, the CRN helps to promote a better understanding of the complex challenges and opportunities confronting the risk community today and serves to establish a collaborative relationship and exchange among experts.

The International Critical Information Infrastructure Protection (CIIP) Handbook is the product of a joint effort within the CRN partner network. The first edition of the CIIP Handbook, published in 2002, provided an inventory of national protection policies in eight countries: Australia, Canada, Germany, the Netherlands, Norway, Sweden, Switzerland, and the United States. The 2002 Handbook proved to be such a success that it had to be reprinted soon after first publication. The 2004 edition offered updates on the existing country surveys, six new country studies (Austria, Finland, France, Great Britain, Italy, and New Zealand), overview chapters on international protection efforts, legal issues, and current trends in research and development, as well as a more profound methodological section and more in-depth analysis in general. The expert base and the number of staff working on the Handbook were both expanded. The 2006 edition continued the tradition of the past two editions and went beyond it at the same time: it not only further expanded the country survey section by including India, Japan, Korea, Malaysia, Singapore, and Russia, but it was also accompanied by a second volume with in-depth analysis of key issues related to

CIIP. The 2008 edition includes another five countries: Brazil, Estonia, Hungary, Poland and Spain.

The editors would like to thank Elgin Brunner and Manuel Suter, researchers at the Center for Security Studies (CSS) at ETH Zurich for their efforts and their high-quality contribution to this important topic. Additionally, the editors would like to thank all the partners involved, in particular the national experts who generously shared their experience and knowledge with us. We also thank the following for their help in the completion of this project: Christopher Findlay, Frank Haydon, Carolin Hilpert, and Fraser McArthur.

Zurich, July 2008

Prof. Dr. Andreas Wenger
Director
Center for Security Studies,
ETH Zurich

Dr. Victor Mauer
Deputy Director
Center for Security Studies,
ETH Zurich

Dr. Myriam Dunn Cavelty
CRN Coordinator
Center for Security Studies,
ETH Zurich

# Abbreviations

| | |
|---|---|
| ACIS: | Advisory Committee for Information Security (Finland) |
| ACMA: | Australian Communications and Media Authority (Australia) |
| ACSI 33: | Australian Communications-Electronic Security Instruction 33 (Australia) |
| ADAE: | Agency for the Development of Electronic Administration (France) |
| AETIC: | Spanish electronics, information technology and telecommunications industries association (Spain) |
| AFP: | Australian Federal Police (Australia) |
| AG KRITIS: | Interministerielle Arbeitsgruppe Kritische Infrastrukturen (Germany) |
| AGD: | Attorney General's Department (Australia) |
| AGIMO: | Australian Government Information Management Office (Australia) |
| AgIO: | Cabinet Office Workgroup on Information Operations (Sweden) |
| AHG: | Ad Hoc Group (NATO) |
| AHTCC: | Australian High Tech Crime Centre (Australia) |
| AIPA: | Authority for IT in the Public Administration (Italy) |
| AIIC: | Association of Italian Experts for Critical Infrastructures / Associazione Italiana Esperti in Infrastrutture Critiche (Italy) |
| AIVD: | Algemene Inlichtingen- en Veiligheidsdienst / General Intelligence and Security Service (The Netherlands) |
| AKSIS: | Arbeitskreis Schutz Kritischer Infrastrukturen / Working Group on Infrastructure Protection (Germany) |
| AMSD: | Accompanying Measure System Dependability (EU) |
| Anatel: | Agência Nacional de Telecomunicações / Federal telecommunications regulatory body (Brazil) |
| APCERT: | Asia Pacific Computer Emergency Response Team |
| AP-CIRT: | Asia Pacific Security Incident Response Coordination |
| APEC: | Asia-Pacific Economic Cooperation |
| APSIRC-WG: | Asia Pacific Security Incident Response Coordination Working Group (Singapore) |
| APWG: | Anti-Phishing Working Group |
| AS / NZS: | Australian and New Zealand Standard for Risk Management (Australia / New Zealand) |
| ASIO: | Australian Security Intelligence Organisation (Australia) |

| | |
|---|---|
| A-SIT: | Center for Secure Information Technology Austria (Austria) |
| ATIA: | Access to Information Act (Canada) |
| AusCERT: | Australian Computer Emergency Response Team (Australia/New Zealand) |
| BAKOM: | Bundesamt für Kommunikation/Federal Office for Communication (Switzerland) |
| BAS: | Protection of Society (Norway) |
| BBK: | Bundesamt für Bevölkerungsschutz und Katastrophenhilfe/Federal Office of Civil Protection and Disaster Response (Germany) |
| BCS: | British Computer Society (United Kingdom) |
| BERR: | Business, Enterprise and Regulatory Reform (United Kingdom) |
| BfV: | Bundesamt für Verfassungsschutz/Federal Office for the Protection of the Constitution (Germany) |
| BIS: | Bureau of Indian Standards (India) |
| BIT: | Bundesamt für Informatik und Telekommunikation/Federal Office of Information Technology, Systems, and Telecommunication (Switzerland) |
| BITKOM: | Bundesverband für Informationswirtschaft, Telekommunikation und Neue Medien (Germany) |
| BITS: | Banking Industry Technology Secretariat (Korea) |
| BKA: | Bundeskriminalamt/Federal Office of Criminal Investigation (Germany) |
| BMBF: | Bundesministerium für Bildung und Forschung/Federal Ministry for Education and Research (Germany) |
| BMI: | Bundesministerium des Inneren/Federal Ministry of the Interior (Austria; Germany) |
| BMJ: | Bundesministerium der Justiz/Federal Ministry of Justice (Germany) |
| BMVg: | Bundesministerium der Verteidigung/Federal Ministry of Defense (Germany) |
| BMVIT: | Ministry for Traffic, Infrastructure and Technology (Austria) |
| BMWA: | Bundesministerium für Wirtschaft und Arbeit/Federal Ministry of Economics and Labour (Germany) |
| BMWi: | Bundesministerium für Wirtschaft and Technologie/Federal Ministry of Economics and Technology (Germany) |
| BND: | Bundesnachrichtendienst/Federal Intelligence Service (Germany) |
| BPOL: | Federal Police (Germany) |
| BSI: | Bundesamt für Sicherheit in der Informationstechnik/Federal Office for Information Security (Germany) |
| BVA: | Bundesverwaltungsamt/Federal Office of Administration (Germany) |

| | |
|---|---|
| BVT: | Federal Agency for State Protection and Counter-Terrorism (Austria) |
| BZK: | Ministry of the Interior and Kingdom Relations (The Netherlands) |
| CAIS: | Centro de Atendimento a Incidentes de Segurança/Security Incidents Attendance Center (Brazil) |
| CanCERT: | Canadian Computer Emergency Response Team (Canada) |
| CAPC: | Civil Aviation Planning Committee (NATO) |
| CART: | Computer Analysis and Response Team (United States) |
| CAS: | Complex Adaptive Systems |
| CATA: | Antivirus Early Warning Center/Centro De Alerta Temprana Antivirus (Spain) |
| CATS: | Center for Asymmetric Threat Studies (Sweden) |
| CBA: | Canadian Bankers Association (Canada) |
| CCA: | Controller of Certifying Authorities (India) |
| CCIP: | Centre for Critical Infrastructure Protection (New Zealand) |
| CCIPS: | Computer Crime and Intellectual Property Section (United States) |
| CCIRC: | Canadian Cyber Incident Response Centre (Canada) |
| CCPC: | Civil Communication Planning Committee (NATO) |
| CCS: | Civil Contingencies Secretariat (United Kingdom) |
| CEA: | Canadian Electricity Association (Canada) |
| CEN: | European Committee for Standardization |
| CenPRA: | Centro de Pesquisas Renato Archer (Brazil) |
| CENTR: | Council of European Top Level Domain Registries |
| CEP: | Civil Emergency Planning (NATO) |
| CEP: | Corporate Executive Programme (FIRST) |
| CEPTOAR: | Capabilities for Engineering of Protection, Technical Operations, Analyses, and Response (Japan) |
| CERT: | Computer Emergency Response Team |
| CERTA: | Computer Emergency Response Team (France) |
| CERT.at: | Computer Emergency Response Team Austria (Austria) |
| CERT-Bund: | German Computer Emergency Response Team for Federal Authorities (Germany) |
| CERT.br: | Computer Emergency Response Team Brazil (Brazil) |
| CERT/CC: | Computer Emergency Response Team Coordination Center |
| CERT-CNN: | Computer Emergency Response Team of the National Cryptology Center/Equipo de Respuesta ante Incidentes de Seguridad Informática de Centro Criptológico Nacional de España (Spain) |
| CERT-Difesa: | Computer Emergency Response Team of the Ministry of Defense (Italy) |

| | |
|---|---|
| CERT-FI: | Computer Emergency Response Team Finland (Finland) |
| CERT GOV PL: | Polish Government's Computer Incident Response Team (Poland) |
| CERT-Hungary: | Computer Emergency Response Team Hungary (Hungary) |
| CERT-In: | Computer Emergency Response Team India (India) |
| CERT-IST: | Computer Emergency Response Team Industry, Services, and Trade (France) |
| CERT-IT: | Italian Computer Emergency Response Team (Italy) |
| CERT-NL: | Computer Emergency Response Team of the Netherlands (The Netherlands) |
| CERT-PA: | Computer Emergency Response Team for the Public Central Administration (Italy) |
| CERT Polska: | Polish Computer Emergency and Response Team (Poland) |
| CERT-RENATER: | Computer Emergency Response Team (France) |
| CERT-RO: | Computer Ermengency Response Team for Government Departments (The Netherlands) |
| CESG: | Communications-Electronics Security Group (United Kingdom) |
| CESS: | Central Electronic Service System (Hungary) |
| CESSSI: | Centre for Training and Advanced Studies on Information Systems Security (France) |
| CESTI: | Information Technology Security Evaluation Center (France) |
| CETIC.br: | Centro de Estudo sobre as Tecnologias da Informação e da Comunicação/Center of Studies on Information and Communication Technologies (Brazil) |
| CFAA: | Computer Fraud and Abuse Act (United States) |
| CFSSI: | Information Systems Security Training Center (France) |
| CGI: | Brazilian Internet Steering Committee/Comitê Gestor da Internet no Brasil (Brazil) |
| CGSI: | Federal Government's Security Committee/Comitê Gestor de Segurança da Informação (Brazil) |
| CHO: | Chief Headquarter of Defense (Norway) |
| CI: | Critical Infrastructure |
| CI2RCO: | Critical Information Infrastructure Research Coordination (EU) |
| CIAC: | Critical Infrastructure Advisory Council (Australia) |
| CIAO: | Critical Infrastructure Assurance Office (United States) |
| CIDDAC: | Cyber Incident Detection Analysis Centre (United States) |
| CIF: | Consultative Industry Forum (Australia) |
| CII: | Confederation of Indian Industry (India) |
| CI: | Critical Infrastructure |
| CID: | Criminal Investigation Department of the Police Force (Singapore) |

| | |
|---|---|
| CII: | Critical Information Infrastructure |
| CIIP: | Critical Information Infrastructure Protection |
| CII-SA: | Critical Infocomm Infrastructure Surety Assessment (Singapore) |
| CIO: | Chief Information Officer |
| CIOS: | National Center for IO/CIP Studies (Sweden) |
| CIP: | Critical Infrastructure Protection |
| CIPG: | Critical Infrastructure Protection Group (Australia) |
| CIPTF: | Critical Infrastructure Protection Task Force (Canada) |
| CIRCA: | Computer Incident Response Coordination Austria (Austria) |
| CIRT: | Computer Incident Response Team |
| CIS: | Center for International Studies (Switzerland) |
| CISI: | Inter-Ministerial Committee for Information Society (France) |
| CISSI: | Commission Interministérielle pour la Sécurité des Systèmes d'Information/Inter-Ministerial Commission for the Security of Information Systems (Fance) |
| CISU: | Critical Infrastructure Studies Unit (Sweden) |
| CIWG: | Critical Infrastructure Working Group (United States) |
| CIWIN: | Critical Infrastructure Warning Information Network (EU) |
| CLUSIF: | Club de la Sécurité des Systèmes d'Information Français (France) |
| CLUSIS | Club de la Sécurité des Systèmes d'Information Suisse (Switzerland) |
| CMA | Communications and Multimedia Act (Malaysia) |
| CMA: | Computer Misure Act (Singapore) |
| CMT: | Federal Crisis Management Training (Switzerland) |
| CNAIPIC: | National Center for Anticriminal Information for Infrastructure Protection/Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (Italy) |
| CNES: | French Space Agency (France) |
| CNI: | Critical National Infrastructure |
| CNIPA: | National Center for Informatics in the Public Administration (Italy) |
| CNPIC: | National Centre for the Protection of the Critical Infrastructures/Centro Nacional de Protección de Infraestructuras Críticas (Spain) |
| COBIT: | Control Objectives for Information Technology (United States) |
| COBR: | Cabinet Office Briefing Room (United Kingdom) |
| COMSEC: | Communications Security (Finland) |
| COSSI: | Information System Security Operation Center (France) |
| CPC: | Civil Protection Committee (NATO) |
| CRC: | Communications Research Centre (Canada) |

| | |
|---|---|
| CPNI: | Centre for the Protection of the National Infrastructure (United Kingdom) |
| CRIEPI: | Central Research Institute of the Electric Power Industry (Japan) |
| CRN: | Comprehensive Risk Analysis and Management Network (Switzerland) |
| CRS: | Congressional Research Service (United States) |
| CS & C : | Office of Cybersecurity and Communications (United States) |
| CSCs: | Common Services Centres (India) |
| CSCSWG : | Cross Sector Cyber Security Working Group (United States) |
| CSD: | Computer Security Division at NIST (United States) |
| CSE: | Communications Security Establishment (Canada) |
| CSEC: | Swedish Certification Body for IT Security (Sweden) |
| CSIA: | Central Sponsor for Information Assurance (United Kingdom) |
| CSIAAG: | Communications Sector Infrastructure Assurance Advisory Group (Australia) |
| CSIRT: | Computer Security Incident Response Team |
| CSIRTUK: | Combined Security Incident Response Team (United Kingdom) |
| CSIS: | Canadian Security Intelligence Service (Canada) |
| CSS: | Center for Security Studies, ETH Zurich (Switzerland) |
| CSTARC: | Cyber Security Tracking, Analysis and Response Center (United States) |
| CSTD: | Commission on Science and Technology for Development (WSIS) |
| CSTI: | Strategic Advisory Board on Information Technologies (France) |
| CTIR: | Computer Security and Incident Response Team / Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal (Brazil) |
| CSTO: | Collective Security Treaty Organization |
| CT: | Counter-terrorism |
| CTEPA: | Canadian Telecommunications Emergency Preparedness Association (Canada) |
| CTI: | Commission for Technology and Innovation (Switzerland) |
| CTOSE: | Cyber Tools On-Line Search for Evidence (EU) |
| CTSA: | Counter Terrorism Security Adviser (CTSA) |
| CYCO: | Swiss Coordination Unit for Cybercrime Control (Switzerland) |
| CYTEX: | Cyber Terror Exercise (Germany) |
| DBCDE | Department of Broadband, Communications and the Digital Economy (Australia) |
| DCITA: | Department of Communications, Information Technology & the Arts (Australia) |
| DCSSI: | Directorate for Security of Information Systems (France) |

| | |
|---|---|
| DdoS: | Distributed Denial of Service |
| DDPS: | Swiss Federal Department of Defense, Civil Protection, and Sports (Switzerland) |
| DDSI: | Dependability Development Support Initiative (EU) |
| deNIS: | German Emergency Preparedness Information System (Germany) |
| DESG: | Domestic and External Security Group (New Zealand) |
| DESS: | Domestic and External Security Secretariat (New Zealand) |
| DFS: | Swedish Information Processing Society (Sweden) |
| DGDSI: | General Directorate for the Development of the Information Society/Dirección General para el Desarrollo de la Sociedad de la Información (Spain) |
| DG INFSO: | Information and Media Directorate-General (EU) |
| DGTP: | Telecom and Post Directorate (The Netherlands) |
| DGTTI: | General Directorate of Telecommunications and Information Technologies/Dirección General de Telecomunicaciones y Tecnología de la Información (Spain) |
| DHS: | Department of Homeland Security (United States) |
| DIA: | Defense Intelligence Agency (United States) |
| DIB: | Defense Industrial Base (United States) |
| DICO: | Dipartimento di Informatica e Comunicazione/Department of Informatics and Communications (Italy) |
| DIT: | Department for Innovation and Technologies (Italy) |
| DIT: | Department of Information Technology (India) |
| DoD: | Department of Defense (United States) |
| DoE: | Department of Energy (United States) |
| DoS: | Denial of Service |
| DPSEPA: | Department of Public Safety and Emergency Preparedness Act (Canada) |
| DSB: | Directorate for Civil Protection and Emergency Planning (Norway) |
| DSD: | Defence Signals Directorate (Australia) |
| DSG: | Datenschutzgesetz/Data Security Law (Austria) |
| DsiN: | Deutschland sicher im Netz/Germany Secure in the Web (Germany) |
| DSK: | Datenschutzkommission/Commission on Data Protection (Austria) |
| DSO: | Departmental Security Officer (New Zealand) |
| DSR: | Datenschutzrat/Council for Data Protection (Austria) |
| DSTL: | Defence Research Centre (United Kingdom) |
| DSTA: | Defence Science and Technology Agency (Singapore) |

| | |
|---|---|
| DSTL: | Defence Science and Technology Laboratory (United Kingdom) |
| DSTO: | Defence Science and Technology Organisation (Australia) |
| DTI: | Department of Trade and Industry (United Kingdom) |
| EAPC: | Euro-Atlantic Partnership Council |
| EBIOS: | Expression of the Needs and Identification of Security Objects (France) |
| ECI: | EU Critical Infrastructures (EU) |
| ECP.NL: | Electronic Commerce Platform in the Netherlands (The Netherlands) |
| EDS: | Electronic Digital Signature (Russia) |
| EFD: | Eidgenössisches Finanzdepartement / Swiss Federal Department of Finance (Switzerland) |
| EIA: | Electronic Industries Alliance (United States) |
| EJPD: | Eidgenössisches Justiz- und Polizeidepartement / Federal Department of Justice and Police (Switzerland) |
| ELAK: | Electronical File (Austria) |
| EMA: | Emergency Management Act (Canada) |
| EMP: | Electromagnetic Pulse |
| ENFSI: | European Network of Forensic Science Institute on Computer Crime (Austria) |
| ENISA: | European Network and Information Security Agency (EU) |
| EO: | Executive Order (United States) |
| EPA: | Environmental Protection Agency (United States) |
| EPCIP: | European Program for the Protection of Critical Infrastructure (EU) |
| ERA: | European Research Area (EU) |
| ESCG: | E-Security Coordination Group (Australia) |
| E-SCIE: | European Control Systems Information Exchange (EU) |
| ESPAc | E-Security Policy and Coordination (Australia) |
| ESRAB: | European Security Research Advisory Board (EU) |
| ESRP: | European Security Research Programme (EU) |
| ETA: | Electronic Transactions Act (Singapore) |
| ETH: | Eidgenössische Technische Hochschule / Swiss Federal Institute of Technology, ETH Zurich (Switzerland) |
| ETRI: | Electronics and Telecommunications Research Institute (Republic of Korea) |
| ETSI: | European Telecommunications Standards Institute (EU) |
| EU: | European Union |
| EUCIWIN: | Critical Infrastructure Warning and Information Network (EU) |
| EVD: | Eidgenössisches Volkswirtschaftsdepartement / Federal Department of Economic Affairs (Switzerland) |

| | |
|---|---|
| EXYSTENCE: | Complex Systems Network of Excellence (EU) |
| EZ: | Ministry of Economic Affairs (The Netherlands) |
| EZB: | Einsatzzentrale Basisraum (Austria) |
| FACA: | Federal Advisory Committee Act (United States) |
| FAPC: | Food and Agriculture Planning Committee (NATO) |
| FAPSI: | Federal Agency for Government Communications and Information (Russia) |
| FBI: | Federal Bureau of Investigation (United States) |
| FDCA: | Finnish Data Communication Association (Finland) |
| FDF: | Swiss Federal Department of Finance (Switzerland) |
| FedCIRC: | Federal Computer Incident Response Center (United States) |
| fedpol: | Federal Office of Police (Switzerland) |
| FEPC: | Federation of Electric Power Companies (Japan) |
| FERC: | Federal Energy Regulatory Commission (United States) |
| FFI: | Norwegian Defense Research Establishment (Norway) |
| FICORA: | Finnish Communications Regulatory Authority (Finland) |
| FIRST: | Forum of Incident and Security Response Teams |
| FMV: | Swedish Defense Material Administration (Sweden) |
| FOCP: | Federal Office for Civil Protection/Bundesamt für Bevölkerungsschutz (Schweiz) |
| FOI: | Swedish Defense Research Agency (Sweden) |
| FOIA: | Freedom of Information Act (United States) |
| FOITT: | Federal Office of Information Technology and Telecommunications (Switzerland) |
| FOKUS: | Fraunhofer Institute for Open Communications/Frauenhofer Institut für offene Kommunikationssysteme (Germany) |
| FP: | Framework Program (EU) |
| FRA: | Swedish National Defense Radio Establishment (Sweden) |
| FS/ISAC: | Financial Services Information Sharing and Analysis Center (United States) |
| FSB: | Federal Security Service of the Russian Federation (Russia) |
| FSUIT: | Swiss Federal Strategy Unit for Information Technology/Informatikstrategieorgan Bund (ISB) (Switzerland) |
| FTC: | Federal Trade Commission (United States) |
| G2B: | government to business |
| G2C: | government to citizen |
| G2G: | government to govern |
| G8: | Group of Eight |
| GAO: | General Accounting Office (United States) |

| | |
|---|---|
| GARR-CERT: | Gestione Ampliamento Rete Ricerca/Academic and Research Network -Computer Emergency Response Team (Italy) |
| GCA: | Global Cybersecurity Agenda (United Nations) |
| GCERT: | Government Computer Emergency Response Team (Malaysia) |
| GCHQ: | Government Communications Headquarters (United Kingdom) |
| GCSB: | Government Communications Security Bureau (New Zealand) |
| GCSG: | Communications-Electronics Security Group (United Kingdom) |
| GdIN: | Gruppo di Interesse Nazionale (Italy) |
| GEA: | Swedish Alliance for Electronic Commerce (Sweden) |
| GICT: | Global Information and Communication Technologies Department (World Bank Group) |
| GIP RENATER: | National Network of Telecommunications for Technology, Education, and Research (France) |
| GMLZ | Gemeinsames Melde- und Lagezentrum/Joint Reporting and Situation Center (Germany) |
| GSI: | Gabinete de Segurança Institucional/Institutional Security Cabinet (Brazil) |
| GOC: | Government Operations Centre (Canada) |
| GoL: | Government-on-Line (Canada) |
| GovCERT.au | Australian Government Computer Emergency Response Team (Australia) |
| GovCERT.ch | Swiss Government's Computer Emergency Response Team (Switzerland) |
| GovCERT.it | Italian Government Computer Emergency Response Team (Italy) |
| GOVCERT.NL: | Government-wide Computer Emergency Response Team (The Netherlands) |
| HERT: | Hacking Emergency Response Team (The Netherlands) |
| HHS: | Department of Health and Human Services (United States) |
| HLEG: | High Level Expert Group (United Nations) |
| HSPD: | Homeland Security Presidential Directive (United States) |
| HTCSG: | High-Tech Crime Subgroup (G8) |
| HTCTD: | High-Tech Crime Technology Division (Japan) |
| I3P: | Institute for Information Infrastructure Protection (United States) |
| IA: | Information Assurance |
| IAAC: | The Information Assurance Advisory Council (United Kingdom) |
| IAAGs: | Infrastructure Assurance Advisory Groups (Australia) |
| IABG: | Industrieanlagen-Betriebsgesellschaft (Germany) |
| IAG: | Infrastructure Analysis Group |
| IAIP: | Directorate for Information Analysis and Infrastructure Protection (United States) |

| | |
|---|---|
| ICCP: | Committee for Information, Computer, and Communications Policy (OECD) |
| ICD: | Infrastructure Coordination Division (United States) |
| ICI: | Istanbul Cooperation Initiative (NATO) |
| ICIC: | Internet Crime Investigation Center (Korea) |
| ICS: | Secretary of the Interdepartmental Committee on Security (New Zealand) |
| ICT: | Information and Communication Technologies |
| ICT-I: | ICT Infrastructure Unit (Switzerland) |
| IDA: | Infocomm Development Authority of Singapore |
| IDC: | Interdepartmental Committee on the Protection of the National Information Infrastructure (Australia) |
| IDS: | Intrusion Detection System |
| IIPC: | Information Infrastructure Protection Centre (India) |
| IIPG: | Information Infrastructure Protection Group (Australia) |
| IISI: | Institute Information Security Issues (Russia) |
| IMPACT: | International Multilateral Partnership Against Cyber-Terrorism (Malaysia) |
| INFOSEC: | Information Systems Security (Australia, New Zealand) |
| IO: | Information Operations |
| IOWG: | Information Operations Working Group |
| IPA: | Information Technology Promotion Agency (Japan) |
| IPAM: | Institute of Public Administration and Management (Singapore) |
| IPC: | Industrial Planning Committee (NATO) |
| IPs: | Infrastructure Profiles |
| IPSC: | Institute for the Protection and Security of Citizen |
| IRIS: | Interconnection of Computer Resources/Interconexión de los Recursos Informáticos (Spain) |
| IRItaly: | Incident Response Italy (Italy) |
| IRTs: | Incident Response Teams (Singapore) |
| ISAC: | Information Sharing and Analysis Center |
| ISCG: | Information Society Coordination Group (Switzerland) |
| ISCOM: | Institute for Information and Communication Technologies/Istituto superiore delle comunicazioni e delle tecnologie dell'informazione (Italy) |
| ISD: | Internal Security Department of the Ministry of Home Affairs (Singapore) |
| ISDF: | French Dependability Institute (France) |
| iSec: | IDA's Infocomm Security Division (Singapore) |
| ISF: | Information Sharing Forum (Malaysia) |
| ISI: | Information Security Inspectorate (Hungary) |

| | |
|---|---|
| ISIDRAS: | Information Security Incident Detection Reporting and Analysis (Australia) |
| ISIT: | Inter-Ministerial Board for Security (Germany) |
| ISN: | International Relations and Security Network (Switzerland) |
| ISP: | Internet Service Provider |
| ISPA: | Federation of the Austrian Internet Service Providers (Austria) |
| ISPC: | Information Security Policy Council (Japan) |
| ISSE: | Information Security Solutions Europe |
| IST: | Institute for Signal Intelligence and Technical Information (Sweden) |
| IST: | Information Society Technologies (EU) |
| ISTDC: | Information Security Technology Development Council (India) |
| ISZT: | Council of Hungarian Internet Service Providers (Hungary) |
| IT: | Information Technology |
| ITAA: | Information Technology Association of America (United States) |
| ITAC: | Integrated Threat Assessment Centre (Canada) |
| ITSC: | Information Technology Standards Committee (Singapore) |
| ITSEAG: | IT Security Expert Advisory Group (Australia) |
| ITSEC: | Information Technology Security Evaluation Criteria (France) |
| ITSEC: | IT Security (Norway) |
| ITU: | International Telecommunication Union |
| IuKDG: | Information and Telecommunications Services Act/Informations- und Kommunikationsdienste-Gesetz (Germany) |
| IWWN: | International Watch and Warning Network Conference |
| JIIRP: | Joint Infrastructures Interdependencies Research Program (Canada) |
| JPCERT/CC: | Japan Computer Emergency Response Coordination Center (Japan) |
| KBN: | State Committee for Scientific Research (Poland) |
| KCC: | Korea Communications Commission (Republic of Korea) |
| KFTC: | Korean Financial Telecommunication and Clearings Institute (Republic of Korea) |
| KF-ISAC: | Korea Financial Information Sharing and Analysis Center (Republic of Korea) |
| KIG: | Coordination Group for Information Society (Switzerland) |
| KIS: | National Information Security Co-ordination Council (Norway) |
| KISA: | Korean Information Security Agency (Republic of Korea) |
| KISC: | Korea Internet Security Center (Republic of Korea) |
| KISEC: | Korea IT Security Evaluation Center (Republic of Korea) |
| KISIA: | Korea Information Security Industry Association (Republic of Korea) |

| | |
|---|---|
| KISIS: | Korea Information Security Industry Support Center (Republic of Korea) |
| KLPD: | Korps Landelijke Politiediensten (Cyber Crime Unit of the Dutch Police) (The Netherlands) |
| KR: | Key Resources |
| KrCERT/CC: | Korea Computer Emergency Response Team Coordination Center (Korea) |
| KS-ISAC: | Korean Security Information Sharing and Analysis Center (Republic of Korea) |
| KSRC: | Korea Spam Response Center (Republic of Korea) |
| KWINT: | Kwetsbaarheid op Internet – Samen werken aan meer veiligheid en betrouwbaarheid (The Netherlands) |
| MAMPU: | Malaysian Administrative Modernization and Management Planning Unit (Malaysia) |
| MBG: | Militärbefugnisgesetz/Military Competence Law (Austria) |
| MCDA: | Multi-Criteria Decision Approach |
| MCMC: | Malaysian Communications and Multimedia Commission (Malaysia) |
| MD: | Mediterrean Dialogue (NATO) |
| MEAC: | Ministry of Economic Affairs and Communication (Estonia) |
| MELANI: | Reporting and Analysis Center for Information Assurance (Switzerland) |
| METI: | Ministry of Economy, Trade and Industry (Japan) |
| MEWC: | Ministry of Energy, Water and Communications (Malaysia) |
| MHA: | Ministry of Home Affairs (Singapore) |
| MIBA: | Hungarian Information Security Evaluation and Certification Scheme (MIBETS) and Information Security Management Framework (MIBIK) jointly (Hungary) |
| MIBETS: | Hungarian Information Security Evaluation and Certification Scheme (Hungary) |
| MIBIK: | Information Security Management Framework (Hungary) |
| MIC: | Ministry of Information and Communication (Korea) |
| MIC: | Ministry of Internal Affairs and Communications (Japan) |
| MICA: | Ministry of Information, Communications, and the Arts (Singapore) |
| MIT: | Ministry for Innovation and Technologies (Italy) |
| MMS: | Multimedia Messaging Service |
| MOC: | Ministry of Communications and Information Technology (India) |
| MoI: | Ministry of the Interior and Kingdom Relations (The Netherlands) |
| MoD: | Ministry of Defense |

| | |
|---|---|
| MODCERT: | Ministry of Defence Computer Emergency Response Team (United Kingdom) |
| MOPAS: | Ministry of Public Administration and Security (Republic of Korea) |
| MOSTI: | Ministry of Science, Technology and Innovation (Malaysia) |
| MTA SZAKI: | Computer and Automation Research Institute of the Hungarian Academy of Sciences (Hungary) |
| MTP: | Multi-annual Thematic Programmes (EU) |
| MyCERT: | Malaysian Computer Emergency Response Team (Malaysia) |
| MyMIS: | Malaysian Public Sector Management of Information and Communications Technology Security Handbook (Malaysia) |
| NACOTEL: | National Continuity Plan for Telecommunications (The Netherlands) |
| NaCTSO: | National Counter Terrorism Security Office (United Kingdom) |
| NAS: | National Alert Service (Hungary) |
| NASK: | Research and Academic Computer Network/Data networks operator (Poland) |
| NASSCOM: | National Association of Software and Service Companies (India) |
| NATO: | North Atlantic Treaty Organisation |
| NAVI: | Dutch Nationaal Adviescentrum Vitale Infrastructuur/National Advisory Centre Critical Infrastructures (The Netherlands) |
| NAZ: | Nationale Alarm Zentrale/National Emergency Operations Center Agency (Switzerland) |
| NBED: | National Board of Economic Defense (Finland) |
| NCA: | National Communications Authority (Hungary) |
| NCMC: | National Cyberthreat Monitoring Centre (Singapore) |
| NCB: | National Computer Board (Singapore) |
| NCC: | National Crisis Center (The Netherlands) |
| NCC: | National Coordinating Center (United States) |
| NCI: | National Critical Infrastructures |
| NCIA: | National Critical Infrastructures Assurance Program (Singapore) |
| NCIAP: | National Critical Infrastructure Assurance Program (Canada) |
| NCIPP: | National Critical Infrastructure Protection Program (Canada) |
| NCO-T: | National Continuity Forum Telecommunications (The Netherlands) |
| NCMC: | National Cyberthereat Monitoring Centre (Singapore) |
| NCPG: | National Contingency Planning Group (Canada) |
| NCS: | National Communications System (United States) |
| NCSA: | National Cyber Security Alliance (United States) |
| NCSC: | National Cyber Security Center (Korea) |
| NCSD: | National Cyber Security Division (United States) |

| | |
|---|---|
| NCSP: | National Cyber Security Partnership (United States) |
| NCTC: | National Counter-Terrorism Committee (Australia) |
| NCTb: | Dutch National Coordinator for Counterterrorism (The Netherlands) |
| NCTP: | National Counter-Terrorism Plan (Australia) |
| NDMS: | National Disaster Mitigation Strategy (Canada) |
| NeGP: | National e-Governance Action Plan (India) |
| NERC: | North American Electricity Reliability Council (United States) |
| NERS: | National Emergency Response System (Canada) |
| NES: | Federal Office for National Economic Supply/Bundesamt für Wirtschaftliche Landesversorgung (BWL) (Switzerland) |
| NESA: | National Emergency Supply Agency (Finland) |
| NESC: | National Emergency Supply Council (Finland) |
| NEST: | National Emergency System (Singapore) |
| NGO: | Non-Governmental Organization |
| NHTCC: | National High Tech Crime Center (The Netherlands) |
| NHTCU: | National Hi-Tech Crime Unit (United Kingdom) |
| NIAC: | National Infrastructure Advisory Council (United States) |
| NIB: | National Information Board (India) |
| NIC: | National Informatics Centre (India) |
| NIC.br: | Network Information Centre (Brazil) |
| NICC: | National Infrastructure against Cybercrime (The Netherlands) |
| NIFF: | National Information Infrastructure Development Program (Hungary) |
| NIIF-CSIRT: | Computer Security Incidents Response Team of the National Information Infrastructure Development Program (Hungary) |
| NII: | National Information Infrastructure |
| NIIP: | National Information Infrastructure Protection (New Zealand) |
| NIPC: | National Infrastructure Protection Center (United States) |
| NIPP: | National Infrastructure Protection Plan (United States) |
| NIRA: | National Infrastructure Risk Assessment (Canada) |
| NIRT: | National Incident Response Team (Japan) |
| NIS: | National Intelligence Service (Republic of Korea) |
| NISA: | National Information Security Alliance (Korea) |
| NISC: | National Infocomm Security Committee (Singapore) |
| NISC: | National Information Security Center (Japan) |
| NISCC: | National Information Security Coordination Cell (India) |
| NISCC: | National Infrastructure Security Co-ordination Centre (United Kingdom) |

| | |
|---|---|
| NISER: | National ICT Security and Emergency Response Centre (Malaysia) |
| NISRI: | National Security Research Institute (Korea) |
| NIST: | National Institute of Standards and Technology (United States) |
| NITA: | National IT Agenda (Malaysia) |
| NITAS: | National Information Technology Alert Service (Australia) |
| NITC: | National Information Technology Council (Malaysia) |
| NLIP: | Branchevereniging van Nederlandse Internet Providers/Consortium of Dutch Internet Providers (The Netherlands) |
| NOC: | Network Operation Centre (Russia) |
| NorCERT: | Norwegian Computer Emergency Response Team (Norway) |
| NorSIS: | Norwegian Center for Information Security (Norway) |
| NPA: | National Police Agency (Japan) |
| NPB: | Swedish National Police Board (Sweden) |
| NPSI: | National Plan for Information Infrastructure Protection (Germany) |
| NPT: | Norwegian Post and Telecommunications Authority (Norway) |
| NRC: | Canadian National Research Council (Canada) |
| NSA: | National Security Agency (United States) |
| NSAC: | National Security Advice Centre (United Kingdom) |
| NSCS: | National Security Council Secretariat (India) |
| NSD: | Industry Security Delegation (Sweden) |
| NSM: | Norwegian National Security Authority (Norway) |
| NSRI: | National Security Research Institute (Korea) |
| NSSC: | National Strategy to Secure Cyberspace (United States) |
| NSSO: | National Security Supervision Office (Hungary) |
| NUS: | National University of Singapore (Singapore) |
| NZCS SigSec: | Computer Society Special Interest Group on Security (New Zealand) |
| NZSA: | New Zealand Security Association (New Zealand) |
| NZSIS: | New Zealand Security Intelligence Service (New Zealand) |
| NZSIT: | New Zealand Security of Information Technology (New Zealand) |
| OASD/NII: | Office of the Assistant Secretary of Defense for Networks and Information Integration (United States) |
| OCIIP: | Office of Computer Investigations and Infrastructure Protection (United States) |
| OCIPEP: | Office of Critical Infrastructure Protection and Emergency Preparedness (Canada) |
| OCSI: | Organismo die Certificazione della Sicurezza Informatica (Italy) |

| | |
|---|---|
| ODESC: | Officials Committee for Domestic and External Security Coordination (New Zealand) |
| OEA: | Office of Energy Assurance (United States) |
| OEC: | Office of Emergency Communications (United States) |
| OECD: | Organisation for Economic Co-operation and Development |
| OFCOM: | Federal Office for Communication (Switzerland) |
| OGIT: | Office of Government Information Technology (Australia) |
| OGO: | Office for Government On-line (Australia) |
| OIP: | Office of Infrastructure Protection (United States) |
| OKOKRIM: | National Authority for Investigation and Prosecution of Economic and Environmental Crime (Norway) |
| OST: | Office of Science and Technology (Uniteg Kingdom) |
| PAGSI: | Government Action Program for an Information Society (France) |
| PB&C: | Planning Board and Committee (NATO) |
| PBIST: | Planning Board for Inland Surface Transportation (NATO) |
| PBOS: | Planning Board for Ocean Shipping (NATO) |
| PCCIP: | Presidential Commission on Critical Infrastructure Protection (United States) |
| PCIIP: | Protected Critical Infrastructure Information Programm (United States) |
| PCIS: | Partnership for Critical Infrastructure Security (United States) |
| PDD: | Presidential Decision Directives (United States) |
| PKI: | Public Key Infrastructure |
| PPO: | Planning and Partnerships Office (PPO) |
| PSB: | Productivity and Standards Board (Singapore) |
| PSC: | Public Safety Canada |
| PSD: | Protective Services Divison (United States) |
| PSEPC: | Public Safety and Emergency Preparedness Canada (Canada) |
| PSS: | Public Safety and Security (Sweden) |
| PSYOP: | Psychological Operations |
| PTS: | Swedish National Post and Telecom Agency (Sweden) |
| R&D: | Research and Development |
| RAKEL: | Radio Communication for Efficient Command (Sweden) |
| RANS: | Russian Association of Networks and Services (Russia) |
| RBNET: | Russian Backbone Network |
| RCMP: | Royal Canadian Mounted Police (Canada) |
| RegTP: | Regulatory Authority for Telecommunications and Posts (Germany) |
| RIPE : | European IP Networks/Réseaux IP Européens |
| RIPN: | Russian Institute of Public Networks |

| | |
|---|---|
| RIA: | Estonian Informatics Centre (Estonia) |
| RISO: | Department of State Information System (Estonia) |
| RMA: | Revolution in Military Affairs |
| RNP: | National Education and Research Network/Rede Nacional de Ensino e Pesquisa (Brazil) |
| RU-CERT: | Computer Emergency Response Team of Russia (Russia) |
| S&T: | Science and Technology (United States) |
| SAI: | Centro Virtuale di Simulazione e Analisi delle Interdipendenze/ Interdependencies Simulation and Analysis Center (Italy) |
| SÄPO: | Swedish Security Service (Sweden) |
| SBA: | Vulnerability Assessment/SårBarhetsAnalys (Sweden) |
| SCADA: | Supervisory Control and Data Acquisition |
| SCC: | Sector Coordinating Council (United States) |
| SCCA: | Swedish Civil Contingencies Agency (Sweden) |
| SCEPC: | Senior Civil Emergency Planning Committee (NATO) |
| SCNS: | Secretaries' Committee on National Security (Australia) |
| SCO: | Shanghai Cooperation Organization (SCO |
| SCOs: | Sectoral Cyber Security Officers (India) |
| SCSSI: | Service Central de la Sécurité des Systèmes d'Information (France) |
| SEI: | Software Engineering Institute (United States) |
| SEMA: | Swedish Emergency Management Agency (Sweden) |
| SERPRO: | Serviço Federal de Processamento de Dados/Federal Data Processing Service (Brazil) |
| SERTIT: | Certification Authority for IT Security in Norway (Norway) |
| SFU: | Strategische Führungsübung/Strategic Leadership Exercise (Switzerland) |
| SGDN: | General Secretariat of National Defense (France) |
| SIG: | Special Interest Group (FIRST) |
| SigG: | Electronic Signature Law (Austria) |
| SIGINT: | Signals Intelligence |
| SII: | Strategic Infrastructure Initiative (Canada) |
| SingCERT: | Singapore Computer Emergency Response Team (Singapore) |
| SIS: | Center for Information Security (Norway) |
| SIS: | Schengen Information System |
| SITIC: | Swedish IT Incident Centre (Sweden) |
| SLT: | Strategic Leadership Training (Switzerland) |
| SMEs: | Small and Medium Enterprises |
| SMS: | Short Message Service |
| SNZ: | Standards New Zealand (New Zealand) |

| | |
|---|---|
| SOCA: | Serious Organised Crime Agency (United Kingdom) |
| SONIA: | Sonderstab Information Assurance / Special Task Force on Information Assurance (Switzerland) |
| SOVI: | Strategic Board for CIP / Strategisch Overleg Vitale Infrastructuur (The Netherlands) |
| SPF: | National Board of Psychological Defence (Sweden) |
| SPF: | Singapore Police Force (Singapore) |
| SPF: | National Board of Psychological Defense (Sweden) |
| SPG: | Security Police Law / Sicherheitspolizeigesetz (Austria) |
| SRSA: | Swedish Rescue Services Agency (Sweden) |
| SSI: | Security of Information Systems (France) |
| SSITAD: | Technical Committee for the Security of Information Systems and Personal Data Processing / Comité Técnico de Seguridad de los Sistemas de Información y Tratamiento Automatizado de Datos Personales (Spain) |
| SSP: | Sector-Specific Plans (United States) |
| StGB: | Austrian Penal Code (Austria) |
| StPO: | Strafprozessordnung / Penal Procedure (Austria) |
| STQC: | Standardization Testing & Quality Certification (India) |
| SWANs: | State Wide Area Networks (India) |
| SWITCH: | Swiss Education and Research Network (Switzerland) |
| TAS: | Telecommunications Authority of Singapore |
| TCD: | Technology Crime Division within the Police Force (Singapore) |
| TDDSG: | Teledienstdatenschutzgesetz (Germany) |
| Tekes: | National Technology Agency (Finland) |
| Telecom-ISAC: | Telecom Information Sharing and Analysis Center (Japan) |
| TERENA: | Trans-European Research and Education Networking Association |
| TESTA: | Trans-European Services for Telematics between Administrations |
| TIEKE: | Finnish Information Society Development Centre (Finland) |
| TISN: | Trusted Information Sharing Network for Critical Infrastructure Protection (Australia) |
| TKG: | Telekommunikationsgesetz/Telecommunication Law (Austria) |
| TMG: | Telecommunications and Media Act / Telemediengesetz (Germany) |
| TNO: | Netherlands Organization for Applied Scientific Research (The Netherlands) |
| TSA: | National Communications Security Group (Sweden) |
| TSWG: | Technical Support Working Group (UN) |
| UN: | United Nations |
| UN ECOSOC: | United Nations Economic and Social Council |

| | |
|---|---|
| UNIDIR: | United Nations Institute for Disarmament Research (UN) |
| UNINETT | Academic Research Network (Norway) |
| UNIRAS: | Unified Incident Reporting and Alert Scheme (United Kingdom) |
| UNITAR: | United Nations Institute for Training and Research (UN) |
| USA PATRIOT: | (Act) Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (United States) |
| US-CERT: | United States Computer Emergency Response Team (United States) |
| V&W: | Ministry of Transport, Public Works, and Water Management (The Netherlands) |
| VAHTI: | Steering Committee for Data Security in State Administration (Finland) |
| VDI: | Warning System for Digital Infrastructure (Norway) |
| VEC: | Veilige Elektronische Communicatie (The Netherlands) |
| VIS: | Visa Information System |
| VROM: | Ministry of Housing, Spatial Planning, and the Environment (The Netherlands) |
| VWS: | Ministry of Health, Welfare and Sport (The Netherlands) |
| WARP: | Warning, Advice, and Reporting Point (United Kingdom) |
| WPISP: | Working Party on Information Security and Privacy (OECD) |
| WSIS: | World Summit on the Information Society (ITU/UN) |
| Y2K: | Year 2 Kilo/Year 2000 Problem/millennium bug |
| ZAS: | Zentrales Ausweichsystem (Austria) |
| ZES: | Zentrum für europäische Strategieforschung/Center for Strategic Studies (Germany) |
| MEAC: | Ministry of Economic Affairs and Communication (Estonia) |
| RISO: | Department of State Information System (Estonia) |
| RIA: | Estonian Informatics Centre |

# Introduction

## Background

The importance of protecting infrastructures has greatly increased in the global security political debate of late, due in particular to the traumatic terrorist attacks in New York and Washington (2001), Madrid (2004), and London (2005). In all of these cases, the perpetrators exploited elements of the civilian infrastructure for the purpose of indiscriminate murder. In the case of the 11 September 2001 attacks in the US, they used the transport infrastructure by turning airplanes into weapons. In Europe, trains, underground railways, and train stations as well as computers were targeted. This approach not only demonstrated the brutal nature of the "new terrorism", but also reinforced the view that traditional concepts of domestic security were no longer commensurate to contemporary requirements and needed to be adapted.

Long before these attacks, the protection of strategically important installations in the domestic economic and social sphere had already been an important part of national defense concepts.[1] The term "Critical Infrastructure Protection" (CIP), however, refers to a broader concept with a distinctly new flavor. First of all, it is no longer restricted to concrete defense against immediate dangers or criminal prosecution after a crime has been committed, but increasingly refers to preventive security measures as well. Furthermore, contemporary modern societies have become significantly more vulnerable, and the spectrum of possible causes of disruptions and crises has become broader and more diffuse. This is why CIP has become a crystallization point for current security policy debates.[2]

[1] Cf. Luiijf, Eric A.M., Helen H. Burger, and Marieke H.A. Klaver. "Critical Infrastructure Protection in The Netherlands: A Quick-scan". In: Gattiker, Urs E., Pia Pedersen, and Karsten Petersen (eds.). EICAR Conference Best Paper Proceedings 2003, http://cipp.gmu.edu/archive/2_NetherlandsCIdefpaper_2003.pdf [last accessed in June 2008].

[2] Dunn Cavelty, Myriam and Kristian Søby Kristensen (2008). "Securing the Homeland: Critical Infrastructure, Risk, and (In)Security". London: Routledge.

## From Threats to Risks

The genesis and establishment of the concept of CIP is the result of two interlinked and at times mutually reinforcing factors: The expansion of the threat spectrum after the Cold War, especially in terms of malicious actors and their capabilities on the one hand, and a new kind of vulnerability due to modern society's dependency on inherently insecure information systems on the other.

During the Cold War, threats were mainly perceived as arising from the aggressive intentions of states to achieve domination over other states. Among other things, the end of the Cold War also heralded the end of unambiguous threat perceptions: Following the disintegration of the Soviet Union, a variety of "new" threats were moved onto the security policy agendas of most countries.[3] The main distinguishing quality of these "new" challenges is the element of uncertainty that surrounds them: uncertainty concerning the identity and goals of potential adversaries, the timeframe within which threats are likely to arise, the contingencies that might be imposed on the state by others, the capabilities against which one must prepare, and uncertainty about the type of challenge one had to prepare for.[4] Clearly, the notion of "threat" as something imminent, direct, and certain no longer accurately describes these challenges. Rather, they can be characterized as "risks", which are by definition indirect, unintended, uncertain, and situated in the future, since they only materialize when they occur in reality.[5]

As a result of these diffuse risks and due to difficulties in locating and identifying enemies, part of the focus of security policies has shifted away from actors, capabilities, and motivations towards general vulnerabilities of entire societies. The catchphrase in this debate is "asymmetry", and the US military has been a driving force behind the shaping of this threat perception in the early 1990s.[6] The

[3] Buzan, Barry, Ole Wæver, and Jaap de Wilde (1998). "Security: A New Framework for Analysis". Boulder: Lynne Rienner.

[4] Goldman, Emily O. (2001). "New Threats, New Identities and New Ways of War: The Sources of Change in National Security Doctrine". Journal of Strategic Studies. Vol. 24, pp. 12–42.

[5] Bailes, Alyson J. K. (2007). "Introduction: A world of risk". In: SIPRI Yearbook 2007: Armaments, Disarmament and International Security, pp. 1–20; Beck, Ulrich (1999). "World Risk Society". Cambridge: Polity Press.

[6] Rattray, Greg. (2001). "Strategic Warfare in Cyberspace". Cambridge: MIT Press.

US as the only remaining superpower was seen as being predestined to become the target of asymmetric warfare. Specifically, those adversaries who were likely to fail against the American war machine might instead plan to bring the US to its knees by striking against vital points at home that are fundamental not to the military alone, but to the essential functioning of industrialized societies as a whole.[7] These points are generally defined as critical infrastructures (CI). They are deemed critical because their incapacitation or destruction would have a debilitating impact on the national security and the economic and social welfare of a nation.[8]

Fear of asymmetrical measures against such "soft targets" was aggravated by the second factor: the so-called information revolution. Most of the CI relies on a spectrum of software-based control systems for smooth, reliable, and continuous operation. In many cases, information and communication technologies (ICT) have become all-embracing, connecting other infrastructure systems and making them interrelated and interdependent. These technologies are in general regarded as inherently insecure: Security has never been a system design driver, and pressure to reduce time-to-market is intense, so that a further explosion of computer and network vulnerabilities is to be expected, leading to the emergence of infrastructures with in-built instability, critical points of failure, and extensive interdependencies.[9] At the same time, the spread of ICT was (and is) seen to make it much easier to attack asymmetrically, as big, specialized weapons systems or an army are no longer required. Borders, already porous in many ways in the real world, are nonexistent in cyberspace.

[7] Berkowitz, Bruce D. (1997). "Warfare in the Information Age". In: John Arquilla and David Ronfeldt (eds). In Athena's Camp: Preparing for Conflict in the Information Age. Santa Monica: RAND, pp. 175–90.

[8] The definition of what to include in a definition of critical infrastructure varies slightly from country to country. This Handbook shows in detail how each country defines the critical infrastructure and what sectors are included.

[9] Rathmell, Andrew (2001). "Controlling Computer Network Operations". Information & Security: An International Journal. Vol. 7, pp. 121–44.

## Evolution of the Critical (Information) Infrastructure Protection (CIIP) Issue

Commensurate with this threat perception, the US was the first nation to address the new vulnerability of the vital infrastructures in a broad and concerted effort. New risks in designated sectors[10] like information and communications, banking and finance, energy, physical distribution, and vital human services were identified by the Presidential Commission on Critical Infrastructure Protection (PCCIP).[11] The PCCIP concluded in 1997 that the US was so dependent on these infrastructures that the government had to view them through the lens of a "national security focus", since serious consequences for the entire nation were to be expected if these elements were unavailable for any significant amount of time.

According to this approach, critical infrastructures should be understood to include material and IT assets, networks, services, and installations that, if disrupted or destroyed, would have a serious impact on the health, security, or economic well-being of citizens and the efficient functioning of a country's government. Such infrastructures could be damaged by structural threats as well as by intentional, actor-based attacks. The first risk category would, for example, include natural catastrophes, human-induced catastrophes (e.g., dam failure, nuclear reactor accident), personnel shortages through strikes or epidemics, organizational shortcomings due to technical or personal failures, human error, technical outages, and dependencies and supply shortages. In the second category, the spectrum of possible attackers is extensive, ranging from bored teenagers, disaffected or dissatisfied employees, organized crime, fanatics and terrorist cells, to hostile states.

[10] A sector is defined as "A group of industries or infrastructures which perform a similar function within a society", see: President's Commission on Critical Infrastructure Protection (PCCIP). "Critical Foundations: Protecting America's Infrastructures". Washington, October 1997: Appendix B, Glossary, B-3. http://www.ihs.gov/misc/links_gateway/download.cfm?doc_id=327&app_dir_id=4&doc_file=PCCIP_Report.pdf [last accessed in June 2008]. Publication quoted in the following as PCCIP.

[11] Ibid.

There is an equally broad range of attack options, including hacker attacks as well as the physical destruction of civilian or military installations. The main focus of early CIP efforts was, however, directed towards the as-yet largely unknown risks emanating from cyberspace: The global information infrastructure appeared to facilitate anonymous attacks from anywhere in the world, while at the same time serving as a source for hacker tools for everyone. Based on this threat perception, a CIP policy crystallized under US President Bill Clinton that was largely directed towards information security. In many ways, other countries followed this lead with a similar focus on the information aspect. The first edition of the CIIP Handbook was clearly influenced by a similar understanding of CIP.

However, since the terrorist attacks of 11 September 2001, there has been a noticeable return of the classical threat concept to the CIP debate. Especially from the US point of view, efforts have been made since then to tackle a series of structural threats within the framework of an increasingly actor-oriented counter-terrorism strategy. In the US, CIP became a key component of Homeland Security and is currently discussed predominantly with a view to developing strategies against terrorism. In this context, the physical aspects of CIP have gained more attention, while the importance of information aspects has diminished slightly in comparison. In the meantime, this CIP focus on counterterrorism has also become a hallmark of recent debates in the EU, which has recently begun to develop a CIP policy that consists mainly of coordinating the measures adopted by member states. The same is true for other parts of the world.

## Distinction between CIP and CIIP

Despite these fluctuations in how CIP is viewed, the CIIP Handbook will continue to focus on critical *information* infrastructure protection. That is, at times, easier said than done: More than ten years after the beginning of the CIP debate, there still is little clarity with regard to a clear and stringent distinction between the two key terms “CIP” and “CIIP”. In official publications, the term CIP is frequently used even if the document is only referring to the information aspects of the issue.

The reason for this is that the two cannot and should not be discussed as completely separate concepts. In our view, CIP is more than CIIP, but CIIP is an essential part of CIP. An exclusive focus on cyber-threats that ignores important traditional physical threats is just as dangerous as the neglect of the virtual dimension – what is needed is a sensible handling of both interrelated concepts. Nonetheless, there is at least one characteristic for distinguishing between the two: While CIP comprises all critical sectors of a nation's infrastructure, CIIP is only a subset of a comprehensive protection effort, as it focuses on measures to secure the critical *information* infrastructure. A Handbook on CIP would have to be considerably more extensive. The definition of exactly what should be subsumed under CI, and what should come under the heading of CII, is another question: Generally, the CII is that part of the global or national information infrastructure that is essentially necessary for the continuity of a country's critical infrastructure services. The CII, to a large degree, consists of, but is not fully congruent with, the information and telecommunications sector, and includes components such as telecommunications, computers/software, the internet, satellites, fiber-optics, etc. The term is also used for the totality of interconnected computers and networks and their critical information flows.

Due to their role in interlinking various other infrastructures and also providing new ways in which they can be targeted, information infrastructures do play a very specific role in the debate, as we have already mentioned. They are regarded as the backbone of critical infrastructures, given that the uninterrupted exchange of data is essential to the operation of infrastructures in general and the services that they provide. Centralized SCADA (Supervisory, Control, and Data Acquisition) systems are widely employed to monitor and control infrastructures remotely. But SCADA-based systems are not secure: once-cloistered systems and networks are increasingly using off-the-shelf products and IP-based networking equipment, and require interconnection via the internet, which opens the door to attackers from the outside in addition to those on the inside.

## Purpose and Key Questions

The CIIP Handbook focuses on *national governmental efforts* to protect critical (information) infrastructure. The overall purpose of the International CIIP Handbook is to provide an overview of CII protection practices in an increasingly broad range of countries. The initial eight country studies in the 2002 edition (Australia, Canada, Germany, the Netherlands, Norway, Sweden, Switzerland, and the United States) were substantially updated and supplemented by six additional surveys in the following 2004 edition (Austria, Finland, France, Italy, New Zealand, and the United Kingdom). In 2006, we added an additional six country surveys to the existing 14, with a distinct focus on Asia (India, Japan, the Republic of Korea, Malaysia, Russia, and Singapore). The current edition includes another five countries (Brazil, Estonia, Hungary, Poland, and Spain).

The Handbook is aimed mainly at security policy analysts, researchers, and practitioners. It can be used either as a reference work for a quick overview of the state of the art in CIIP policy formulation, or as a starting point for further, more in-depth research. As in previous years, the Handbook does not offer any benchmarking or analysis of these policies. This is done in additional publications of the Center for Security Studies.

## Structure of Country Surveys

For each country survey, five focal points of high importance covering conceptual and organizational aspects of CIIP are considered:

1. The definition of **critical sectors**: The first section lists the critical sectors identified by the specific country and provides, when available, definitions of CII and CIIP.
2. **Past and present CIIP initiatives and policy**: The second section gives an overview of the most important steps taken at the governmental level since the late 1990s to handle CIIP. The focus is on initiatives and the main elements of CIIP policy. This includes descriptions of specific committees,

commissions, task forces, and working groups, the main findings of key official reports and fundamental studies, and important national programs.

3 **Organizational structures**: The third section gives an overview of important public actors in the national CIIP organizational framework. It only characterizes the specific responsibilities or public actors at the state (federal) level (such as ministries, national offices, agencies, coordination groups, etc.). Public actors at the lower state level and private actors (companies, industry, etc.) are omitted. Due to the growing importance of public-private partnerships, the most important of these are also presented.

4 **Early-warning approaches and public outreach**: The fourth section describes national organizations responsible for CIIP early warning, namely CIIP-related information-sharing organizations such as CERTs (Computer Emergency Response Teams), ISACs (Information Sharing and Analysis Centers), etc. Furthermore, reference is made to the development of comprehensive early-warning alert and incident response structures. Moreover, public outreach initiatives are described.

5 **Law and legislation**: The fifth section lists important pieces of legislation enacted for the promotion of CIIP. This includes acts defining the responsibilities of the government authorities in case of emergencies as well as legislation dealing with issues such as technical IT security, data protection, damage to data, fraudulent use of a computer, the handling of electronic signatures, etc.

## Structure of Surveys of International Protection Policies

It is well known that threats to CIP/CIIP do not respect functional or geographic boundaries, and the various sectors share cross-border vulnerabilities and interdependencies. This is especially true as all infrastructures rely on energy and telecommunications for support. All of the above factors strengthen the case for making CIP/CIIP an international co-operation effort: Strong international partnerships between governments and critical infrastructure owners and operators are becoming essential. The security of cyberspace has become an important consideration in many countries, and governments worldwide are already putting a fair amount of effort into cyber-security. The 2003 WSIS Declaration of Principles[12] and two succeeding UN resolutions[13] rightly state that a global culture of cyber-security is a prerequisite for the development of the Information Society and for building confidence among users of ICTs.

Many international organizations are dealing with this challenge and have taken steps to raise awareness, establish international partnerships, and agree on common rules and practices. In its second part, the CIIP Handbook looks at protection policies by ***international organizations, institutions and initiatives***, namely the European Union (EU), the Forum of Incident Response and Security Teams (FIRST), the G8 Group, NATO, the OECD, the United Nations (UN), and the World Bank Group. Each chapter is structured individually.

## Methodology

The surveys were compiled in a three-step procedure.

1 First, open-source material was collected from online resources, publicly available government papers, workshops, and conference proceedings. This information was used to write a first draft of the country surveys. However, the availability of this open-source information, and especially the availability of documents on the internet, varies considerably in quantity and

[12] World Summit on the Information Society. "Declaration of Principles Building the Information Society: A Global Challenge in the New Millennium". Document WSIS-03/GENEVA/DOC/4-E, 12 December 2003. http://www.itu.int/wsis/docs/geneva/official/dop.html [last accessed in June 2008]; World Summit on the Information Society. "Plan of Action". Document WSIS-03/GENEVA/DOC/5-E, 12 December 2003. http://www.itu.int/wsis/docs/geneva/official/poa.html [last accessed in June 2008].

[13] In UN Resolution 57/239 of December 2002, the UN General Assembly outlined elements for creating a global culture of cyber-security, inviting member states and all relevant international organizations to take account of them in their preparations for the summit. In December 2003, UN Resolution 58/199 further emphasized the promotion of a global culture of cyber-security and the protection of critical information infrastructures.

quality from country to country. Additionally, a lot of relevant information is only available in the original language.

2 The second and most important step was the collaboration with the national experts from government and government-related organizations in the field and from academic institutions. The experts were asked to correct, complete, and update the draft country surveys.[14]

3 Finally, all of the input by national and international experts was worked into the final versions of the country studies and surveys of the international protection policies.

Since expert input was crucial for all country surveys, it is obvious that the individual perspectives and viewpoints of the consulted experts had a significant impact on the end result. This is also one of the major reasons why the individual surveys differ considerably in focus and general direction, and in their understanding of the nature of CIIP.

The Handbook includes an extensive appendix, with a bibliography for each country containing the most important documents, a collection of links, and a list of the experts involved.[15] In addition, the "Countries at a Glance" pages provide a quick overview of the most important actors and documents in each country.

As the information revolution is an ongoing and dynamic process that is fundamentally changing the fabric of security and society, continuing efforts to understand these changes are necessary. This requires research into information-age security issues, the identification of new vulnerabilities, and new ways for countering threats efficiently and effectively. The International CIIP Handbook aims to make a small contribution towards this ambitious goal. The entire publication is available on the internet (http://www.crn.ethz.ch). We kindly ask the reader to inform us of any inaccuracies or to submit any comments regarding the content. The Center for Security Studies further plans to establish a "special

[14] The authors tried to include all the opinions of the persons contacted. Without the invaluable support and help of these experts, this work would not have been possible. In the final version, however, the Handbook represents solely the authors' views and interpretations. The deadline for information-gathering and expert input was 15 June 2008. More recent developments could not be considered in this edition.

[15] All links last checked in May 2008.

interest community" in the field of CIIP in order to foster increased collaboration between topical experts in CIIP in 2009. An online version of the CIIP Handbook will be part of this community.

# Part I

# CIIP Country Surveys

# Australia

## Critical Sectors

Australia takes an all-hazards approach to the protection of critical infrastructures, whether information-based or not. The definition of critical infrastructure (CI) accepted by Australia is "those physical facilities, supply chains, information technologies and communication networks that, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic well-being of the nation or affect Australia's ability to conduct national defense and ensure national security."[1] The national information infrastructure (NII) is a subset of the critical infrastructure. As in many countries, the majority of the elements of the critical infrastructure are owned or operated as commercial enterprises.

In Australia, the CIP program is led by the Attorney-General's Department (AGD), primarily through the Trusted Information Sharing Network for Critical

[*] The Country Survey of Australia 2008 was reviewed by Alex Webling, Attorney-General's Department, Australian Government.

[1] Attorney-General's Department National Security Website. http://www.ag.gov.au/www/agd/agd.nsf/Page/Nationalsecurity_CriticalInfrastructureProtection.

Infrastructure Protection (TISN). The TISN brings together the nine sectors considered to be critical to Australia. These are:[2]

- Communications (Telecommunications (Phone, Fax, Internet, Cable, Satellites) and Electronic Mass Communications),
- Energy (Gas, Petroleum Fuels, Refineries, Pipelines, Electricity Generation and Transmission),
- Banking and Finance (Banking, Finance, and Trading Exchanges),
- Food Supply (Bulk Production, Storage, and Distribution),
- Emergency Services,
- Health (Hospitals, Public Health, and Research and Development Laboratories),
- Mass Gatherings (Icons (e.g., Sydney Opera House) and places of mass gatherings)
- Transport (Air Traffic Control, Road, Sea, Rail, and Inter-modal (Cargo Distribution Centers)),
- Utilities (Water, Waste Water, and Waste Management).

## Past and Present Initiatives and Policies

### Guiding Principles of Australia's CIP Policy

Critical Infrastructure Protection (CIP) requires the active participation of the owners and operators of infrastructure, regulators, professional bodies, and industry associations, in cooperation with all levels of government, and the public. To ensure this cooperation and coordination, all of these participants should commit to the following set of common, fundamental principles of CIP.[3] These principles are to be read as a whole, as each sets the context for the one following.

[2] http://www.tisn.gov.au/agd/WWW/TISNhome.nsf/Page/Business-Govt_partnership.

[3] http://www.tisn.gov.au/.

- CIP is centered on the need to minimize risks to public health, safety, and confidence, to ensure Australia's economic security and maintain the country's international competitiveness, and to ensure the continuity of government and its services;
- The objectives of CIP are to identify critical infrastructure, analyze vulnerability and interdependence, and protect Australia from, and prepare for, all hazards;
- Because all critical infrastructures cannot be protected from all threats, appropriate risk management techniques should be used to determine their relative severity and duration, the level of protective security, and to set priorities for the allocation of resources and the application of the best mitigation strategies for business continuity;
- The responsibility for managing risk within physical facilities, supply chains, information technologies, and communication networks primarily rests with the owners and operators;
- CIP needs to be undertaken with an all-hazards approach, with full consideration of interdependencies between businesses, sectors, jurisdictions, and government agencies;
- CIP requires a consistent cooperative partnership between the owners and operators of critical infrastructure and governments;
- The sharing of information relating to threats and vulnerabilities will assist governments, and owners and operators of critical infrastructure, in managing risk better;
- Care should be taken, when referring to national security threats to critical infrastructure, including terrorism, to avoid causing undue concern in the Australian domestic community and to potential tourists and investors overseas;
- Stronger research and analysis capabilities can ensure that risk mitigation strategies are tailored to meet Australia's unique critical infrastructure circumstances.

## CIP and Counter-Terrorism Policy

The National Counter-Terrorism Committee (NCTC) has primary responsibility for the oversight of the protection of critical infrastructures from terrorism. In general, however, CIP is a shared responsibility of the corporate sector and the Australian federal, state, and territory governments. In the field of CIIP, the Attorney-General's Department coordinates arrangements.[4]

The Australian government takes actions in the following fields:

- Identifying Australia's critical infrastructure and determining broad areas of risk;
- Assisting businesses in mitigating their risk through business-government partnerships, e.g., the Trusted Information Sharing Network (TISN) and Infrastructure Assurance Advisory Groups (IAAGs), and through state and territory governments;
- Promoting domestic and international best practices in CIP.

## e-Security

Resulting from a review of the e-Security environment, the former government released an e-Security national policy statement in 2007. The former government followed this up with funding of AUS$74 million over four years for e-Security initiatives.[5] The catalyst for this action was the increasing interconnectedness of the electronic environment and the need to address e-Security threats to different segments on the Australian economy holistically.[6] In consequence, the agenda appoints a new interdepartmental committee with responsibility across the entire range of government, the E-Security Policy and Coordination (ESPaC), to coordinate e-Security policy throughout the different areas.

[4] Commonwealth of Australia. "National Counter-Terrorism Plan". (2nd ed.), September 2005. http://www.nationalsecurity.gov.au/agd/WWW/rwpattach.nsf/VAP/(5738DF09EBC4B7EAE52BF217B46ED3DA)~NCTP_Sept_2005.pdf/$file/NCTP_Sept_2005.pdf.

[5] http://www.homelandsecurity.org.au/files/2007_e-security_agenda.pdf.

[6] Australian Government. "E-Security National Agenda 2007". http://www.dbcde.gov.au/__data/assets/pdf_file/71201/ESNA_Public_Policy_Statement.pdf.

In order to assign the roles and responsibilities of relevant Australian government agencies clearly, three priorities are defined by the agenda:

- Reducing the e-Security risk to Australian government information and communication systems;
- Reducing the e-Security risk to Australia's national critical infrastructure;
- Enhancing the protection of home users and SMEs from electronic attacks and frauds.

These new priorities and the focus on the interconnectivity of the different areas have had a considerable impact on the administrative arrangements in the field of e-Security (see chapter Organizational Overview). A second departure from the 2001 agenda is the emphasis on initiatives to address sophisticated and targeted attacks that are difficult to detect and fight by conventional measures. Thirdly, it has been decided to review the new agenda every two years instead of every four years, given the rapid evolvement of new e-Security threats.[7]

One of the major initiatives was a significant expansion of the Australian Government Computer Emergency Readiness Team[8] (GovCERT.au) within the AGD.

## Organizational Overview

In Australia, the CIP program is led by the Attorney-General's Department (AGD), in close collaboration with the owners and operators of critical infrastructures. CIP efforts are primarily coordinated through the Trusted Information Sharing Network for critical infrastructure protection (TISN),[9] which provides

[7] Athol Yates. "National Security Briefing Notes", July 2007. http://www.homelandsecurity.org.au/files/2007_e-security_agenda.pdf.

[8] http://www.tisn.gov.au/agd/WWW/rwpattach.nsf/VAP/(930C12A9101F61D43493D44C70E84EAA)~GovCERT.au+October+2007.PDF/$file/GovCERT.au+October+2007.PDF.

[9] http://www.tisn.gov.au/.

the framework for public-private collaboration in the field of CIP and CIIP (see the chapter on Organizational Overview).

The AGD collaborates also closely with other public agencies. In 2007, as a result of the budgetary announcement by the former government and the revised E-Security National Agenda, the role and responsibilities of several public agencies increased. The most important administrative change concerned the establishment of a whole of government E-Security Policy and Coordination Committee (ESPaC) in line with the push towards a holistic approach to addressing the security of the electronic environment. While the newly created ESPaC is a standing interdepartmental committee with responsibility for e-Security policy, all agencies involved in CIIP collaborate closely. For instance, the Defence Signals Directorate (DSD), the Australian Security Intelligence Organisation (ASIO), and the Australian Federal Police (AFP) are engaged in formal Joint Operating Arrangements supporting threat and vulnerability assessment and the analysis of, and the response to, critical incidents affecting the integrity of Australia's information infrastructure.

## Public Agencies

### Attorney-General's Department (AGD)

Attorney-General's Department (AGD), provides expert support to the Government in the maintenance and improvement of Australia's system of law and justice and its national security and emergency management systems. The mission of the Attorney-General's Department is achieving a just and secure society.[10]

Within the department, the Security and Critical Infrastructure Division (SCID) is responsible for the administration and development of legislation and the provision of legal and policy advice with respect to counter-terrorism, national security, telecommunications interception and critical infrastructure protection. The Division coordinates Australian Government activities in critical

[10] The Attorney-General's Department. "About the Department". http://www.ag.gov.au/www/agd/agd.nsf/Page/About_the_Department.

infrastructure protection, building on the work to protect Australia's National Information Infrastructure that began in 1999, and provides policy and legal policy advice on these issues. The division performs a leadership role in the development of a business-government partnership for critical infrastructure protection with Australian industry.[11]

## E-Security Policy and Coordination (ESPaC Committee)

The E-Security Policy and Coordination (ESPaC) Committee was established in 2007 and replaced two former committees – the Electronic Security Coordination Group (ESCG), run by the Department of Broadband, Communications and the Digital Economy, and the Information Infrastructure Protection Group, run by the AGD. The incorporation of these agencies into the new ESPaC committee "ensures effective e-security coordination across the three areas of critical infrastructure, home and SMEs, and government."[12]

The tasks of the ESPaC Committee correspond to those of its predecessors (the Electronic Security Coordination Group and the Information Infrastructure Protection Group): awareness raising, promoting e-Security skills, advancing research and development, and coordinating the government policies related to e-Security.

The ESPaC Committee is chaired by the AGD and is comprised of representatives from the following government agencies: the Australian Communications and Media Authority; the Australian Government Information Management Office; the Australian Federal Police; the Australian Security Intelligence Organization; the Department of Broadband, Communications and the Digital Economy; the Defence Signal Directorate; the Department of Defence; the Department of the Prime Minister and Cabinet; and the Office of National Assessments.

The Information Infrastructure Protection Group (IIPG) was an interdepartmental committee of the Australian government responsible for providing

[11] http://www.ag.gov.au/www/agd/agd.nsf/Page/Organisational_StructureNational_Security_and_Criminal _JusticeSecurity_and_Critical_Infrastructure.

[12] http://www.tisn.gov.au/.

policy coordination and/or technical response in relation to threats to the National Information Infrastructure (NII). It was replaced by the ESPaC.[13]

## Department of Broadband, Communications and the Digital Economy (DBCDE)

The Department of Broadband, Communications and the Digital Economy (DBCDE), formerly the Department of Communications, Information Technology and the Arts, (DCITA) participates in the Australian government's CIP activities through the Trusted Information Sharing Network (TISN). It chairs and provides secretariat support to the IT Security Expert Advisory Group (ITSEAG). The ITSEAG provides advice to the TISN on current and emerging security issues affecting owners and operators of critical infrastructure, including:

- Voice over Internet Protocol (VoIP) enterprise systems,
- Supervisory Control and Data Acquisition (SCADA) systems,
- Wireless services.

DBCDE also provides the secretariat for the Communications Sector Infrastructure Assurance Advisory Group (CSIAAG) of the TISN, which has developed an all-hazards risk management framework for the national critical communications infrastructure.[14]

## Australian Government Computer Emergency Readiness Team (GovCERT.au)

GovCERT.au was established in 2005 within the Attorney-General's Department to enhance Australia's preparedness with regard to attacks on information security. GovCERT.au is responsible for:

[13] "E-Security National Agenda 2007", op. cit., p.1.

[14] http://www.dbcde.gov.au/communications_for_business/security/critical_infrastructure_security.

- Liaising with the Computer Emergency Response Teams of foreign governments;
- Coordinating enquiries from foreign governments about cyber-security issues that affect Australia's critical infrastructure and business sector;
- Coordinating the Australian government's policy on how to prepare for, respond to, and recover from computer emergencies affecting the national information infrastructure;
- Managing the Australian government's Computer Network Vulnerability Assessment Program,[15] which provides cash grants to critical infrastructure owners and operators to undertake security assessments of their IT systems and networks, including physical and personnel security aspects relating to those networks.

GovCERT.au is the Australian government's point of contact for foreign governments on Computer Emergency Response issues affecting the national information infrastructure.

GovCERT.au receives information about IT security issues from foreign governments that needs to be passed on to Australian critical infrastructure owners and operators. GovCERT.au does not handle day-to-day computer incidents.[16]

## Australian Government Information Management Office (AGIMO)

The Australian Government Information Management Office (AGIMO), part of the Department of Finance and Administration, provides strategic advice, activities, and representation relating to the application of ICT to government administration, information, and services.

AGIMO's functions and responsibilities include:

[15] http://www.tisn.gov.au/agd/WWW/tisnhome.nsf/Page/CIP_Projects#section2.

[16] http://www.ag.gov.au/govcert.

- Promoting improved government services through technical interoperability and the integration of business processes across Australian government services and with state/territory and local authorities;
- Developing and enhancing government e-procurement processes;
- Promoting comprehensive telecommunications arrangements for the entire government;
- Identifying and promoting the development of the ICT infrastructure necessary to implement emerging strategies for the entire government;
- Developing an e-Government Authentication Framework to assist people in verifying electronic communications.

In cooperation with other government bodies, AGIMO manages international contacts and represents Australia in world forums on ICT-related issues. AGIMO also manages the .gov.au domain in consultation with state and territory governments.[17]

## Defence Signals Directorate (DSD)

The Defence Signals Directorate (DSD) is Australia's national authority on information security and signals intelligence. DSD plays an integral role in the protection of Australia's official communications and information systems. It does so by providing expert assistance to Australian agencies in relation to cryptography, network security, and the development of guidelines and policies on information security.

The activities of the DSD's Information Security Group (INFOSEC) include information and incident collection, analysis and warning services, setting awareness and certification standards, and defensive measures, including protective security measures, response arrangements, and contingency planning. In addition to its support for Australian government departments and authorities, INFOSEC

[17] http://www.agimo.gov.au.

also plays an important role working with industry towards the development of new cryptographic products.[18]

## Australian Security Intelligence Organisation (ASIO)

The Australian Security Intelligence Organisation (ASIO) is Australia's national security service. Its functions are set out in the Australian Security Intelligence Organisation Act 1979 (the ASIO Act). ASIO's main role is to gather information and produce intelligence that will enable it to warn the government about activities or situations that might endanger Australia's national security. The ASIO Act defines security as the protection of Australia and its people from espionage, sabotage, politically motivated violence, the promotion of communal violence, attacks on Australia's defense system, and acts of foreign interference. Some of these terms are further defined in the ASIO Act.[19]

## The Australian Federal Police (AFP)

The introduction of the Cybercrime Act (2001) prompted the Australian Federal Police (AFP) to join forces with state and territory police to create a national organization to address the threat of cyber-crime. The distinction between cyber-crime and cyber-terrorism is blurred because many of the tools and techniques are common to both activities. Consequently, the creation of the Australian High Tech Crime Centre (AHTCC) was a major and important CIIP measure. The AHTCC provides a national coordinated approach to dealing with instances of high-tech crime affecting the Australian jurisdiction, including the investigation of electronic attacks against the National Information Infrastructure.[20]

[18] http://www.dsd.gov.au.
[19] http://www.asio.gov.au.
[20] http://www.ahtcc.gov.au.

## Public-Private Partnerships

### The Trusted Information Sharing Network for Critical Infrastructure Protection (TISN)

Because the vast majority of the critical infrastructure is owned or operated on a commercial basis, public-private collaboration is a key component of CIIP. The Attorney-General's Department writes: "As with most businesses, those who own or run critical infrastructure know the best way to protect it, how to manage an incident and how to get things up and running again. While the Government believes that regulations are not the best way to protect all types of critical infrastructure in some areas regulations are needed for special reasons. For example, in the transport industry regulations are needed so Australia can meet international obligations."[21] The Trusted Information Sharing Network for Critical Infrastructure Protection (TISN) is the most important initiative to encourage the cooperation between the private and the public actors.

Building on the recommendations of the first Consultative Industry Forum (CIF),[22] the former government announced the formation of the Business-Government Task Force on Critical Infrastructure. The task force recommended replacing the CIF with a "learning network" to share information about critical infrastructure protection. In 2002, the government announced the creation of a Trusted Information-Sharing Network for Critical Infrastructure Protection (TISN).[23]

The TISN is organized according to Australia's critical infrastructure sectors. Each of the sector groups, the so-called Infrastructure Assurance Advisory Groups (IAAGs), is chaired by a representative of the critical infrastructure from that sector[24]. Membership is restricted to owners and operators of CI and government. Logistical support for the group is provided by government agencies that deal with the sector on a day to day basis, e.g., the Health Department

[21] http://www.ag.gov.au/www/agd/agd.nsf/Page/Nationalsecurity_CriticalInfrastructureProtection.

[22] This Forum resulted from the government's first report in the CIIP field, NII Report 1998, op. cit.

[23] http://www.cript.gov.au.

[24] http://www.tisn.gov.au.

with the Health group. The Attorney-General's Department provides support to Emergency Services, Banking, and Mass Gatherings. Each sector group is represented by their chair at the Critical Infrastructure Advisory Council (CIAC). The CIAC reports to the attorney-general. It is a way for critical infrastructure owners and operators to communicate with the Australian government at a high level. It also feeds into Australia's counter-terrorism arrangements.

Two permanent Expert Advisory Groups have been set up to advise the Critical Infrastructure Advisory Council – one for IT Security and the other for Critical Infrastructure Protection Futures.[25]

## Early Warning and Public Outreach

There are two key organizations that provide comprehensive early-warning services for cyber-attacks in Australia. The Defence Signals Directorate (DSD) has the remit to assist federal and state/territory IT networks, and the Australian Computer Emergency Response Team (AusCERT) provides some similar services to private sector operators of CI. In addition, the Australian government has launched the OnSecure website, run by the DSD.

### Information Security Incident Detection Reporting and Analysis Scheme (ISIDRAS)

The DSD manages the Information Security Incident Detection Reporting and Analysis Scheme (ISIDRAS). The function of the ISIDRAS is the collection of information on security incidents that affect the security or operability of government computer and communication systems.

The ISIDRAS facilitates high-level analysis of information security incidents with the aim of improving knowledge of both threats and vulnerabilities to Australian government information systems and about how to protect these

[25] http://www.tisn.gov.au/agd/WWW/rwpattach.nsf/VAP/(930C12A9101F61D43493D44C70E84EAA)~TISN+diagram+v.2+Dec+07.pdf/$file/TISN+diagram+v.2+Dec+07.pdf.

systems more effectively. ISIDRAS provides regular reporting of incidents. Government agencies that have detected a security breach can report the incident by completing an Australian Government IT Security Incident Reporting Form or via the OnSecure Website (which is a joint initiative between the Defence Signal Directorate and the Australian government Information Management Office to assist government agencies in dealing with information security breaches).[26] Information derived from these reports is used as a basis for threat assessments and security advice.

## Australian Computer Emergency Response Team (AusCERT)

The Australian Computer Emergency Response Team (AusCERT) is an independent non-profit organization located at the University of Queensland. It provides an important information security service to the private sector and to some government agencies on a fee-for-service basis. AusCERT's aims are to reduce the probability of successful attacks, to reduce the direct costs of security to organizations, and to lower the risk of consequential damage.[27] In May 2003, the Australian government announced the launch of AusCERT's National Information Technology Alert Service (NITAS),[28] which is sponsored by the federal government. NITAS provides a free service to subscribers, most of whom are owners and operators of the NII.[29]

[26] http://www.onsecure.gov.au.

[27] http://www.auscert.org.au and "NII Report 1998", op. cit. p. 2.

[28] http://www.nationalsecurity.gov.au/www/attorneygeneralHome.nsf/0/64534A395BA69A4CA256D24007BDCA2.

[29] http://www.national.auscert.org.au.

## Law and Legislation

### Electronic Transactions Act 1999

The Electronic Transactions Act of 1999 creates a light-handed regulatory regime for using electronic communications in transactions. It facilitates electronic commerce in Australia by removing existing legal impediments under Commonwealth law that may prevent a person from using electronic communications. The act gives business and the community the option of using electronic communications when dealing with government agencies.[30]

### Cybercrime Act 2001

The Cybercrime Act of 2001 amended the Criminal Code Act 1995. It also amended the Crimes Act 1914 and the Customs Act 1901 to enhance the applicability of the existing search-and-seizure provisions relating to electronically stored data. It gives federal law enforcement agencies the authority to investigate and prosecute groups who use the internet to plan and launch cyber-attacks (such as hacking, computer virus propagation, or denial-of-service attacks) that could seriously interfere with the functioning of the government, the financial sector, and industry. The offenses and investigation powers were drafted in a manner to make them consistent with the draft of the Council of Europe's Cybercrime Convention.

The act covers:

- Unauthorized modification of data to cause impairment;
- Unauthorized impairment of electronic communication;
- Unauthorized access to, or modification of, restricted data;
- Unauthorized impairment of data stored on a computer disk, etc.;
- Possessing, producing, supplying, or obtaining data with intent to commit a computer offense;

[30] http://www.ag.gov.au/agd/WWW/securitylawHome.nsf/Page/e-commerce_Electronic_Transactions_Act_-_Advice_for_Commonwealth_Departments.

- Causing an unauthorized computer function with intent to commit a serious offense.

The offenses were drafted in a way that recognizes the inter-jurisdictional character and extend to situations where:

- The conduct occurs wholly or partly in Australia;
- The result of the conduct occurs wholly or partly in Australia; or
- The offender was an Australian citizen or Australian company.

## Security Legislation Amendment (Terrorism) Act 2002

The Security Legislation Amendment (Terrorism) Act 2002[31] amended the Criminal Code Act 1995 to:

- Create a new offense of engaging in a terrorist act and a range of related offenses;
- Modernize Australia's treason offense; and
- Create offenses relating to membership in or other specified links with a terrorist organization.

An organization can be listed in regulations if the attorney-general is satisfied that the organization is a terrorist organization and that the organization has been identified in a decision of the United Nations Security Council relating to terrorism. A court may also find that an organization is a terrorist organization.[32]

The act also specifically outlawed cyber-terrorism: "The action or threat of action which seriously interferes with, seriously disrupts, or destroys, an electronic system including, but not limited to information, telecommunications and financial systems [...]. The action is done or the threat is made with the intention of:

[31] Security Legislation Amendment (Terrorism) Act 2002, No. 65, 2002. "An Act to enhance the Commonwealth's ability to combat terrorism and treason, and for related purposes." http://scaleplus.law.gov.au/html/comact/11/6499/pdf/0652002.pdf.

[32] http://www.nationalsecurity.gov.au/agd/www/NationalSecurityHome.nsf/Page/RW-PA41035442ED47EF7 CA256D6A001215A5.

advancing a political, religious or ideological cause; and coercing, or influencing by intimidation, the government of the Commonwealth or a State, Territory or foreign country (or part of)."[33]

## Spam Act 2003

Australia's anti-spam legislation was introduced in 2003 in response to concerns about the impact of spam on the effectiveness of electronic communication and the costs imposed on end users. The Spam Act 2003[34] prohibits the sending of spam, which is defined as a commercial electronic message sent without the consent of the addressee via e-mail, short message service (SMS), multimedia message service (MMS), or instant messaging. The requirements under the Spam Act apply to all commercial electronic messages, including both bulk and individual messages. The Australian Communications and Media Authority (ACMA) has enforcement responsibility for the Spam Act.

In June 2006, the former Department of Communications, Information Technology and the Arts (now Department of Broadband, Communications and the Digital Economy) released a review of the Spam Act[35] which found that the measures in the Act had been successful in curbing spam, but that it remained a significant problem.

[33] Security Legislation Amendment (Terrorism) Act 2002, op. cit.

[34] http://www.dbcde.gov.au/__data/assets/pdf_file/0015/34431/Main_Features_of_the_spam_act.pdf.

[35] http://www.dbcde.gov.au/__data/assets/pdf_file/0008/40220/Report_on_the_Spam_Act_2003 _Review- June_2006.pdf.

# Austria

## Critical Sectors

Contemporary sources of dangers and risks to the state, the society, and the individual may be found in the fields of politics, the economy, the military, society, the environment, culture and religion, and information technology (IT). Information and communication technology has acquired a dimension of its own in security policy because it links all other security aspects, thus becoming a power factor in its own right and leaving room for many options. Austria as a modern society and as a small state is particularly vulnerable in the area of information. This includes both the military and the civilian sectors, and increasingly business and industry as well.[1]

Accordingly, Critical Information Infrastructure Protection is of crucial importance for Austria. Responding to a parliamentary inquiry,[2] the Austrian federal chancellor defined critical infrastructures as "natural resources; services; information technology facilities; networks; and other assets which, if disrupted

[*] The Country Survey of Austria 2008 was reviewed by Dr. Otto Hellwig, TU Graz.

[1] Resolution by the Austrian parliament. "Security and Defense Doctrine: Analysis" – Draft expert report of 23 January 2001. http://www.austria.gv.at/2004/4/18/doktrin_e.pdf.

[2] http://www.parlament.gv.at/pls/portal/docs/page/PG/DE/XXII/J/J_04641/imfname_067709.pdf.

or destroyed would have serious impact on the health, safety, or economic well-being of the citizens or the effective functioning of the Government."[3] This definition conforms to the definition elaborated by the EU (see chapter on the EU in this book).

The same inquiry also raised the question of whether there was a list of critical infrastructures in Austria.[4] In its answer, the Ministry of Internal Affairs clarified that there is a list of civilian objects worthy of protection, but they are not explicitly denoted as critical infrastructure. However, it can be assumed that Critical Infrastructure Protection in Austria manly refers mainly to these objects. The list of civilian objects worthy of protection includes about 180 items, which are categorized in the following classes:

- Institutions of the legislative, executive, and judiciary powers,
- Infrastructure facilities of energy supply companies,
- Information and communication Technologies,
- Infrastructure facilities that ensure the provision of vital goods,
- Transport and traffic infrastructures.

## Past and Present Initiatives and Policies

Following the Security and Defense Doctrine of 2001, which can be considered to be the guideline for Austria's security and defense policy, security in all its dimensions is the basic prerequisite for the existence and functioning of a democracy as well as for the economic welfare of the community and its citizens. Therefore, security must be conceived and implemented within a comprehensive security policy.

There have been several organizational and procedural efforts since the 1990s to manage CIP/CIIP in Austria. The issue of CIIP has been addressed by the government, especially by the Ministry of Internal Affairs; the Ministry of

[3] http://www.parlament.gv.at/pls/portal/docs/page/PG/DE/XXII/AB/AB_04595/imfname_069768.pdf.

[4] Ibid.

Defense; the Ministry of Traffic, Innovation, and Technology; and the Federal Chancellery, which has taken the leadership and is the central point in different projects.

On the European level, Austria takes part in all relevant EU activities regarding the protection of critical infrastructures, such as the European Program for the Protection of Critical Infrastructure (EPCIP) and the Critical Infrastructure Warning Information Network (EUCIWIN). Austria, like most other EU member states, shares the opinion that the protection of critical infrastructures has to follow the principle of subsidiarity, which means that the protection of the critical infrastructure is primarily the task of the member states. Activities of the EU are seen as complementary measures.

## Security and Defense Doctrine 2001

According to the principle of comprehensive security, the Security and Defense Doctrine[5] recommends the development of the existing Comprehensive National Defense Program into a system of Comprehensive Security Provision by focusing on the new risks and threats and by amending legal provisions.[6] One can therefore deduce that this will also include all measures referring to CIIP.[7] This doctrine clearly stresses that for small states, full and unimpaired access to the information they require is a basis for their freedom of action in security matters.[8]

[5] http://www.bundeskanzleramt.at/2004/4/18/doktrin_e.pdf.

[6] Security and Defense Doctrine, op. cit.

[7] The concept of "Comprehensive National Defense" as developed from 1961 onwards was embedded in the Constitution in 1975. Under Article 9a of the Austrian Constitution, the role of Comprehensive National Defense is to "maintain [Austria's] independence from external influence as well as the inviolability and unity of its territory, especially to maintain and defend permanent neutrality". Together with the constitutional amendment, the Austrian parliament unanimously adopted a resolution in 1975 "on the fundamental formulation of Comprehensive National Defense in Austria" (defense doctrine). These were the foundations of the national defense plan, which was adopted by the Austrian government in 1983 and identified the "protection of the country's population and fundamental values from all threats" as a basic goal of Austrian security policy.

[8] Security and Defense Doctrine, op. cit.

The implementation of Austria's security policy within the framework of the Comprehensive Security Provision relies on systematic co-operation among various policy areas on the basis of appropriate sub-strategies.

## IT Strategy and the "Platform Digital Austria"

The IT strategy of the government was formulated in July 2001, based on a decision of the Council of Ministers of 6 June 2001 referring to the New Structuring of the IT Strategy of the Government. The strategy consisted of the following three service types: Administration and Public Relations, Techniques and Standards, and Project Management and International Affairs. A special body, the ICT Board, was established to guarantee strategic co-ordination of ICT within the framework of the public government. This board was composed of the chief information officers of all the Federal Ministries and was located at the Federal Chancellery. It was responsible for coordinating the IT activities with each ministry, the local authorities, and the municipalities.

In 2005, the strategy was restructured. The basic elements of the 2001 strategy were retained, and the existing organizations were consolidated. However, in order to ensure sustainability, the ICT Board and the E-Cooperation board (the body responsible for coordination of e-government) were summarized in one unit, the ICT-Strategy Unit of the federal government.[9] This group forms the central unit of the new "Platform Digital Austria", where all IT and e-government efforts are coordinated. The ICT-Strategy Unit is responsible for public relations; the ICT budget, controlling, and sourcing; law, organization, and international activities; program and project management; and technical infrastructure.

## Citizen Card and e-government

The Austrian Citizen Card Concept does not define a single citizen card for electronic identification, but only specifies the minimum technical requirements in a neutral way. Because of the open, technologically neutral approach, a variety

[9] Digital Austria. "Administration on the Net: An ABC Guide for E-Government in Austria", p. 28. http://www.digitales.oesterreich.gv.at/DocView.axd?CobId=19394.

of entities can issue citizen cards. These include both public bodies (including federal ministries and universities) and private bodies (certification authorities, banks) and can even involve other technologies such as mobile phone signatures.[10] In order to make use of the possibilities offered by electronic identification, citizens need to register their card as citizen card, download software, and buy a reader for the chip. After this registration process, they can use their card for e-identification and for electronic signatures. Different governmental services can be accessed by using the citizen card, and the e-government activities will be extended continuously.[11]

## Zentrales Ausweichsystem (ZAS)

After a fire at the Austrian Central Bank at the end of the 1970s, the government decided to establish an alternative replacement system for the data stock of the government. This system is located in the so-called Einsatzzentrale Basisraum (EZB) in St. Johann/Salzburg. Due to its coordinative function in the procurement of IT technologies, the Federal Chancellery has been responsible for the development of the EZB.[12]

The Zentrale Ausweichsystem (ZAS) has been a central part of the governmental crisis prevention system since the 1980s and has been fully operational on a day-to-day basis ever since. Some fundamental and very important systems (like the law information system/RIS) are run by this system. In addition, the ZAS serves as an archive for important backup data, such as the data from the public record office and from the Schengen Information System.[13]

[10] http://www.buergerkarte.at.

[11] http://www.help.gv.at/sigliste/sig_bund.jsp?cmsid=281.

[12] The ZAS is located on an installation of the Austrian military; therefore, not much is publicly known about the institution itself.

[13] Cf. Der Standard, "Österreichs Hochsicherheits-Datenspeicher wird 25 Jahre alt" (15 September 2007).

### Austrian Information Security Handbook

By order of the Federal Chancellery, the Center for Secure Information Technology Austria (A-sit, see below) publishes the Austrian Information Security Handbook (known until 2005 as the IT-Security Handbook). This handbook gives an overview of IT security in general and informs readers in a broad and comprehensive way about fundamental aspects and measures in the field of IT. The handbook was updated in 2003, 2004, and 2007 based on the idea that security is a continuous process. It consists of two parts: "IT Security Management", which offers concrete instructions in this field; and "IT Security Measures", which describes standard security measures for IT systems requiring a medium security level.[14]

### Official Austrian Data Security Website

The Official Austrian Data Security Website,[15] which is coordinated by the Federal Chancellery, serves as an information desk for citizens in important matters such as data security, the Schengen Information System, Europol, etc. It also informs the public about the work of the Commission on Data Protection, whose reports are available on the website. It also serves as a complaint board for citizens who want to report violations of their data privacy.

## Organizational Overview

At the public level, no single central authority is responsible for CII/CIIP, which is considered to be a cross-agency task. However, the Federal Chancellery fulfils a coordinating task. CIIP is mainly addressed by the Ministry of Internal Affairs, the Ministry of Defense, and the Ministry of Traffic, Innovation, and Technology. In addition, the Center for Secure Information Technology Austria (A-SIT)

[14] The complete handbook is available at http://www.a-sit.at/pdfs/OE-SIHA_I_II_V2-3_2007-05-23.pdf.

[15] http://www.dsk.gv.at/indexe.htm.

and the Stopline.at – Initiative, both organized as public-private partnerships perform important tasks in the field of CIIP.

## Public Agencies

### Ministry of Internal Affairs (BMI)

Several divisions of the Ministry of Internal Affairs (BMI) deal with CIIP, especially with aspects of data security and cyber-crime. For example, the head office for the public safety at the Federal Crime Police Office operates a reporting center for child pornography.[16]

Another important agency belonging to the BMI is the Federal Agency for State Protection and Counter-Terrorism (BVT), which is responsible for the coordination of personal security and the security of installations. In addition, it evaluates and develops the ability to provide protection on a permanent basis with regard to possible new threat scenarios.

The BMI also serves as the point of contact for European Processes concerning Critical Infrastructure Protection.

### Ministry of Defense

In the framework of the Ministry of Defense, Department II (also known as the "control department") is responsible for all aspects of information warfare. It fulfills its duties in close cooperation with the Leadership Support Command[17] and the two military intelligence services.[18] One of these, the Abwehramt, which is responsible for the protection of the armed forces, also has a special department called Electronic Defense.[19]

[16] http://www.bmi.gv.at/kriminalpolizei.

[17] The Austrian armed forces and the Ministry of Defense are currently undergoing reform, so that a change in responsibilities is possible.

[18] "Heeresnachrichtenamt" and "Heeresabwehramt".

[19] The chief of this department, Colonel Walter J. Unger, published several articles concerning IT security and cyberterrorism. See e.g.: Walter J. Unger and Heinz Vetschera, "Cyber War und Cyber Terrorismus als neue Formen des Krieges". In: Österreichische Militärische Zeitschrift, No. 2/ 2005; pp. 203–11; Walter J. Unger. "Angriff aus dem Cyberspace I-III". In: Truppendienst No. 2/ 2004; pp. 143–7; No. 3/ 2004; pp. 271–5; No. 4/2004; pp. 382–6.

The Austrian Federal Constitution and the Defense Law determine the cooperation between the army and civil authorities in crisis situations if the latter are not able to guarantee the maintenance of public order and inner security themselves. Part of this is the protection of civilian installations against interference by unauthorized third parties, including the protection of critical information infrastructures.

The final report of the Politico-Military Commission,[20] which was released in autumn 2004, recommends that the Austrian armed forces be given an important role in the protection of the vital, civilian ICT, as well as the capacity to provide redundant systems in case of catastrophes or threats.[21]

These protective measures have been tested in several exercises held in close co-operation with the civilian institutions. The largest maneuver of this kind in Austria took place in the federal states of Carinthia and Styria from 13–16 April 2004. The Schutz 2004 maneuver was planned and executed as a security assistance mission under the leadership of the civil authorities.

## Ministry for Traffic, Innovation, and Technology (BMVIT)

The Ministry for Traffic, Innovation, and Technology (BMVIT) is responsible for the safety of the public critical infrastructure. It operates a coordinating center for private owners and operators of critical infrastructure, and a center for security research. One of its recent activities has been to order an ICT master plan that would analyze the strengths and weaknesses and the state of the art of Austria's critical infrastructure. Another part of this mandate consisted in presenting options for measures, targets, missions, and visions.[22] The BMVIT also coordinates the Austrian Security Research Program, in which critical infrastructure protection will play an essential part.[23]

[20] Bundesheerreformkommission. http://www.bmlv.gv.at/facts/bh_2010/archiv/pdf/endbericht_bhrk.pdf.

[21] Bundesheerreformkommission. "Endbericht 2004", pp.49f.

[22] http://www.bmvit.gv.at.

[23] http://www.kiras.at/wDeutsch/index.php and http://www.bmvit.gv.at/innovation/sicherheits forschung/index.html.

### Commission on Data Protection (DSK)

The Commission on Data Protection (DSK) serves as independent control authority that deals with data processing in the public and private sectors.[24] The DSK is located at the Federal Chancellery. All citizens have the right to appeal to this commission if their rights in the field of data security are violated. The commission verifies these claims and takes measures to remedy confirmed violations. The Council on Data Protection has exclusive consultative agendas and periodically publishes the Report on Data Security.

## Public-Private Partnerships

### Center for Secure Information Technology Austria (A-SIT)

The Center for Secure Information Technology Austria (A-SIT) was founded in May 1999 as an association supported by the Austrian National Bank, the Ministry of Finance, and the University of Technology in Graz. Its tasks include general monitoring issues of IT security[25] and the evaluation of encryption procedures,[26] as well as supporting the introduction of the Citizen Card, supporting public institutions, and developing a security policy for all important electronic payment systems for the Austrian National Bank. It is also a member of the Computer Incident Response Coordination Austria (CIRCA).

### Stopline.at

Stopline.at is an online center that can be addressed by all internet users – also anonymously if they wish – who come across child pornography or right-wing extremist content on the internet. The relevant laws describing the respective crimes are §207a StGB (Austrian penal code) regarding child pornography, and the Austrian National Socialist prohibition law and the law against displaying

[24] For more information, see: http://www.dsk.gv.at/indexe.htm.

[25] A-SIT offers tools and demonstration examples on its homepage: http://demo.a-sit.at.

[26] http://www.a-sit.at/asit/asit.htm.

National Socialist regalia as well as symbols of right-wing radicalism, respectively.

Stopline.at was founded as a private initiative by the Austrian internet service providers and has become reporting office that is authorized and accepted by the public authorities. Stopline.at cooperates closely with the Federal Ministry of the Interior (Federal Office of Criminal Investigation and Federal Office for the Protection of the Constitution and Counter-Terrorism).

## Early Warning and Public Outreach

### Computer Incident Response Coordination Austria (CIRCA)

The Computer Incident Response Coordination Austria (CIRCA) is Austria's main organization in the field of IT early-warning systems. It is a public-private partnership whose main actors are the Federal Chancellery, the Federation of the Austrian Internet Service Providers (ISPA), and A-SIT. Other members are representatives of the social partners (economic interest groups), the federal states, and of other critical infrastructure providers. It is a web of trust between Internet Service Providers (ISPs), IP network operators from the public and private sectors, and enterprises in the field of IT security. The electronic communication network of the private sector is run by ISPA, whereas the Federal Chancellery has the lead in the public sector.

The aim of this Austrian security net is to provide an early-warning system against worms, viruses, distributed denial-of-service attacks, and other threats that endanger IP networks and their users. Therefore, CIRCA issues alerts and risk assessments and provides information about precautionary measures. Its strategy is both proactive and reactive, and involves a continuous exchange of information and news between the Federal Chancellery and CIRCA.[27]

[27] http://www.circa.at.

## Computer Emergency Response Team (CERT.at)

In March 2008, the Austrian domain registry nic.at launched the Austrian Computer Emergency Response Team (CERT.at).[28] The purpose of the CERT is to coordinate security efforts and incident response for IT security problems on a national level in Austria. The level of support given by CERT.at varies depending on the type and severity of the incident or issue, the type of constituent, the size of the user community affected, and CERT.at's resources at the time. Special attention is given to issues affecting critical infrastructure. In addition, the CERT also releases educational material for SMEs and the general public.

The CERT.at cooperates with local and international CERTs as well as with other information security teams. It therefore shares information about incidents and security breaches with its partners. Nevertheless, it strictly protects the privacy of its customers.

## Law and Legislation

There is a broad variety of legal acts and laws dealing with CII/CIIP in a very broad sense. Most of them refer to the processing, collection, transfer, and protection of (personal) data through or by public agencies (e.g. the police and security agencies).

The general responsibilities of governmental authorities are laid out in the Bundesministeriengesetz (Federal Ministry Law), which defines the agendas of each ministry.

The following can be regarded as the central and most relevant legislative acts:

[28] http://www.cert.at/english/missionstatement/content.html.

## Information Security Law and Information Security Order

With the Information Security Law[29] and the Information Security Order,[30] Austria guarantees the secure use of classified information within the jurisdiction of the federal government according to international law. They regulate the access, transmission, identification, electronic processing, registration, and preservation of classified information. In accordance with international law, information regarding security arrangements within the EU or with other states qualifies as classified information. The Information Security Law specifies four types of classified information:

- Limited: if the unauthorized transmission of information would be contrary to the interests mentioned in Article 20, paragraph 3 of the Federal Constitution;
- Confidential: If the information has to be kept secret according to additional federal laws and if maintaining secrecy is in the public interest;
- Restricted: If the information is confidential and its publication would harm the interests mentioned in Article 20, paragraph 3 of the Federal Constitution;
- Top Secret: If the information is secret and its publication could seriously damage the interests mentioned in Article 20, paragraph 3 of the Federal Constitution.

Consequently, every type of classification corresponds to a certain security infrastructure (building, organizational structures, and personnel).

The Data Security Law therefore only grants access to Confidential, Restricted, and Top Secret information to individuals who have completed an advanced security examination according to paragraphs 55 to 55b of the Security Police Act. In the civilian sphere, this security examination is conducted by the Federal Office for Constitutional Protection and Counter-Terrorism.

[29] BGBl I Nr. 23/2002.

[30] BGBl II Nr. 548/2003.

## Data Security Law 2000

The Data Security Law (DSG)[31] contains extensive regulations on the processing of personal data. With this law, Austria adopted the EU guideline for data security of the year 1995. The DSG 2000 stresses the importance of data-security measures and measures to enhance confidentiality for personal data. As a rule, the user of personal data is responsible for ensuring that the information is used in a correct manner, that no unauthorized persons have access to data, that the data is not destroyed, and that its secure storage is guaranteed. The DSG lists the following as civil rights:

- The fundamental right to a secure processing of personal data,
- the right of information;
- the right to have incorrect or wrong data corrected,
- and the right to have data deleted.

Another important part of the DSG's activities is the duty to report. This means that with certain exceptions (e.g., for reasons of national security), all applications for personal data must be reported. Additionally, the Data Security Website contains all necessary information, forms, and addresses for rapid reporting.

## Security Police Law

The Security Police Law (SPG)[32] defines the duties and authority of the civilian security services. Several articles and/or sections refer to the collection, transfer, storage, and deletion of personal data,[33] as well as measures to prevent the unauthorized use of data. It also provides special rights for individuals whose privacy has been violated by the security services.[34]

[31] BGBl 165/99; see the explanations given by the Ministry of Internal Affairs. http://www.bmi.gv.at.

[32] BGBl 566/91 idF BGBl 85/2000.

[33] Cf. especially section 4 of the law, "Verwenden personenbezogener Daten im Rahmen der Sicherheitspolizei".

[34] Cf. especially section 6 of the law, "Besonderer Rechtsschutz".

Together with this law, the office of a “legal protection agent”[35] was established as a controlling institution. The main duty of the legal protection agent is to protect the rights of citizens by ensuring that investigations of threats as well as observation and surveillance stay within legal rules.

## Military Competence Law

In analogy to the Security Police Law, the Military Competence Law (MBG)[36] regulates the tasks and duties of the Austrian armed forces, including the two military intelligence services.[37] The MBG regulates the collection, transfer, and deletion of personal data. Paragraph 55 regulates the rights of citizens in cases where data security measures have been disregarded. The MBG also provides for the establishment of the institution of a “legal protection agent” who monitors the legality of measures undertaken by the intelligence services.[38]

## Telecommunication Law

The Telecommunication Law[39] (TKG) includes extensive and detailed regulations referring to data security in general, and specific regulations regarding communication exchange. Furthermore, these regulations stipulate confidentiality of telecommunication.[40] The law also states that the suppliers of communication lines are responsible for securing all data. Paragraph 89 obliges the suppliers of communication lines to place all technical means necessary for the surveillance of telecommunication at the disposal of the security agencies.

[35] “Rechtsschutzbeauftragter” (ombudsman in charge of protecting the rights of citizens).

[36] BGBl 86/2000.

[37] Second Section of the Law on Intelligence Services.

[38] Paragraph 57 of the law.

[39] Telekommunikationsgesetz, BGBl 100/1997 idF BGBl 134/2002.

[40] Fernmeldegeheimnis, Datenschutz. Chapter 12, paragraphs 87–101.

## Penal Code (StGB)

Several articles of the Austrian Penal Code (StGB) refer to CII/CIIP. Some new regulations were introduced to the Penal Code in 2002:[41]

Paragraph 118a: Unlawfully accessing a computer system: This crime is punishable with a prison sentence up to six months or a fine. The law applies not only to illegal access, but also to unauthorized registration on a computer system or to those who offer these possibilities to another person, make them public, or use them to gain benefit. The law also applies to cases where users who are authorized to use part of the system have accessed other parts that are off-limits to them. But an essential element is that a violation of security measures has to have occurred. Thus, if no security measures are in place, unauthorized access is not a crime. It is worth mentioning that the perpetrator will only be prosecuted with authorization from the injured party.

Paragraph 119: Infraction of the confidentiality of telecommunications: This crime is defined in a similar way to violations of the privacy of correspondence. The punishments and the requirement for the prosecution are the same as in paragraph 118a.

Paragraph 119a: Improper interception of data: This constitutes a crime that is punished and prosecuted. It is essential that the intercepted data not be intended for the intercepting person. It does not matter whether the perpetrators intend to use the data for themselves, to make it public, or to offer it to another party. The law makes no distinction between the methods applied.

Paragraph 126b: Disruption of the operability of computer systems: The elements of the crime of "Disruption of the operability of computer systems" are directly connected with paragraph 126a. The law outlaws the disruption of systems by introducing or sending data. The authorization of the injured party is not needed for prosecution, because this law applies to the diffusion of viruses, worms, etc.

Paragraph 126c: Abuse of computer programs or access data: This article is a very complex one. It prohibits the abuse of computer programs or access data, such as passwords. It is generally intended to cover Trojans and spy programs, as

[41] http://www.cybercrimelaw.net/countries/austria.html.

well as accessing and distributing passwords and access codes for various purposes. However, the maximum punishment is not higher than in the other articles.

## Penal Procedure (StPO)

The Penal Procedure (StPO) regulates the special investigation methods for combating organized crime. These methods are provisions for optical and acoustic surveillance by civilian security institutions. The law also regulates the installation of a legal protection agent who monitors the legality of the special investigation methods. According to the StPO, the Minister of Justice is obliged to report annually on the use of special investigation methods to the Council for Data Protection (DSR),[42] the Commission on Data Protection (DSK), and the Austrian parliament.[43]

In 2004, Austria introduced the European arrest warrant into its Penal Procedure System. It is an EU regulation that simplifies the extradition of persons for trial or for the enforcement of sentences. It comprises a catalog of 32 crimes where no close examination is required for extradition. A major problem is that these 32 offenses are not defined properly. One of these crimes is “cyber-crime”, which has given rise to a lot of controversy, because each of the 25 member states may define it in a different way. In the Austrian penal code, for example, there is no such offence as “cyber-crime”.

## Electronic Signature Law (SigG)

Since 1999, the Electronic Signature Law (SigG)[44] has regulated the admission of electronic signatures in the Austrian legal system. The controlling board is the Austrian Telecom Control Commission, which gives the suppliers the necessary

[42] The Council for Data Protection (Datenschutzrat, DSK) is a consultative body, which advises the government in questions concerning data protection. http://e-campus.uibk.ac.at/planet-et-fix/M6/3_Datenschutzrecht/3_Institutionen/K633_20datenschutzrat.htm.

[43] Cf. Bundesministerium für Justiz. “Gesamtbericht über den Einsatz besonderer Ermittlungsmethoden im Jahr 2001” (Vienna 2002).

[44] Signaturgesetz BGBl 1999/190.

certificates. It also informs its constituency about security measures related to electronic signatures.[45] Since 24 September 2002, it has been fully operational with the Public-Key-Infrastructure (PKI).

[45] http://www.signatur.rtr.at.

# Brazil

## Critical Sectors

Broadly defined, the Brazilian critical infrastructures include the areas of oil, electric energy, and telecommunications.[1] More specifically, the SecGov 2006 conference[2] held in Brasilia in November 2006 and sponsored by the Institutional Security Cabinet (Gabinete de Segurança Institucional – GSI) had the goal of discussing topics and questions on Critical Infrastructure Security in Brazil, Information and Communication Security and Terrorism. Eight discussion panels took place on the following topics:

- Public Safety,
- Energy,

[*] The Country Survey of Brazil 2008 was reviewed by Mariana Balboni, Brazilian Internet Steering Committee; Regina Maria De Felice Souza, Agência Nacional de Telecomunicações – Presidency; and João Henrique de A. Franco and Sérgio Luis Ribeiro, CPqD Telecom & IT Solutions

[1] Claudio Pinhanez. "Internet in Developing Countries: The Case of Brazil". http://www.research.ibm.com/people/p/pinhanez/publications/netbrasil.htm.

[2] http://www.secgov.com.br.

- Finance,
- Transport Systems,
- Water Supply,
- Public Health,
- Telecommunications,
- Terrorism.

Although the Brazilian government has not formally defined what the critical infrastructures are, at least the first seven topics are unofficially considered to represent critical sectors.[3]

As regards critical *information* infrastructure, the focus lies on telecommunications and the internet. Based on the understanding that critical infrastructure protection on a nationwide level has consequences that can impact a nation socially, politically, and economically, a new approach was developed and proposed specifically by the federal telecommunications regulatory body, Anatel (see the chapter on Organizational Overview), to be applied to the telecommunications infrastructure, in order to understand the related risks and to develop a suitable program based on four main points: contextualization, a protection strategy, a set of methodologies, and software tools to support them. These methodologies include the development of tools for identifying critical (information and communication) infrastructures and the potential threat landscape, for scenario creation, and for diagnosing.[4] Moreover, information security is no longer understood as an exclusive problem of the sectors related to IT, or even of a particular organization, industry, or government; it is understood instead as consisting of regional and global strategies that facilitate an organized response to the threats and vulnerabilities associated with technology use.[5]

[3] Information provided by an expert.

[4] Regina Maria De Felice Souza. “Critical telecommunication infrastructure project”. In: InfoCitel Electronic Bulletin no. 33, March 2007. http://www.citel.oas.org/newsletter/2007/marzo/infraestructura_i.asp

[5] 2nd COLAIS. “2nd Latin American Conference for Security Incident Response”. Rio de Janeiro, 6–12 October 2006. http://www.rnp.br/en/events/colaris/.

## Past and Present Initiatives and Policies

As mentioned above, Brazilian policies for information infrastructure protection focus on two particular aspects: the internet and telecommunications. Both of these, it is argued, play an important role in social (and digital) inclusion and are essential for national cohesion. The policies adopted in order to create trust in critical network infrastructures[6] show that the two sectors cannot be separated, since the interests of telecom and internet providers in operating secure networks are clearly inter-related, and the latter depend almost entirely on the former for backbone infrastructure and access networks. The Brazilian government has initiated several initiatives in association with internet diffusion, network protection, and communications security.

### Brazilian Internet Steering Committee (CGI)

The initiatives of internet governance are mainly conducted under the auspices of the Brazilian Internet Steering Committee (Comitê Gestor da Internet no Brasil – CGI). This committee is a multi-stakeholder organization composed of members of government agencies, backbone operators, representatives of the internet service provider industry, users, and the academic community, and was jointly created in 1995 by the Ministry of Communications and the Ministry of Science and Technology.[7] The committee's main tasks are:

- To propose policies and procedures related to the regulation of internet activities;
- To recommend standards for technical and operational procedures for the internet in Brazil;

[6] Robert Shaw. "Creating Trust in Critical Network Infrastructures: The Case of Brazil". ITU Workshop on Creating Trust in Critical Network Infrastructures, Seoul, Republic of Korea, 20–22 May, 2002.

[7] The Brazilian Internet Steering Committee was created by interministerial ordinance no. 147 of 31 May 1995 and altered by presidential decree no. 4829 of 3 September 2003. Since July of 2004, the representatives of the civil society are chosen democratically to participate directly in the deliberations and to debate priorities for the internet, along with the government.

- To establish strategic directives related to the use and development of the internet in Brazil;
- To promote studies and technical standards for the network and security of services in the country;
- To coordinate the allocation of internet addresses and the registration of domain names;
- To collect, organize, and disseminate information on internet services, including indicators and statistics.

The committee maintains three working groups – on network engineering, on computer security, and on the training of human resources – in order to provide technical, administrative, and operational input for the committee's decisions and recommendations. Moreover, several projects in areas of fundamental importance for the operation and development of the internet in Brazil are coordinated. In order to execute its activities, the non-profit civil organization Brazilian Network Information Center NIC.br was created.

The Brazilian Internet Steering Committee has lately issued the second edition of its Survey on the Use of Information and Communication Technologies in Brazil – ICT Enterprises and ICT Households, reflecting the concern and the commitment of the committee in monitoring and sharing information about the evolution of the internet, which is considered an essential tool for social and economic development, as well as for the democratic participation of citizens and countries in the information society.[8]

Of particular importance are also some of the recently initiated combined actions to improve internet security, such as instruction for users. Several initiatives are undertaken by the Computer Emergency Response Team Brazil (CERT.br), which is maintained by the Internet Steering Committee. The Internet Security Best Practices[9] document has been published since 2000 in order to

[8] Brazilian Internet Steering Committee, Brazilian Network Information Center (ed.). Preface to the "Survey on the Use of Information and Communication Technologies in Brazil – ICT Households and ICT Enterprises 2006" (second edition, São Paulo, 2007). http://www.cetic.br/tic/2006/indicadores-2006.pdf.

[9] http://cartilha.cert.br (in Portugese).

help increase users' security awareness. While this document was written specifically for internet end users and has been constantly updated to reflect the evolving nature of attack and protection technologies, another document has been developed by CERT.br that is aimed specifically at companies: the Best Practices for Internet Network Administrators.[10] This document is addressed to security professionals and network professionals who do not have a dedicated security team at their disposal.[11]

## Brazilian electronic government program (e-gov)

The Brazilian government sees itself as having an important role to play both as a promoter and as a user of information and communication technologies. Therefore, the government has made the adoption of advanced information communication technologies for its administrative processes and delivery of services to its citizens a high priority. In 2000, it launched an electronic government initiative under the auspices of the Information Society Program of the Ministry of Science and Technology with three overall aims relating to the goal of digital inclusion: to universalize services, to make the government accessible to everyone, and to advance the infrastructure. A presidential decree established the Executive Committee of Electronic Government on 18 October 2000. Three years later, the presidency of Brazil published another important decree creating eight technical committees of e-government, with tasks including the implementation of free software, the advancement of digital inclusion, the integration of systems, legal systems and software licenses, the administration of websites and online services, network infrastructure, government to govern (G2G), and knowledge and strategic information management.[12] The Brazilian e-government model aims at integrating the different government organs in order to guarantee multiple channels of access for the citizens, institutions, local executives, and civil servants

[10] http://www.cert.br/docs/seg-adm-redes.

[11] Christine Hoeppers and Klus Steding-Jessen. "Information Security in Brazil". In: Brazilian Internet Steering Committee/Mariana Balboni (ed.). Survey on the Use of Information and Communication Technologies in Brazil 2005 – ICT HOUSEHOLDS and ICT ENTERPRISIS, (First Edition 2006). http://www.cetic.br/tic/2005/indicadores-2005.pdf.

[12] http://www.governoeletronico.gov.br.

through manifold devices such as the traditional office counter and telephone, but also internet and digital TV.[13] In concrete terms, the driving principles of Brazil's electronic government are defined as follows:[14]

- The priority of electronic government is to promote citizenship;
- Digital inclusion is inseparable from electronic government;
- Free software is a strategic appeal to implement electronic government;
- Knowledge management is a strategic instrument for the articulation and administration of the public policies of electronic government;
- Electronic government needs to rationalize the use of resources;
- Electronic government needs to relate to the integrated outline of policies, systems, templates, and norms;
- The activities of electronic government must be integrated with other levels of government.

## Organizational Overview

Major public efforts in Brazil concerning CIIP include the Information Security Steering Committee, the national policies for ICT under the auspices of both the Ministry of Science and Technology and the Ministry of Communication, and the Brazilian Network Information Center. Brazil has a complex and very sophisticated infrastructure of institutions involved in developing information security policy. Information security issues lie within the jurisdiction of the Institutional Security Cabinet (Gabinete de Segurança Institucional – GSI), which is an essential organ of the Presidency of the Brazilian Republic and assigned with the competence to coordinate the activities respective to information security.[15]

[13] http://portal.etsi.org/docbox/Workshop/@METIS_Kick-off/Presentations/E-gov%20interoperability%20in%20Brazil%20ePing.ppt.

[14] http://www.governoeletronico.gov.br.

[15] http://www.presidencia.gov.br/estrutura_presidencia/gsi/sobre.

The GSI's activities are defined by decree no. 5083 of 17 May 2004.[16] It does not handle security issues directly, but works through other related organizations. Under its auspices, the Information Security Committee was formed.

As public-private partnerships, Anatel (the federal telecommunications regulatory body), Serpro (the federal data processing service), and CERT.br (the Computer Emergency Response Team Brazil) strive to further and deepen the cooperation between the public and the private sectors.

## Public Agencies

### Information Security Steering Committee (CGSI)

The Brazilian Information Security Steering Committee (Comitê Gestor da Segurança Informação - CGSI) was created by decree no. 3505 on 13 June 2000.[17] It is composed by representatives from every ministry.[18] The participants discuss information security issues and define the future policy directions of the Brazilian federal administration in working groups. This committee oversees the federal government's commitment under decree no. 3505, which stipulates that there must be an information security policy for every department of the Brazilian federal government.[19] Information security is defined by the committee as including the protection of the information systems from denial of service to authorized users, and against intrusion or unauthorized modification of data and information. It is seen as broadly including the security of human resources, of documents and material, of areas and installations of communication and computing, as well as being designed to prevent, detect, deter, and document eventual threats and their development.[20]

[16] http://www.presidencia.gov.br/estrutura_presidencia/casa_civil/atos/destaque/estreg_gsi/view? searchterm=5083.

[17] http://www.planalto.gov.br/gsi/cgsi.

[18] The current list of representatives is available here: http://www.planalto.gov.br/gsi/cgsi/.

[19] Robert Bruce et al. "International Policy Framework for Protecting Critical Information Infrastructure: A discussion Paper Outlining Key Policy Issues". TNO Report 33680, Tuck School of Business at Dartmouth, Delft (30 June 2005).

[20] http://www.planalto.gov.br/gsi/cgsi.

## National Policies for ICT

The Ministry of Science and Technology maintains a program dedicated to information and communications technologies (ICT). This program formulates a national policy and addresses issues such as software, microelectronics, network services, legal questions, and digital inclusion.[21] The focus lies on the technological and developmental aspects of the information and communication technologies.

Likewise, the Ministry of Communications maintains programs addressing digital inclusion, radio-diffusion, postal services, and telecommunications. These programs all aim to democratize access to these different means of communication and information and to reduce social and regional inequalities therein.[22]

## Brazilian Network Information Center (NIC.br)

As mentioned above, the Brazilian Internet Steering Committee (CGI) was created by interministerial ordinance no. 147 of 31 May 1995 and altered by presidential decree no. 4829 of 3 September 2003. It is a public agency by nature, but its members include representatives of the private corporate and third sectors, as well as of academia. It is responsible for promoting the technical quality, innovation, and dissemination of internet governance and services, and has created the Brazilian Network Information Center (NIC.br)[23] in order to execute its activities. These activities include services – registro.br, CERT.br, and PTT.br – as well as projects such as antispam.br, statistics and indicators, and the internet security card.

This is to say that, as a set of services, the center coordinates Brazilian domain registration and IP assignments, it sponsors the CERT.br, and aims at providing the necessary infrastructure for the direct interconnection between the diverse networks that operate in the metropolitan regions (Ponto de Troca de Tráfego – PTT). Moreover, the committee's Center of Studies on Information and Communication Technologies (Centro de Estudo sobre as Tecnologias da

[21] http://www.mct.gov.br/index.php/content/view/2143.html.

[22] http://www.mc.gov.br.

[23] http://www.nic.br.

Informação e da Comunicação – CETIC.br) is responsible for the collection, analysis, and dissemination of data about the use and penetration of the internet in Brazil.[24]

The projects maintained by the Internet Steering Committee's executive branch, the Network Information Center, include, as mentioned, an anti-spam website designed to serve as an impartial and technically based source of reference concerning spam. This site represents the effort to inform both the users and network administrators about spam, its implications, and the forms of protection and combat. Furthermore, two other projects work on the statistics and indicators about Brazilian internet development and growth and on a document containing recommendations about how to navigate the internet more securely and about how individuals can protect themselves against so-called 'cyber-threats'.

## Public-Private Partnerships

### Anatel

Anatel (Agência Nacional de Telecomunicações), the federal telecommunications regulatory body modeled on the Federal Communications Commission of the US, was established with the mission of enabling a new model for Brazilian telecommunications, starting with the privatization of the Telebrás system. After privatization has been achieved between 1995 and 2003, the main role of Anatel became that of regulation, concession, and supervision of the telecommunications services in the country.[25] Among the important issues under discussion are the mechanisms for achieving cooperation between the Brazilian government and the private sector under the auspices of Anatel. Initial steps have been taken to address cyber-security issues facing the Brazilian telecom sector infrastructure through cooperation between private companies and this regulatory body.[26] Moreover, and as mentioned earlier, the methodology proposed and used by Anatel in order to identify critical infrastructure – called MI2C – was used for

[24] http://www.cetic.br.

[25] http://www.globaliswatch.org/files/pdf/GISW_Brazil.pdf.

[26] Cf. Robert Bruce et al., op. cit.

the purpose of defining the critical parts of the Brazilian telecommunications infrastructure.[27]

## SERPRO

The SERPRO (Serviço Federal de Processamento de Dados) is a private company owned by the Brazilian government with the mandate of providing networking services for information technologies to government agencies in Brazil. Serpro supports thousands of federal government IT systems and runs a large IP-based government intranet system. There are extensive physical and logical security arrangements in place. Serpro has a security committee of about 35 people who develop government system security policies. The coordinator of the committee is a member of the above- mentioned Federal Government's Security Committee (CGSI). Moreover, Serpro cooperates on security issues with the Brazilian Internet Steering Committee and its Computer Emergency Response Team.[28] Serpro maintains different programs grouped under the three labels of governmental, entrepreneurial, and citizenship matters, which are closely linked to the Brazilian e-government program.

## CERT.br partnerships

The Computer Emergency Response Team Brazil, maintained by the Internet Steering Committee, has a close partnership with the Software Engineering Institute (SEI) of Carnegie Mellon in matters of education. Within this partnership, the governmental cell is provided with educational courses in computer security creation and management, technical formation of information security, and the fundamentals and details of incident handling. Moreover, due to this cooperation, Brazil is a member to the Carnegie Mellon Software Engineering

[27] MI$^2$C is described in Bezerra, E.K., Nakamura, E.T., Ribeiro, S.L. "Critical telecommunications infrastructure protection in Brazil", First IEEE International Workshop on Critical Infrastructure Protection, 2005. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1572288.

[28] Cf. Robert Shaw., op. cit.

Institute (SEI) CERT coordination center, which is useful in networking and coordinating information security issues internationally.

Moreover, CERT.br is a member of the global Forum of Incident Response and Security Teams (FIRST),[29] which, by bringing together a variety of Computer Security Incident Response Teams (CSIRTs) from government, commercial, and educational organizations worldwide, aims to foster cooperation and coordination in incident prevention, to stimulate rapid reaction to incidents, and to promote information-sharing among members.

CERT.br is also a research partner of the Anti-Phishing Working Group (APWG), which is the global pan-industrial and law enforcement association focused on eliminating the fraud and identity theft that result from phishing, pharming, and e-mail spoofing of all types.[30]

## Early Warning and Public Outreach

### CTIR Gov[31]

The Computer Security and Incident Response Team (Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal, CTIR Gov) is subordinate to the Institutional Security Office of the Presidency of the Republic (GSI) and deals with incidents on networks belonging to the federal public administration of Brazil. An executive order of 30 June 2003 created a working group responsible for determining the various aspects related to the installation and operation of a Computer Emergency Center. The mission of CTIR Gov is to coordinate responses to computer security incidents, to assure the necessary information exchange, and thereby to offer its constituency services that are both reactive (by responding as soon as notification arrives) and proactive (designed to prevent incidents and to reduce their impact). The reactive services aim to reveal the patterns and tendencies by continuous observation of events

[29] http://www.first.org.

[30] http://www.antiphishing.org.

[31] http://www.ctir.gov.br.

in order to serve as input to security recommendations, which are later issued to the constituency. The proactive services, which include information assets analysis and constitutive structures from the various information technology environments in the Federal Public Administration, provide a broad view of available resources, their usefulness, and associated risks.

## CERT.br

CERT.br,[32] formerly known as NBSO/Brazilian CERT, is the Brazilian National Computer Emergency Response Team, maintained by the NIC.br – the executive branch of the Brazilian Internet Steering Committee. CERT.br is a service organization that is responsible for receiving, reviewing, and responding to computer security incident reports and activity related to networks connected to the Brazilian internet. Besides doing incident handling activities, CERT.br also works to increase awareness in the community and to help new Computer Security and Incidence Response Teams (CSIRTs) to establish their activities. The range of services of CERT.br includes: [33]

- To provide a focal point for reporting computer security incidents that provides coordinated support in response (and indication to others) to such reports;
- To establish collaborative relationships with other entities such as law enforcement, service providers, and telecom companies;
- To support tracing intruder activity;
- To provide training in incident response, specially for CSIRT staff and for institutions starting the creation of a CSIRT.

Additionally, CERT.br maintains a list of all Brazilian CSIRTs.[34] CERT.br also participates in the coordination of the Brazilian Honeypots Alliance and uses the data collected thereby to identify malicious activity originating in the

[32] http://www.cert.br/index-en.html.

[33] http://www.cert.br/mission.html.

[34] This list is accessible at http://www.cert.br/contact-br.html.

Brazilian internet space, and to notify the administrators of the networks involved in malicious activities identified.

## Brazilian Honeypots Alliance

The objective of the Brazilian Honeypots Alliance / Distributed Honeypots Project[35] is to increase the capacity for incident detection, event correlation, and trend analysis in the Brazilian internet space. To achieve these goals, the project is working to:

- Set up a network comprising distributed low-interaction honeypots, covering most of the Brazilian IP address space;
- Build a data analysis system that allows to study the attacks trends and correlations;
- Work with CSIRTs to disseminate the information.

The project is jointly coordinated by the CERT.br and the CenPRA (Centro de Pesquisas Renato Archer), a research institution of the Ministry of Science and Technology.[36] The honeypots network has 25 partner institutions including representatives from academia, the government, industry, and the military, which provide hardware and network blocks and maintain their own honeypots. Statistics about malicious activities observed in the honeypots are generated daily.[37] The collected data is used for intrusion detection purposes.

## RNP / CAIS

In order to coordinate separate initiatives and secure the integration of regional networks into a national network, the Ministry of Science and Technology created the National Education and Research Network (Rede Nacional de Ensino e Pesquisa – RNP) in 1989 and assigned to it the task of building a national

[35] http://www.honeypots-alliance.org.br.

[36] http://www.cenpra.gov.br.

[37] http://www.honeypots-alliance.org.br/stats.

internet network infrastructure for academic purposes. Ten years later, in 1999, the Ministry of Science and Technology and the Ministry of Education jointly started the inter-ministerial Program for the Implantation and Maintenance of the RNP, with the aim of elevating the academic network to a new position. This RNP2 backbone was officially inaugurated in 2000. Since 2002, the RNP has had an agreement with the government to reach certain goals aimed at fostering the activities of technological research in network development and the operation of advanced network means and services that benefit national education and research.[38] The RNP was the basic platform for the early development of internet technology in Brazil, and because of its historic role, it continues to play an important role in security issues.[39]

The RNP's Security Incidents Attendance Center (Centro de Atendimento a Incidentes de Segurança – CAIS), which was created in 1997, is more specifically concerned with network security within the RNP. The mission of CAIS is to resolve and prevent security incidents on the networks of RNP2, to divulge information and security alerts, and also to participate in international organizations for networking purposes. Hence, CAIS acts in the detection, solution, and prevention of security incidents on the Brazilian academic network, in addition to developing, promoting, and spreading security practices for the networks. Its concrete activities range from the providing of incident response services and the promotion of the creation of new security groups nationwide to the testing and recommendation of security tools and policies.[40]

## Laws and Legislation

Decree no. 3505 of 13 June 2000 establishes the information security policy to be used throughout the government and across all related partners in a number of different areas, including:

[38] http://www.rnp.br/en/rnp/history.html.

[39] Cf. Robert Shaw, op. cit.

[40] For a more detailed list, see http://www.rnp.br/cais/sobre.html.

- Classification and treatment of information;
- Research in technologies to support national defense;
- Accreditation and certification of products and services;
- Assurance of interoperability of systems;
- Establishing rules and standards relating to cryptography;
- Systems for the confidentiality, availability, and integrity of information.[41]

This decree was updated on 21 June 2004. The update makes the Secretaria de Comunicação de Governo e Gestão Estratégica da Presidência da República a full member of the Comitê Gestor de Segurança da Informação (CGSI).[42]

## Brazilian Penal Code

Two amendments to the Brazilian Penal Code dating from 2000 created two new offenses relative to information security. Articles 313-A and 313-B of law no. 9983 of 14 July 2000, respectively, criminalize

- The "entry, or facilitation on the part of an authorized employee of the entry, of false data, improper alteration or exclusion of correct data with respect to the computer systems or the data bank of the public administration for purposes of achieving an improper advantage for himself or for some other person, or of causing damages", as well as;
- The "modification or alteration of the information system or computer program by an employee, without authorization by or the request of a competent authority".[43]

[41] Cf. Robert Bruce et al., op. cit.

[42] http://www.planalto.gov.br/casacivil/site/exec/arquivos.cfm?cod=560&tip=doc.

[43] This law is an amendment of decree-law no. 2848 of 7 December 1940 in the Penal Code.

## Cybercrime laws

Brazil's criminal law[44] states that gaining unauthorized access to a computer system or violation of the secrecy of a computer system belonging to either a financial institution or securities dealer is a crime under article 18 of law no. 7492 of 16 June 1986, which defines crimes against the national financial system.

Senate bill PLS 00152[45] of 1991 defines the crimes involving wrongful use of computer (and also contains other provisions). This legislation defines as a crime the violation of data by means or clandestine of hidden access to a computer program or system, as well as the violation of the secrecy of data by gaining access to information contained in the system or physical medium of a third party.

Moreover, Brazil has several laws prohibiting the interception of telephone, data, or telematic communications. These laws ensuring privacy and criminalizing data interception are outlined both in the Brazilian Federal Constitution and in public law.[46]

## Brazilian Cybercrime Bill

The Brazilian Congress is currently discussing a more specialized Cybercrime Bill. Under the responsibility of Senator Eduardo Azeredo, this bill is said to be inspired by the Convention on Cybercrime of the Council of Europe[47] and attempts to bring together three draft bills dating from 1996 and 1999. In both the criminal and the military criminal codes, 11 offenses are to be typified:[48]

[44] This section is based on: Marc D. Goodman and Susan W. Brenner. "The Emerging Consensus on Criminal Conduct in Cyberspace". In: UCLA Journal of Law and Technology, Vol. 6, issue 1, 2002.

[45] http://legis.senado.gov.br/pls/prodasen/PRODASEN.LAYOUT_MATE_DETALHE.SHOW_MATERIA?P_COD_MAT=1463.

[46] For more details, cf. Goodman and Brenner, op. cit.

[47] See also: http://www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_technical_cooperation/cyber/567-LEG-country%20profile%20Brazil%20_30%20May%2007_.pdf.

[48] Senado Federal, Gabinete do Senador Eduardo Azeredo. Octopus Interface Conference – cooperation against Cybercrime. "Cybercrime legislation in Brazil, Presentation by Senator Eduardo Azeredo". (Strasbourg, 11 June 2007).

- Dissemination of malicious codes aimed at stealing passwords (phishing);
- Credit card fraud;
- Cell phone cloning;
- Offenses against honor (libel, slander, and defamation, with the stipulation of increased penalties);
- Dissemination of malicious codes aimed at causing harm (viruses, trojans, worms, etc.);
- Unauthorized access to computer network;
- Unauthorized access to information;
- Unauthorized possession, transportation, or provision of such information;
- Unauthorized disclosure of a database;
- Compound larceny with the use of computer systems;
- Disruption of public utility services;
- Attacks against a computer network – DoS, DDos, DNS, etc.

While this bill is still under discussion, in the meantime, cyber-crimes in Brazil are being judged in analogy to the Brazilian Penal code.

# Canada

## Critical Sectors

In Canada, critical infrastructure (CI) consists of the physical and information technology facilities, networks, and assets essential to the health, safety, security, or economic well-being of Canadians, and the effective functioning of government.[1] Canada's federal government (i.e., the government of Canada, and each of the provincial and territorial governments) structures its respective critical infrastructure programs as it deems appropriate. The government of Canada classifies critical infrastructure within the ten sectors listed below:

- Energy and Utilities,
- Communications and Information Technology,
- Finance,
- Health Care,
- Food,
- Water,

[*] The Country Survey of Canada 2008 was reviewed by Claudia Zuccolo, Marta Khan, Michel De Jong, and Suki Wong (Public Safety Canada).

[1] http://publicsafety.gc.ca/prg/em/nciap/about-en.asp.

- Transportation,
- Safety,
- Government,
- Manufacturing.[2]

The government of Canada recognizes that the nation's critical infrastructure could potentially be affected by both physical and cyber threats, whether natural or human-induced. Recognizing the complex nature of the threat environment, the government has adopted an all-hazards approach to protect critical infrastructure.

## Past and Present Initiatives and Policies

Canada began implementing dedicated CIP and CIIP policies in 2001 in response to the new risk environment and the increasing interconnectedness of both physical and cyber-based infrastructures. In 2003, the government of Canada brought together the office responsible for critical infrastructure and emergency preparedness and the various agencies responsible for national security into one department, Public Safety and Emergency Preparedness Canada (PSEPC). This department, which is now called Public Safety Canada, was created to keep Canadians safe from a range of risks, including natural disasters, crime, and terrorism. Its responsibilities include ensuring a coordinated response to threats and developing initiatives and programs aimed at strengthening Canada's critical infrastructure.[3]

Given the interdependencies and connectedness between critical infrastructures, the interruption of any one service could have a cascading effect and disrupt other essential services or systems. For example, during the North American Power Outage of 2003, large segments of rural and urban communities were in the dark: traffic and street lights were out; banking and government

[2] Ibid.

[3] http://www.publicsafety.gc.ca/abt/index-eng.aspx.

services were interrupted, and fuel distribution was disrupted. The disruption in one sector – electricity – affected a score of others, interrupting the delivery of important services to Canadians.

In light of this increasing interdependency, Public Safety Canada has taken a leadership role in promoting a national partnership among private and public-sector critical infrastructure stakeholders. This leadership has led to the development of the National Strategy and Action Plan for Critical Infrastructure (National Strategy and Action Plan).

## The National Strategy and Action Plan for Critical Infrastructure

To address the need for coordinated action, federal, provincial, and territorial governments have drafted a National Strategy and Action Plan that will enhance the resiliency of Canada's critical infrastructure. Its goal is to build a safer, more secure, and more resilient Canada. To achieve this goal, the National Strategy sets out a model for public-private sector partnership, an information sharing framework, and a risk-based approach to protecting critical infrastructure. The Action Plan identifies near-term deliverables that will be used to establish national priorities, goals, and requirements so that funding and resources are applied in the most effective manner. [4]

Achieving meaningful progress under the National Strategy and Action Plan calls for critical infrastructure partners to have:

- Risk-based plans and programs in place addressing and anticipating risks and threats;
- Access to robust information-sharing networks that include relevant intelligence and threat analysis; and
- Plans in place to identify and address dependencies and interdependencies to allow for more timely and effective response and recovery.[5]

[4] Public Safety Canada. "Working Towards a National Strategy and Action Plan for Critical Infrastructure. Draft for Consultation", 2008. http://www.publicsafety.gc.ca/prg/em/cip/_fl/nat-strat-critical-infrastructure-eng.pdf.

[5] Ibid.

The public-private partnership described in the National Strategy and Action Plan provides the bedrock for effective critical infrastructure protection. Governments and private-sector partners each bring core competencies that add value to the partnership and enhance Canada's protective posture.

The government can support industry efforts and assist in broad-scale protection through activities such as:

- Providing owners and operators with timely, accurate, and useful information on risks and threats;
- Ensuring that industry is engaged as early as possible in the development of risk management activities and emergency management plans; and
- Working with industry to develop and prioritize key activities for each sector.

The federal government will establish sector networks for each of the ten critical infrastructure sectors, which will provide standing fora for public-private sector partners to engage in information exchange and address critical infrastructure priorities (e.g., identify and address risks, develop plans, and conduct exercises). The federal government will also establish a National Cross-Sector Forum, which will be composed of representatives from each of the ten sector networks. The Forum will identify and address cross-sector interdependencies, and provide advice and recommendations to the minister of public safety.[6]

Risk management under the National Strategy and Action Plan builds on the Emergency Management Act,[7] which requires federal ministers to identify risks, address these risks through plans and conduct exercises. This risk management approach includes:

- Risk profiles that identify and assess risks;
- Plans to protect the most vulnerable areas of critical infrastructure;
- Exercises to validate plans and protective measures; and
- Risk management tools and guidance.

[6] Ibid.

[7] http://www.publicsafety.gc.ca/media/nr/2007/bk20070807-eng.aspx.

The National Strategy and Action Plan for Critical Infrastructure represents the first milestone in the road ahead. This document identifies a clear set of goals and objectives and outlines the guiding principles that will underpin our efforts to secure infrastructure vital to our public health and safety, national security, governance, economy, and public confidence. Most importantly, it establishes a foundation for building and fostering a cooperative environment where governments and industry can work together to protect our critical infrastructure and secure the foundations of our country and way of life.

## Information-Sharing

Information-sharing is one of the most significant issues in CIP and CIIP. Canada has been working to identify better ways to achieve this goal. Information-sharing can be viewed as a means to manage actions that can help deter, prevent, mitigate, and respond to the impact of a threat, as well as a tool to manage risk.

Government of Canada information-sharing practices related to CIP and CIIP are based on the principles articulated in the Access to Information Act (ATIA),[8] which include the public's right to access information held by the government of Canada along with specific exceptions to that right. For example, when confidential information is provided to the government of Canada by a foreign government, that information is protected by a specific and mandatory exemption in the Access to Information Act (ATIA) and cannot be disclosed.

Building on Canada's current system of safeguards, the Emergency Management Act[9] includes important amendments to the ATIA that protect specific critical infrastructure and emergency management information shared by private-sector owners and operators of Canada's critical infrastructure. This type of information will enable the government of Canada to develop comprehensive emergency management plans and mitigation and preparedness measures, improve warning capabilities, and develop better defenses and responses.

To support the information-sharing requirements in the National Strategy and Action Plan for Critical Infrastructure, Canada has developed two guides

[8] http://laws.justice.gc.ca/en/showdoc/cs/A-1///en?page=1.

[9] See the chapter on Law and Legislation.

called "Information Sharing and Protection under the Emergency Management Act"[10] and "Identifying and Marking Critical Infrastructure Information Shared in Confidence with the Government of Canada",[11] both of which elaborate on the information protection measures in the Emergency Management Act. These guides form a framework that provides a clear structure for the process of establishing information-sharing relationships, and encourage consistent approaches among participants, while ensuring that such processes are workable for and relevant to all key stakeholders. The primary goals of Canada's information-sharing framework are to assess threats and vulnerabilities, improve warning and reporting capabilities, and analyze attacks to develop better defenses and responses.

## Organizational Overview

In Canada, the lead department dealing with CIP and CIIP is Public Safety Canada. As mentioned above, the department was created in 2003 out of the integration of the former Department of the Solicitor General, the National Crime Prevention Centre, and the former Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP).

The premise for Public Safety Canada's CIP and CIIP efforts is accurate and timely threat information. The Integrated Threat Assessment Centre (ITAC) helps to arrange the information collected by various intelligence sources. In addition, the Permanent High-Level Forum on Emergencies was established to ensure cooperation between the federal and local governments.

In Canada, the private sector owns and operates more than 80 per cent of the nation's critical infrastructure. This underscores the need for effective relationships between the government of Canada and the private sector, and between all levels of government and the organizations involved in preventing and responding to the various potential threats.

[10] http://www.publicsafety.gc.ca/prg/em/cip/_fl/information-sharing-and-protection-under-the-ema-eng.pdf.

[11] http://www.publicsafety.gc.ca/prg/em/cip/_fl/labelling-sensitive-cip-information-eng.pdf.

## Public Agencies

### Public Safety Canada

Public Safety Canada provides policy advice and support to the minister of public safety on issues related to public safety, including national security and emergency management, policing and law enforcement, interoperability and information-sharing, border management, corrections and conditional release, Aboriginal policing, and crime prevention. The Public Safety Canada portfolio also includes the Royal Canadian Mounted Police (RCMP), the Canadian Security Intelligence Service (CSIS), the Correctional Service of Canada, the National Parole Board, the Canada Firearms Centre, the Canada Border Services Agency, and three review bodies.[12]

Public Safety Canada continues the mandate given to the Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) to combine critical infrastructure protection and emergency management responsibilities in one organization. This approach reflects the new risk environment, where the physical and virtual dimensions of infrastructures are increasingly interconnected. Combining critical infrastructure protection and emergency management resources and policy tools with acquired knowledge and experience in emergency management should ensure a stronger, more integrated and effective national security posture. Critical infrastructure protection and emergency management are not seen as separate endeavors, but as part of the assurance and protection continuum.

Public Safety Canada is the focal point for coordinating, analyzing, and sharing information related to physical and virtual threats to the Canadian critical infrastructure. Once it has received notification, the Government Operations Center, located in Public Safety Canada, assesses the threat to Canada and further distributes the bulletin and assessment to critical infrastructure owners and operators as well as emergency management contacts in Canada. [13]

[12] http://www.publicsafety.gc.ca/abt/wwa/index-eng.aspx.

[13] Information provided by an expert.

### Integrated Threat Assessment Centre (ITAC)

The Integrated Threat Assessment Centre (ITAC)[14] was created to facilitate the integration of intelligence from various sources into comprehensive threat assessments. These are based on intelligence and trend analysis evaluating both the probability and potential consequences of threats. Such assessments are aimed at assisting the government of Canada to coordinate activities in response to specific threats more effectively in order to prevent or mitigate risks to public safety.

Several federal government departments feed into ITAC, including: Public Safety Canada, the CSIS, the Department of National Defence, the Canada Border Services Agency, Foreign Affairs Canada, Transport Canada, the RCMP, the Communications Security Establishment, the Privy Council Office, and the Ontario Provincial Police.[15] The focus of the threat assessments is on events and trends related to domestic and international terrorism. Although the assessments are related to national security issues, they are produced at various levels of classification, allowing for a broader distribution. ITAC assessments are currently distributed to the federal government and foreign partners through ITAC; law enforcement agencies receive the assessments through the RCMP.

### Federal Provincial High-Level Forum on Emergencies

Major emergencies require extremely close cooperation between the federal government, provinces and territories, municipalities, and first responders. The government of Canada has therefore invited provinces and territories to establish a permanent high-level forum on emergencies in order to allow for regular strategic discussion of emergency management issues among key national players.[16]

## Public-Private Partnerships

The Canadian private sector, which owns and operates more than 80 per cent of the nation's infrastructure, plays a key role in securing cyberspace. National sector

[14] http://www.itac-ciem.gc.ca/index-eng.asp.

[15] http://www.itac-ciem.gc.ca/prtnrs/index-eng.asp.

[16] Information provided by an expert.

associations such as the Canadian Electricity Association (CEA), the Canadian Bankers Association (CBA), the Canadian Telecommunications Emergency Preparedness Association (CTEPA), and others have been active in promoting enhanced CIP/CIIP efforts. Currently, Canada's CI sectors are working to enhance information-sharing among their members, with government, and between sectors.

It is increasingly recognized that information on threats, vulnerabilities, corrective measures, and best practices should be shared widely across sectors and with governments. Canadian industry and governments at all levels are working together to improve information-sharing and analysis efforts. Industry sectors have identified a variety of challenges, including such issues as timeliness and relevancy of threat information. As industry efforts to increase cooperation and information-sharing mature, so will the national ability to respond to and manage cyber-incidents and attacks.[17]

## Early Warning

### Canadian Cyber Incident Response Centre (CCIRC)

Public Safety Canada's Canadian Cyber Incident Response Centre (CCIRC)[18] provides national and international leadership in cyber-readiness and response. CCIRC is Canada's national focal point for coordinating cyber-security incident response and monitoring the cyber-threat environment 24 hours a day, seven days a week.

CCIRC leverages the IT security capabilities of the federal government to provide the following services to critical infrastructure sectors:

- Incident response, coordination, and support;
- Monitoring and analysis of the cyber-threat environment;
- IT security-related technical advice;

[17] Cf. Public Safety Canada. "Working Towards a National Strategy", op. cit.

[18] http://www.publicsafety.gc.ca/prg/em/ccirc/index-eng.aspx.

- National awareness and education (training, standards, best practices).

When warranted, Public Safety Canada issues cyber-alerts and advisories, as well as other cyber-related information products to respond to potential, imminent, or actual threats, vulnerabilities, or incidents affecting Canada's critical infrastructure. This information is made available to all levels of government, as well as to non-government organizations.

CCIRC will build upon existing international relationships and is designed for improved interoperability with its allied partners.

## Government Operations Centre (GOC)

Public Safety Canada is home to the Government Operations Centre (GOC).[19] The GOC operates 24 hours a day, seven days a week. Its purpose is to provide strategic-level coordination and direction on behalf of the government of Canada in response to an emerging or occurring event affecting the national interest. It also receives and issues information dealing with any emerging or occurring threat to the safety and security of Canadians and Canada's critical infrastructure.

Information received by the GOC is quickly verified, analyzed, and distributed to the appropriate response organizations. This is made possible through Public Safety Canada's close linkages with other government departments and agencies; provincial, territorial, and municipal governments; and the private sector.

Calling upon resources and experts in various fields, the GOC helps to ensure that the right resources are in the right place at the right time. It coordinates the response to calls for help from other government departments and agencies; provincial, territorial, and municipal governments; and the private sector.

[19] http://www.publicsafety.gc.ca/prg/em/goc/index-eng.aspx.

# Law and Legislation

## Canadian Criminal Code Sections

- 342.1 (1): Every one who, fraudulently and without colour of right, (a) obtains, directly or indirectly, any computer service, (b) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly , any function of a computer system, (c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or an offence under section 430 in relation to data or a computer system, or (d) uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (a), (b) or (c) is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction.[20]
- 342.2 (1): Every person who, without lawful justification or excuse, makes, possesses, sells, offers for sale or distributes any instrument or device or any component thereof, the design of which renders it primarily useful for committing an offence under section 342.1, under circumstances that give rise to a reasonable inference that the instrument, device or component has been used or is or was intended to be used to commit an offence contrary to that section, (a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years; or (b) is guilty of an offence punishable on summary conviction.[21]
- 430. (1.1): Every one commits mischief who willfully (a) destroys or alters data; (b) renders data meaningless, useless or ineffective; (c) obstructs, interrupts or interferes with the lawful use of data; or (d) obstructs, intercepts

[20] http://laws.justice.gc.ca/en/showdoc/cs/C-46/bo-ga:l_IX-gb:s_335//en#anchorbo-ga:l_IX-gb:s_335.

[21] Ibid.

or interferes with any person in the lawful use of data or denies access to data to any person who is entitled to access thereto.[22]

## Emergency Management Act 2007

The Emergency Management Act (EMA) came into force in August 2007 and replaced its predecessor, the Emergency Preparedness Act 1985, with new and more comprehensive measures that strengthen the federal role in emergency management and critical infrastructure protection.

The purpose of the new Emergency Management Act (EMA) is to strengthen the readiness posture of the government of Canada to prepare for, mitigate the impact of, and respond to all hazards in Canada by emphasizing the need for a common and integrated approach to emergency management activities in the government of Canada. It recognizes that emergency management in an evolving risk environment requires a collective and concerted approach between all jurisdictions, including the private sector and non-governmental organizations. The act reflects a comprehensive, all-hazards approach to emergency management.

The EMA sets out the duties and responsibilities of the minister in providing national leadership by coordinating emergency management for the government of Canada. In particular, this involves:

- Coordinating the federal response to emergencies in Canada and the US;
- Establishing standardized elements for emergency plans within the government of Canada;
- Monitoring, evaluating, and testing the robustness of EM plans of government institutions;
- Enhancing cooperation with other jurisdictions and entities by promoting common standards and information-sharing.

The EMA also outlines the responsibilities of other federal ministers in carrying out their emergency management responsibilities.

[22] http://laws.justice.gc.ca/en/showdoc/cs/C-46/bo-ga:l_X-gb:s_422//en#anchorbo-ga:l_X-gb:s_422.

The act addresses a common concern within the private sector: the confidentiality of the information shared with government, and specifically its protection from disclosure in response to a request under the Access to Information Act. Such releases could harm the competitive position and business reputation of service providers and prevents the building of trusted partnerships between industry and government. The importance of information-sharing was recognized in the EMA with the inclusion a consequential amendment to the Access to Information Act that exempts from disclosure critical infrastructure and emergency management information that is shared in confidence with the government.[23]

## The Department of Public Safety and Emergency Preparedness Act 2005

The Department of Public Safety and Emergency Preparedness Act[24] is Public Safety Canada's enabling legislation that sets out the general powers, duties, and functions for the department. The act establishes the public safety minister's powers and authorities to secure public safety and emergency preparedness, and to provide leadership at the national level.

[23] http://www.publicsafety.gc.ca/media/nr/2007/bk20070807-eng.aspx.

[24] http://laws.justice.gc.ca/en/P-31.55/index.html.

# Estonia

## Critical Sectors

Estonia is one of the most rapidly developing information societies in Central and Eastern Europe. Estonia attracted a lot of attention in 2005 when it carried out its first round of internet-based voting in the local government elections of 2005 (in 2007, Estonia even became the first country in the world to feature e-voting in parliamentary elections). These elections were the results of constant and ambitious efforts to foster the information society.

The uninterrupted functioning of information and communication infrastructures (ICTs) provides the basis for such a highly developed information society. Information security and the protection of critical information infrastructures are therefore essential parts of Estonia's security policy.[1]

There are following critical sectors as defined by the Emergency Preparedness Act (consolidated text July 2002): "Vitally important sectors and the ministries administering these are the following:

* The Country Survey of Estonia 2008 was reviewed by Thomas Viira, Estonian Informatics Center, and Jaak Tepandi, Institute of Informatics, Tallinn University of Technology.

[1] Information security and CIIP became even more important after the online attacks on Estonian government sites of April/May 2007, which attracted worldwide attention.

- Maintenance of public order, fire extinguishing and rescue work, organization of protection of data banks – the Ministry of Internal Affairs;
- Functioning of the energy and gas system, organization of supply with staple goods; organization of telecommunications and postal services, and transport – the Ministry of Economic Affairs and Communications;
- Organization of supply with foodstuffs – the Ministry of Agriculture;
- Functioning of the financial system – the Ministry of Finance;
- Organization of health care, social insurance and social welfare, provision of psycho-social help, assistance to refugees and the evacuated, labor force calculation – the Ministry of Social Affairs;
- Organization of protection of cultural property – the Ministry of Culture;
- Organization of environmental protection and monitoring – the Ministry of the Environment.

The Ministry of Internal Affairs is the leading ministry in the field of crisis management." [2]

## Past and Present Initiatives and Policy

"I would not consider it an exaggeration to say that "e" has put Estonia back on the world map."[3] This statement by Meelis Atonen, the then Minister of Economic Affairs and Communication in the preface of the policy paper Estonian IT Policy: Towards a More Service-Centered and Citizen Friendly State: Estonian Information Policy 2004–2006, outlines the importance of IT for Estonia.

Accordingly, the Estonian government has promoted various initiatives to strengthen the IT-sector. The first policy paper, Principles of Estonian Information

[2] http://www.rescue.ee/index.php?page=143&PHPSESSID=220faec9593e393510ea6f39fef5a197.

[3] Meelis Atonen. "Preface". In: Ministry of Economic Affairs and Communication. "Estonian IT Policy: Towards a More Service-Centered and Citizen-Friendly State. Principles of the Estonian Information Policy 2004–2006." http://www.riso.ee/en/files/Policy.pdf.

Society, was set out in 1998. It was followed by the above-mentioned paper, which defined the principles of the Estonian information policy for 2004–2006; and since January 2007, the Estonian IT policy has been defined by the Estonian Information Society Strategy 2013.

Due to these strategies and their efficient implementation, Estonia succeeded in making considerable progress on the way towards an information society (for example, Estonia successfully launched new ID cards in 2002 that can also be used for issuing digital signatures and for using web-based services of the state).[4]

## National Security Concept of the Republic of Estonia 2004

With the nation's rapid transformation into an information society, information security and the protection of communication infrastructure became important issues of national security. The National Security Concept 2004 therefore refers explicitly to the risks stemming from threats to information security. It is stated that "the constantly increasing rate at which electronic information systems are adopted in Estonia, and their connection with and dependence upon world-wide information systems, increases the threat of computer crime as well as the vulnerability of information systems, including spheres of primary importance to national security."[5]

## National Information Security Policy

One of the aims of the policy paper for the Estonian information policy 2004–2006 was to define basic principles of a common IT security policy.[6] These basic principles were elaborated by a joint working group representing both the public and the private sectors and formulated in the National Information Security Policy.

[4] http://www.id.ee/?id=11019.

[5] http://web-static.vm.ee/static/failid/067/National_Security_Concept_2004.pdf.

[6] http://www.riso.ee/en/files/Policy.pdf.

The purpose of the Estonian Information Security Policy is to contribute to the development of a secure and security-aware information society. More specifically, the policy includes the following goals: elimination of non-acceptable risks to electronic communication networks and communication systems; defense of basic human rights; raising awareness about IT security and providing the respective training; participation in international initiatives related to e-security; and increasing the competitiveness of the Estonian economy.[7]

In order to achieve these goals, the Estonian information security policy comprises five domains:

- Cooperation and coordination at the national and international levels: this domain includes initiatives such as the development and maintenance of a computer incident response capacity as well as participation in the European Network and Information Security Agency (ENISA);
- Crisis management and cybercrime: this domain includes preparations of crisis management plans and all initiatives designed to fight national and international cybercrime;
- Education and training: activities related to awareness-raising in government agencies as well as in the private sector and among the general public;
- Legislation and regulation related to IT security: specification, elaboration, and implementation of procedures, documentation, and means for ensuring information security;
- Activities for the protection of people and assets: protection of human rights and particularly of personal data.

As the Ministry of Economic Affairs and Communication states in the yearbook 2005 on Information Technology in Public Administration of Estonia,[8]

[7] http://www.riso.ee/en/information-policy/security.

[8] Ministry of Economic Affairs and Communications of Estonia. "Information Technology in Public Administration of Estonia 2005", p. 33. http://www.riso.ee/en/pub/yearbook_2005.pdf.

the Information Security Policy is designed to address IT security issues in the public sector as well as in the private sector.

In the same yearbook, information security is also clearly defined as part of critical infrastructure protection efforts: "The information security policy contributes to critical information infrastructure protection and takes into account information security aspects in other fields of critical information protection. The various fields of information security policy provide support and basic data for the protection of critical infrastructure and vice versa."[9]

## Estonian ID Card

The Estonian ID card is not only a plastic card for the identification of its owner, but also contains a chip with a personal data file and two certificates enabling secure electronic authentication and digital signature.[10] It can be used for internet-based services provided by the Estonian government as well as for several services offered by the private sector.

Ninety per cent of the residents of Estonia already carry the new ID card. However, only a minority uses the ID card as an identification and authentication tool for digital services. The Estonian government, in cooperation with private-sector partners, tries to promote the usage of the ID card (see the chapter on Organizational Overview for the public-private initiative Computer Protection 2009).

## Estonian Information Society Strategy 2013

Since January 2007, the new Estonian Information Society Strategy 2013 entered into force, setting out the general framework, objectives, and respective action fields for the development of the information society in Estonia. The strategy emphasizes the importance of cooperation between the public and private sectors and the need for coordination among all ministries involved.

[9] Ibid., p. 48.

[10] Ministry of Economic Affairs and Communications of Estonia. "Information Technology in Public Administration of Estonia 2006", p. 23. http://www.riso.ee/en/pub/2006it/.

Three objectives are mapped out by the strategy:

- Development of a citizen-centered and inclusive information society: the percentage of internet users in Estonia is to be further increased;
- Development of a knowledge-based economy: ICT uptake by enterprises is to be promoted and the competitiveness of the ICT sector to be increased;
- Development of citizen-centered, transparent, and efficient public administration by improving the efficiency of the public sector and providing user-friendly e-services in the public sector.

One of the principles for the development of the information society as defined in the document also refers to the importance of information security. It is stated that "the development of the information society must not undermine people's sense of security."[11] Non-acceptable risk must be avoided, and personal data and identities must be secured.

## The Estonian IT interoperability framework

The Estonian IT interoperability framework[12] is a set of standards and guidelines aimed at ensuring the provision of services for public administration institutions, enterprises, and citizens both in the national and in the European context. The latest version of the document (available in Estonian)[13] comprises the IT security interoperability framework, which specifies the activities related to CIIP and the use of the system of security measures by organizations.

## The Estonian Cybersecurity Strategy

The Estonian Cybersecurity Strategy lays out the priorities and activities aimed at improving the security of country's cyberspace. The Cybersecurity Strategy

[11] Estonian government. "Estonian Information Society Strategy 2013", p. 4. http://www.riso.ee/en/files/IYA_ENGLISH_v1.pdf.

[12] http://www.riso.ee/en/information-policy/interoperability.

[13] http://www.riso.ee/wiki/Pealeht.

concentrates on the following areas: the responsibilities of state and private organizations, vulnerability assessments of critical national information infrastructure, the response system, domestic and international legal instruments, international cooperation, and training and awareness-raising issues.[14]

## Organizational Overview

In Estonia, there is no single central authority responsible for CIIP. Several ministries and their respective subunits are directly involved. However, the main tasks of CIIP are assigned to the Ministry of Economic Affairs and Communication (MEAC).[15] The MEAC plays a leading role with regard to information security, since two central agencies for the national IT policy are subordinated to the MEAC: The Department of State Information System (RISO), which is the central body for overall ICT coordination; and the Estonian Informatics Centre (RIA), which constitutes the implementing body under the MEAC. Other important public agencies that are dealing with CIIP are located within the Ministry of the Internal Affairs and within the Ministry of Defense. These two ministries are responsible for internal security and crisis management. With the project Computer Protection 2009, there is also an important public-private partnership, which aims to foster the security of the Estonian information society.

### Public Agencies

#### The Department of State Information System (RISO)

Within the Ministry of Economic Affairs and Communication (MEAC), the Department of State Information System (RISO)[16] is responsible for overall ICT coordination. With regard to IT security, it ensures the involvement of the private sector and cooperation among the different IT managers of the governmental agencies. In order to improve the security of the governmental communication

[14] Information provided by an expert.
[15] http://www.mkm.ee/index.php.
[16] http://www.riso.ee/en/.

network, RISO also coordinates the actions of the county and local governments and launches and supports broad public awareness campaigns.

The department also prepares appropriate legislation drafts and defines standard procedures for e-government. These regulative measures are usually developed in coordination with other ministries and with the private sector.

At the international level, RISO participates in the European Network and Information Security Agency (ENISA), and is involved in other cross-border initiatives, such as the development of the International Telecommunication Union (ITU) Global Cybersecurity Agenda.

## The Estonian Informatics Centre (RIA)

The Estonian Informatics Centre (RIA) was established to develop and manage data communication services for governmental organizations. Thus, the RIA is responsible for the technical security of the state's communication and information infrastructure. That includes measures to ensure the security of the governmental portals (which consists of three platforms on the internet);[17] preventive measures to maintain the security of the governmental data communication network; and monitoring and improving the overall security of IT in Estonia.

In 2005, the Estonian Computer Emergency Response Team (CERT) was established at RIA, in compliance with the obligation to form a national center for IT security, as laid out in the policy paper "Principles of the Estonian Information Policy 2004–2006". With the establishment of the Estonian CERT, the RIA has consolidated its role as the responsible body for the technical facets of CIIP. (For more information on the Estonian CERT, see the chapter on Early Warning and Public Outreach).

## The Estonian National Communications Board

The Estonian National Communications Board manages and regulates the postal sector as well as the market for electronic communications in Estonia. It is

[17] http://www.riik.ee, which is the e-government platform; http://www.eesti.ee, which is the information platform; and https://www.esti.ee, which is the citizens' portal.

responsible for the management of limited communication resources (e.g., radio frequencies) as well as for the regulation of the electronic communications market in Estonia.[18] In this function, the National Communication Board oversees the companies operating in the field of electronic communications and ensures the compliance of these companies with security requirements.

### The Security Agencies

The task of the security agencies – the Security Police Board (belonging to the Ministry of Internal Affairs) and the Information Board (located within the Ministry of Defense) – is to ensure national security and maintain constitutional order through non-military preventive measures.[19] The functions of the Security Police Board are to prevent espionage, protect state secrets, and combat terrorism and corruption. The Information Board, in turn, collects intelligence concerning foreign countries and is responsible for the security of electronically transmitted information.

## Public-Private Partnerships

### Computer Protection 2009

Computer Protection 2009 is a joint project of the Look@World Foundation and the Ministry of Economics and Communications. The Look@World Foundation was established in 2001 by ten leading companies in Estonia with the goal to foster the development of the IT society in Estonia.

The Computer Protection 2009 project (also called Look@World 2) aims to foster the security of the Estonian information society, so that in 2009, Estonia will be the country "with the most secure information security in the world".[20] To achieve this ambitious goal, the signing partners of the initiative started broad promotion programs to raise public awareness of IT security. In particu-

[18] http://www.sa.ee/atp/?id=3476.

[19] Estonian government. "National Security Concept of the Republic of Estonia 2004", p. 16.

[20] http://www.riso.ee/en/node/80.

lar, they try to encourage citizens to use their ID card for electronic personal authentication.

The main activities of the foundation, however, include sharing of information among companies, public agencies, and citizens on how to adequately recognize threats to information security and to protect oneself against them.[21] Improving and promoting internet security-related dialog and cooperation between the public and private sector is a distinctive concern of the Computer Protection 2009 initiative.

## Early Warning and Public Outreach

### CERT Estonia

Established in 2005 at the Department for Handling Information Security Incidents of the Estonian Informatics Centre (RIA), the Computer Emergency Response Team of Estonia is responsible for the management of security incidents in the .ee computer networks. Its main task is "to assist internet users in Estonia in the implementation of preventive measures in order to reduce possible damage from security incidents and to help them in responding to security threats".[22] This means that CERT Estonia offers support for incident handling and acts as an early-warning center for IT security.

The process of incident handling comprises the collection of information on incidents, analysis of attacks, and coordination of the response activities. However, since not all incidents are of the same importance, it is also important to assign priorities to each incident according to the severity level and scope. In assessing this prioritization, CERT Estonia takes the following aspects into account: the number of affected users; the type of incident; the target of an attack as well as the attack's point of origin; and the required resources for handling the incident.[23]

[21] Ministry of Economic Affairs and Communications of Estonia. "Information Technology in Public Administration of Estonia 2006", p. 42.

[22] http://www.ria.ee/28201.

[23] http://www.ria.ee/28201.

Of course, attacks on critical infrastructures that may jeopardize people's lives would be considered to be incidents of highest priority.

In the domain of early warning, CERT Estonia cooperates with various national and international partners. The broad network enables the CERT to recognize new threats and vulnerabilities in a timely manner. Warnings are mainly issued in cases of attacks with higher level of severity, extremely widespread threats, and highly severe vulnerabilities.[24]

In addition, once CERT Estonia has managed to successfully launch the above-mentioned services, it also intends to contribute to the promotion of awareness-raising in the field of IT security.[25]

### Infosecurity Portal

When the Computer Protection 2009 initiative was launched, a gateway to IT security- related information and discussions was established that is available in Estonian and in Russian.[26] The portals contain numerous links, articles, and news, and enable the users to obtain and share information about threats related to the internet. The goal of the portal is to help citizens to familiarize themselves with the world of information security.

## Law and Legislation

Since 1997 Estonia enacted a series of laws with regard to CIIP in general. Estonia was also among the first countries to sign the Council of Europe's Convention on Cybercrime in 2001, and fully enacted it in 2004.

The following legal instruments are relevant to information security and CIIP:

[24] Ministry of Economic Affairs and Communications of Estonia. "Information Technology in Public Administration of Estonia 2005", p. 36.

[25] http://www.ria.ee/28201.

[26] The Estonian version is available at http://www.arvutikaitse.ee; the Russian one can be found at http://www.infosecurity.ee.

- Emergency Preparedness Act: This act provides the legal basis for the organization of emergency preparedness of and for crisis management by the national government, government agencies, and local governments;[27]
- State Secrets Act: defines state secrets, access to state secrets, and the basic procedure for the processing of state secrets;[28]
- Personal Data Protection Act: This act determines the principles for processing personal data (Chapter 1). Paragraph 6 defines the principle of security, which is binding for all processors of personal data: "security measures to prevent the involuntary or unauthorised alteration, disclosure or destruction of personal data shall be applied in order to protect the data";[29]
- Public Information Act: The purpose of this act is to ensure that the public and every person has the opportunity to access information intended for public use, based on the principles of a democratic and social rule of law and an open society, and to create opportunities for the public to monitor the performance of public duties. The act defines the state information system, describes the organization of databases belonging to a state information system, and lays out the legal basis for providing and using data services. The act provides for an approach integrating different areas of government through legislation that defines the administrative system of the state information system and other support systems for the state information system, as well as the status of databases established within the information system of the public sector;[30]
- Electronic Communications Act: This act defines the requirements for the publicly available electronic communications networks and communications services. With regard to CIIP, the security requirements are of particular interest: "A communications undertaking must guarantee the

[27] http://www.rescue.ee/index.php?page=143&PHPSESSID=220faec9593e393510ea6f39fef5a197.

[28] http://www.legaltext.ee/text/en/X30057K7.htm.

[29] http://www.legaltext.ee/text/en/X70030.htm.

[30] http://www.esis.ee/ist2004/106.html.

security of a communications network and prevent third persons from accessing the data […] without legal grounds;”[31]

- Information Society Services Act: This act provides the requirements for information society service providers, the organization of supervision, and liability for violation of this act.[32]

## Penal Code

- Several articles of the Estonian penal code refer to information security:
- Article 206 (Computer sabotage): Unlawful replacement, deletion, damaging or blocking of data or programs in a computer, as well as unlawful entry of data or programs in a computer is punishable by fines or imprisonment.
- Article 207: Damaging or obstruction a connection to a computer network or computer system is punishable.
- Article 208: Spreading computer viruses is punishable by fines or imprisonment.
- Article 217: Unlawful use of a computer, computer system, or computer network by way of removing a code, password, or other protective measures is punishable by fines or imprisonment.
- Article 284: Unlawfully handing over the protection codes of a computer, computer system, or computer network, if committed for the purpose of personal gain and in a manner which causes significant damage or results in other serious consequences, is punishable by fines or imprisonment.

[31] http://www.legaltext.ee/text/en/X90001K2.htm, Chapter 10, Paragraph 101.

[32] http://www.legaltext.ee/text/en/X80043.htm.

# Finland

## Critical Sectors

Finland aims to ensure society's ability to function in all circumstances by securing the functioning of both official infrastructures and those administered by individual citizens and businesses. Consequently, as an information society, Finland can only function smoothly if its critical information infrastructure is fully operational, because any disruptions may result in dramatic consequences.

The critical sectors and the protection policies for critical infrastructures are defined in the Security of Supply Act and in the Decree of the National Emergency Supply Agency (NESA) of 1992.[1] Based on these acts, the Finnish government sets official goals for the development of security of supply, which are updated every 5–6 years. The current governmental decision is from 2002, but there is already a proposal for a new decision, which is to be enacted in 2008

[*] The Country Survey of Finland 2008 was reviewed by Hannu Sivonen, Ilkka Kananen, and Veli-Pekka Kuparinen, National Emergency Supply Agency (NESA).

[1] The Security of Supply Act is the legal basis for ensuring supplies of various basic materials in the case of emergency situations. Based on this act, the National Emergency Supply Agency (NESA), a subordinate agency to the Ministry of Trade and Industry (now Ministry of Employment and the Economy), was founded in 1993 for the development and maintenance of security of supply. NESA is the national stock-holding agency of Finland.

(the critical infrastructure will be defined in more detail, but the definition will include the same sectors as in 2002).[2]

Currently, the following infrastructures and services are deemed to be critical in Finland:

- Energy Networks and Supply,
- Electronic Information and Communication Systems, including communication networks, IT systems (including SCADA systems), electronic mass media, and payment systems of banks and insurances,
- Transportation and Logistics Systems,
- Water supply and Other Municipal Utilities,
- Infrastructure Construction and Maintenance,
- Financial Services,
- Food Supply,
- Health Services,
- Print Media.

The government focuses on safeguarding society's critical infrastructure. The objective is to protect fundamental structures by using non-critical technology and organizations, even during disturbances and emergency situations. Accordingly, an essential aspect of safeguarding the technology is ensuring the system's ability to recover.

## Past and Present Initiatives and Policies

### Governmental Support for the Information Society

From the early 1990s on, the Finnish government has worked continuously on new programs aimed at promoting the Information Society, its infrastructure,

[2] Information provided by an expert.

and the protection of the infrastructure. On the basis of their reports, several ministries have produced action plans and provided funding for Information Society projects.

In 2005, the Finnish government issued a strategy resolution, which includes an Information Society Programme.[3] This program promotes the development of the Information Society in the areas of telecommunication infrastructure, digital television, citizens' skills to utilize the Information Society, research and development, and ICT in public administration and business.

As part of the implementation of this program, the government drafted the National Knowledge Society Strategy for 2007–2015.[4] The vision of the strategy is "good life in information society", and accordingly, it aims to support the "transformation of Finland into an internationally attractive, human-centric and competitive knowledge and service society."[5]

As the previous strategies in regard to the information society, the National Information Society Strategy 2007–2015 emphasizes the security of networks so that citizens can trust the electronic services. In addition it highlights the importance of well-functioning infrastructures: "Information networks are dependent upon basic infrastructure, such as electricity supply. Security of supply in the information society is especially important in crisis situations."[6]

[3] The Finnish Government. "Information Society Programme" (April 2005). http://www.tietoyhteiskuntaohjelma.fi/esittely/en_GB/introduction/_files/11233297000000607/default/tietoyhteiskuntaojelma_en_2005.pdf.

[4] The Finnish Government. "National Knowledge Society Strategy for 2007–2015" (September 2006). http://www.tietoyhteiskuntaohjelma.fi/esittely/en_GB/introduction/_files/76222690188788831/default/Strategia.

[5] Ibid., p. 4.

[6] Ibid., p.12.

## Strategy for Securing the Functions Vital to Society 2006

In order to ensure the security of critical infrastructures, the Finnish government issued the Strategy for Securing the Functions Vital to Society.[7] The strategy was first released in 2003 and was reviewed and updated in 2006.[8]

The strategy paper divides the vital functions into seven broad areas: management of government affairs, international activities, national military defense, internal security, functioning of the economy and infrastructure, the population's income security and capability to function, and psychological crisis tolerance.

Electronic information and communication systems are recognized as an important part of a well-functioning society. It is vital to secure electronic communication networks and their information security, to determine basic security levels for services and technical systems, and to ensure that the regulations on construction and maintenance of systems are observed. In addition, it is critical to coordinate the development of networks used by the authorities, to safeguard the state's information-processing capacity, and to provide guidelines for public electronic services, the public data administration, and information security. Among vital threats to society, the strategy paper lists threats to information and communication systems first.

## Security and Defense Policy 2004

The Finnish government submits a Security and Defense Policy report to parliament every three or four years. The next report will be published in 2008. In 2004,[9] the report emphasized the growing importance of electronic information

[7] The Finnish Government. "Strategy for Securing the Functions Vital to Society" (2003). http://www.defmin.fi/files/168/2587_2047_Government_Resolution_On_Securing_ The_Functions_Vital_To_Society_1_.pdf.

[8] The Finnish Government. "Strategy for Securing the Functions Vital to Security" (2006). http://www.defmin.fi/files/858/06_12_12_YETTS__in_english.pdf.

[9] The Finnish Government. "Finnish Security and Defence Policy" (2004). http://www.defmin.fi/files/311/2574_2160_English_White_paper_2004_1_.pdf.

and communications technology systems for the functioning of modern society. It is no longer possible to shift to the use of manual reserve systems.

Along with the rest of society, criminals also use networks and systems. Therefore, specific chapters in this policy paper are devoted to combating cyber-crime and to securing society's electronic communications and information systems. According to the report, the capacity of the police for protecting information systems, telecommunication connections, and electronic transactions, as well as for combating cyber-crime, will be expanded. Cooperation between the police and the Finnish Communications Regulatory Authority (FICORA) will raise the level of information systems protection required in an open network environment.

The security level of communication networks is being increased. ICT used by major government agencies, security authorities, and vital industries are safeguarded by prioritization and by the construction of communication networks and data systems for special use. One example is Finland's Public Authority Network VIRVE.[10]

## National Information Security Strategy

In 2001, the government set up an Advisory Committee for Information Security (ACIS) under the Finnish Communications Regulatory Authority (FICORA) as a point of contact for citizens, companies, organizations, and authorities on information security issues.

In 2002, ACIS released its "National Information Security Strategy Proposal",[11] which was approved by the government in 2003. The paper lists detailed policy objectives and measures to be implemented as well as the responsibilities of the various stakeholders. The priority areas of the strategy are to secure electronic services, to secure biometric identification, to protect critical

[10] Finland's Public Authority Network VIRVE, based on TETRA (Terrestrial Trunked Radio) technology, is being expanded by increasing the number of users. Among the user groups are fire and rescue services, police, border guards, customs, the military, and health services. http://www.virve.com.

[11] Advisory Committee for Information Security. "National Information Security Strategy Proposal" (2002). http://www.ficora.fi/englanti/document/infos.pdf.

infrastructure, to combat cyber-crime, to protect the national information assets, to enhance information security awareness by promoting the annual National Information Security Day, and to improve awareness in business enterprises.

The most visible result of the implementation of the strategy has been National Information Security Day on 11 February, held for the fifth time in 2008. The day promotes secure internet usage, particularly for schoolchildren and their parents. Another important result is the strengthening of the national Computer Emergency Response Team (CERT-FI) to give special service for actors in critical sectors in Finland.[12]

## Organizational Overview

In Finland, there are three major public agencies dealing with CIIP. The Finnish Communications Regulatory Authority (FICORA) promotes the Information Society, as well as technical regulation and standardizations; the National Emergency Supply Agency (NESA) analyzes threats and risk against critical (information) infrastructures; and finally, the Steering Committee for Data Security in State Administration (VAHTI) develops policy guidelines and practical guides for the security of information systems.

In addition, there are three important public-private partnerships in the field of CIIP: The National Emergency Supply Council (NESC), the Ubiquitous Information Society Advisory Board, and the Finnish Information Society Development Centre (TIEKE).

### Public Agencies

#### Finnish Communications Regulatory Authority (FICORA)

The Finnish Communications Regulatory Authority (FICORA)[13] belongs to the Ministry of Transport and Communications. FICORA is a general administra-

[12] Information provided by an expert.

[13] http://www.ficora.fi/en/index/viestintavirasto/esittely.html.

tive authority for issues concerning electronic communications and Information Society services. Its mission is to promote the development of the Information Society in Finland. The specific duty of FICORA is to safeguard the functionality and efficiency of the communications markets in order to ensure that consumers have access to competitive and technically advanced communications services that are affordable as well as of good quality.

FICORA's mission includes issuing technical regulations and coordinating standardization at the national level. It also oversees the protection of privacy and securing data in electronic communications. In addition, FICORA encourages national and international co-operation.

FICORA also ensures that telecommunications operators are prepared for emergencies. The operators must report significant information security incidents as well as any threats, faults, or disturbances in telecommunication networks and services to FICORA. FICORA checks the operators for compliance with the Communications Market Act and the Act on the Protection of Privacy in Electronic Communications and monitors compliance with the relevant technical regulations and standards. In pursuing this task, FICORA collects information from the operators and conducts inspections.

Finally, FICORA operates the CERT-FI (see the chapter on Early Warning and Public Outreach), which is tasked with the detection and resolution of data security infringements.[14]

## National Emergency Supply Agency (NESA)

The National Emergency Supply Agency (NESA)[15] is the cross-administrative operative authority for the security of supply in Finland. NESA works under the auspices of the Ministry of Employment and the Economy. In addition, NESA serves to develop cooperation between the public and private sectors in the field of economic preparedness, in coordinating preparations within the public administration, and in developing and maintaining the security of supply.

[14] http://www.cert.fi/en/index.html.

[15] http://www.nesa.fi.

NESA and the National Emergency Supply Council (NESC, see below) analyze threats and risks that may affect the critical infrastructure. NESA itself conducts research and finances research commissioned by outside organizations. NESA and NESC formulate plans and guidelines for public authorities and businesses with respect to the management and control of such threats and risks.

NESA has a growing role in securing the critical national infrastructure by developing and financing both technical backup systems and electromagnetic pulse (EMP)-secure premises for systems. Finland's vital communication and IT systems are located in the capital region. This is a risky concentration. Therefore, NESA owns two computer backup / colocation centers outside the capital region in order to secure society's critical IT systems in exceptional conditions.[16]

The National Fixed Line Telephone Backup Network is a digital, nation-wide separate network that was built to secure the lines of communication of vital public organizations, as well as other key subscribers, in exceptional situations and crises. The Ministry of Transport and Communications and NESA are jointly developing the network so that it can also secure other telecommunication services than voice services. NESA is involved in the development and maintenance of Finland's Public Authority Network VIRVE.

In addition, NESA has financed several projects to secure the communication and broadcast systems. These projects and activities are related to reserve systems, emergency and warning message broadcasting systems, and the construction of circuitous routes for critical nodes of networks.

In CIIP matters, NESA has participated in the preparation of European Programme for Critical Infrastructure Protection (EPCIP) and Critical Infrastructure Warning Information Network (CIWIN).[17]

## Steering Committee for Data Security in State Administration (VAHTI)

The central government's data-security and information-management policies are steered and developed by the Ministry of Finance. Guidelines are developed by

[16] Information provided by an expert.

[17] Information provided by an expert.

the Steering Committee for Data Security in State Administration (VAHTI),[18] a broad group of experts.

For the central government, the issue of data security includes a number of areas such as the use of the internet, data management outsourcing, remote work, e-mail, protection from viruses, personnel security, physical security, data communication security, and database security. The Ministry of Finance works in close cooperation with other ministries and agencies to support and facilitate cooperation in the development of e-government and electronic services in the state sector.

VAHTI has published an extensive collection of practical guides (some of them in English) for information system security. The guides are intended for the state administration, but they are also used by many private organizations.[19]

## Public-Private Partnerships

### National Emergency Supply Council (NESC)

Established in 1955, the National Emergency Supply Council (NESC, previously National Board of Economic Defense),[20] under the auspices of the Ministry of Employment and the Economy, supports and assists NESA activities (see also chapter on Law and Legislation). NESC also plans and coordinates economic preparations for implementation in case of exceptional circumstances in Finland.

NESC is a network of committees consisting of the leading experts from both the public administration and the business world. Its tasks are to analyze threats against the country's security of supply, to plan measures to control these threats, and to promote readiness planning in individual industrial sites.

NESC's areas of responsibility include the Information Society, transport logistics, food supply, energy supply, healthcare services, financial services, and defense-related and other critical industrial sectors. NESC members include

[18] http://www.vm.fi/vm/en/13_public_management_reforms16746/051_state_it/001_state_it_organisation/index.jsp.

[19] Information provided by an expert.

[20] http://www.nesa.fi/organisation/national-board-of-economic-defence.

representatives of ministries, government agencies, the private business sector, and various industrial organizations. Approximately 800 people work within the NESC.

NESC has several planning bodies in the area of information infrastructure. They have prepared instructions and basic plans for the ICT sector as well as for other vital branches of the infrastructure. In addition, NESC studies and follows up on risks and threats to the critical infrastructure and security of supply. Databases and methods have been developed to support and improve the level of readiness to act in exceptional situations.

## Ubiquitous Information Society Advisory Board

The Ubiquitous Information Society Advisory Board[21] is a body with members from ministries, public administration, NGOs, and business life. Its task is to ensure that the National Information Society Strategy will be put into practice.

One of the six working groups in the board has the task of outlining a new national information security strategy and of coordinating its implementation. The working group's term of office will last from September 2007 to February 2011.[22]

## Finnish Information Society Development Centre (TIEKE)

Since 1998, the Finnish Information Society Development Centre (TIEKE)[23] has been a key player in the development of the Information Society in Finland. TIEKE's goal is to create viable tools and expertise for use in the Information Society. Specifically, TIEKE's main focus is on the development of networking and interoperability.

TIEKE's membership includes more than 100 organizations and companies involved in the Information Society. The members operate in the areas of trade, industry, and public administration, and thus also serve individual citizens.

[21] http://www.arjentietoyhteiskunta.fi/inenglish.

[22] Information provided by an expert.

[23] http://www.tieke.fi/in_english/about_tieke.

## Early Warning and Public Outreach

### Computer Emergency Response Team Finland (CERT-FI)

FICORA's CERT-FI[24] group prevents, observes, and solves information security violations and gathers information on threats to information security. CERT-FI cooperates with national and international CERT actors and representatives of trade and industry. It is in contact with suppliers of equipment, networks, and software as well as with the police and other authorities.

CERT-FI receives notifications from telecommunications operators concerning information security incidents and threats. In addition, CERT-FI continuously follows up current global events related to information security, security problems of information systems, security incidents, and responses to them.

In 2007, CERT-FI was contacted 2664 times. The information security helpline for customers operates during business hours, but the threats and incidents are supervised around the clock, seven days a week.

Starting in 2007, CERT-FI's manpower was substantially increased. CERT-FI now also provides special service for actors in critical sectors in Finland. The special service includes a 24/7 incident warning and handling service (available also via SMS and via the VIRVE Public Authority Network), personal advice, and focused product vulnerability warnings.

[24] http://www.cert.fi/en/index.html.

# Law and Legislation[25]

## Bill for National Emergency Supply Council 2008/ Act on the National Board of Economic Defense 1960

The Act on the National Board of Economic Defense (NBED) (238/1960)[26] is the legal basis for the National Emergency Supply Council (NESC). It obliges the NBED to plan and organize activities needed to secure the economy and the livelihood of the population in exceptional situations. NBED has the legal right to obtain, from enterprises and other important actors, information that is necessary for performing its planning and organizational tasks.

In 2008, a bill for amendment of the Act on the National Board of Economic Defense was introduced to the parliament. According to the bill, the name of the board will be changed to National Emergency Supply Council (NESC). The board of directors will be shared with the National Emergency Supply Agency (NESA). The committee network and the legal jurisdiction will remain unchanged.

## Emergency Powers Act 1991

In case of serious disturbances and in emergencies, public authorities need special powers to safeguard society's essential activities. The most important provisions are contained in the Emergency Powers Act (1080/1991).[27] In crisis situations, this law empowers the government to issue provisions concerning the critical infrastructures and other functions of society.

In 2008, a bill for amendment of the Emergency Powers Act was introduced to the parliament. Under the provisions of the bill, the conditions in which the

[25] The official texts of Finnish legislation have been published in Finnish and Swedish. Some laws have an unofficial English translation. Unless otherwise indicated, we refer to the official texts.

[26] Act on the National Board of Economic Defence (NBED) (238/1960). http://www.finlex.fi/fi/laki/alkup/1960/19600238.

[27] Emergency Powers Act (1080/1991) (unofficial English translation). http://www.finlex.fi/en/laki/kaannokset/1991/en19911080.pdf.

emergency powers can be implemented are specified in more detail than in the existing act, in harmony with the new Constitution of Finland of 2000.[28]

## Security of Supply Act 1992/2005

Critical infrastructure protection actions are based on both the Security of Supply Act (1390/1992)[29] and the Decree of the National Emergency Supply Agency (NESA) (1391/1992).[30] The Finnish government specified the development of security of supply as one of the official goals for 2002.[31] The Security of Supply Act was amended in 2005 (688/2005).[32] The amendment refers to severe disturbances in otherwise normal circumstances (not only in crisis situations as defined in the Emergency Powers Act). The amendment emphasizes the securing of technical systems.

## Penal Code

In the Finnish Penal Code, Chapter 38, Amendments 578/1995[33] and 540/2007[34] specifically outlaw the endangering of information systems, and tampering with telecommunication systems.

[28] Information provided by an expert.

[29] Security of Supply Act (1390/1992). http://www.finlex.fi/fi/laki/ajantasa/1992/19921390.

[30] The Decree of the National Emergency Supply Agency (NESA) (1391/1992). http://www.finlex.fi/fi/laki/ajantasa/1992/19921391.

[31] Government decision on the Goals of Security of Supply (2002). http://www.finlex.fi/fi/laki/alkup/2002/20020350.

[32] The Amendment of the Security of Supply Act (688/2005). http://www.finlex.fi/fi/esitykset/he/2005/20050044.

[33] Penal Code Chapter 38 Amendment (578/1995) (unofficial English translation). http://www.finlex.fi/pdf/saadkaan/E8890039.PDF.

[34] http://www.finlex.fi/fi/laki/alkup/2007/20070540?search%5Btype%5D=pika&search%5Bpika%5D=540%2F2007.

## Act on Television and Radio Operations 1998

This act (744/1998)[35] obliges television or radio broadcasters to ensure that they can continue transmitting with minimum disruption even in the exceptional circumstances referred to in the Emergency Powers Act. Additionally, broadcasters must transmit information from the authorities to the public if it is necessary to save human lives, protect property, or safeguard the functioning of society.

## Act on Provision of Information Society Services 2002

This act (458/2002)[36] defines the rules of offering electronic services and the right of the authorities to limit the services if they constitute threats to consumers or to public security.

## Communications Market Act 2003

This act (393/2003)[37] obliges the communications operators to ensure the functioning of their services, regardless of whether the disturbances occur during normal times, exceptional situations, or in times of crises. The act assures the telecommunications operators that any extra expenses incurred through such preparatory measures will be reimbursed to the operators by the National Emergency Supply Agency (NESA).

An amendment is being prepared which would specify the roles and authority of the Ministry of Transport and Communications and FICORA in detail, in accordance with the new Emergency Powers Act.

[35] Act on Television and Radio Operations (744/1998) (unofficial English translation). http://www.finlex.fi/fi/laki/kaannokset/1998/en19980744.pdf.

[36] Act on Provision of Information Society Services (458/2002) (unofficial English translation). http://www.finlex.fi/en/laki/kaannokset/2002/en20020458.pdf.

[37] Communications Market Act (393/2003) (unofficial English translation). http://www.finlex.fi/en/laki/kaannokset/2003/en20030393.pdf.

## Act on the Protection of Privacy in Electronic Communications 2004

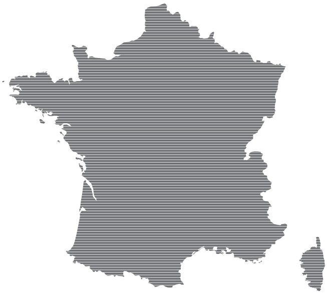
This Act (516/2004)[38] states that telecommunications operators or service providers must secure their services and inform the authorities about any violations. The operators or providers have the right to eliminate any programs that threaten information security. They may also limit or stop the traffic when necessary for the protection of information security.

The Amendment (198/2006)[39] obligates the operator also to transmit authority originated emergency SMS messages that are addressed to specified recipient groups.

[38] Act on the Protection of Privacy in Electronic Communications (516/2004) (unofficial English translation). http://www.finlex.fi/en/laki/kaannokset/2004/en20040516.pdf.

[39] http://www.finlex.fi/fi/laki/alkup/2006/20060198?search%5Btype%5D=pika&search%5Bpika%5D=198%2F2006.

# France



## Critical Sectors

All infrastructures that are vital to the maintenance of primary social and economic processes are considered critical sectors in France. These critical sectors are the following:[1]

- Finance,
- Industry,
- Energy,
- The work of the judiciary,
- Public Health,
- The work of national civil authorities,
- Electronic Communication, Audiovisual Media, and Information Technology,
- Transport Systems,
- Water Supply,

[*] The Country Survey of France 2008 was reviewed by Stanislas de Maupeou, SGDN – DCSSI – Sous-direction opérations Chef du CERTA.

[1] Decree No. 2006-212 dated 23 February 2006 on the protection of essential economic sectors. Information provided by an expert.

- Food,
- Space and Research,
- The Armed Forces.

A decree was issued in 2006 on the protection of essential economic sectors;[2] it aims to upgrade regulations pertaining to vulnerabilities by harmonizing the interagency state approach for analyzing hazards in terms of the nature of the threat, while expanding the list of issues to be taken into account and by including the flexible measures provided for within the framework of the Vigipirate plan.[3] Thus, each of the 12 essential economic sectors will include a national security directive for essential operators, who are in turn tasked with setting up their own operator security plan under the supervision of the ministry they are subordinated to; this plan is also intended for other major agencies to set up their own protection plans.

The French regulatory framework has been updated accordingly. Its approach is based on risk management and prevention / reaction plans. The national committee, the interdepartmental commission, and the defense and security delegates are encouraged to share information. The above-mentioned 12 sectors and the actors therein have to elaborate a national security directive, and all operators are instructed to refine the national security directive into an operator security plan for their specific context. For each critical point, the operators have to refine the operator security plan into particular protection plans, and the authorities are directed to elaborate an external protection plan.[4]

[2] Ibid.

[3] Vigipirate is France's national security alert system. Created in 1978, it has since been activated three times, in 1995, 2000, and 2004. For more information, see: http://www.archives.premier-ministre.gouv.fr/raffarin_version2/information/fiches_52/plan_vigipirate_50932.html.

[4] Information provided by an expert.

# Past and Present Initiatives and Policies

## Government Action Program for an Information Society (PAGSI)

In August 1997, the prime minister of France designated the information and communication society as a priority for government action. The objective was to build an information society for all, to prevent a digital divide, and to help France catch up with other countries in terms of internet usage. Making government services available online has been the main goal of the formation of the Government Action Program for an Information Society (PAGSI)[5] (adopted at the meeting of the Inter-ministerial Committee for Information Society (CISI) in January 1998).[6] In addition to the improvement of general public services, standardization, and training for civil servants, the action plan supported projects in the fields of education, culture, electronic commerce, and research and innovation, and established appropriate regulations for the safer use of information technologies and networks. Two of the main priorities of the action plan were managing the Security of Information Systems (SSI) and combating cyberthreats.[7]

## Expression of the Needs and Identification of Security Objects (EBIOS)

In 1997, the Central Information Systems Security Division (DCSSI) developed and published the first version of the guide Expression of the Needs and Identification of Security Objects (EBIOS). Since then, it has been regularly updated and expanded.[8] EBIOS outlines methodological tools for risk analysis concerning the security of information systems. The method allows for commu-

[5] http://www.education.gouv.fr/realisations/communication/samra.htm.

[6] http://www.internet.gouv.fr.

[7] Service d'Information du Gouvernement. "Four years of government measures to promote the information society" (August 2001).

[8] All consecutive versions are available on the site of the Prime Minister's Office. "Serveur thématique sur la sécurité des systèmes d'information". http://www.ssi.gouv.fr/fr/confiance/ebiospresentation.html.

nication about information systems security within organizations and between the individuals concerned. The methodological framework of EBIOS consists of tools for apprehending the method, for training, and for contributing to its shared development.[9]

## State Information System Security Reinforcement Plan (2004–2007)

The director of the French Prime Minister's Office instructed the ministerial departments and the General Secretariat of National Defense to prepare a specific plan of action by October 2003 to "secure the main central and local governmental networks, and those used for vital infrastructure management"[10]. This plan of action was approved on 16 December of the same year. The so-called "State Information System Security Reinforcement Plan" had the following four objectives:[11]

- To secure communication channels for senior state officials; that is, to ensure, under all circumstances, the security of all protected communication means for the use of senior authorities, based on supervision under the direct control of state authorities;
- To secure government information systems; that is, to secure the new e-government functions in accordance with the Agency for the Development of Electronic Administration's (ADAE)[12] strategic e-government plan and guidelines, and to explain security policies;
- To set up operational capabilities to respond to computer attacks;
- To include the French information system security policy within the scope of the French security policy in the EU.

[9] http://www.ssi.gouv.fr/fr/confiance/methodes.html.

[10] Prime Minister's Office. "State Information System Security Reinforcement Plan (2004–2007)" (10 March 2004). http://www.ssi.gouv.fr/site_documents/PRSSI/PRSSI-en.pdf.

[11] http://www.ssi.gouv.fr/fr/confiance/methodes.html.

[12] Agence pour le Dévéloppement de l'Administration Électronique (ADAE). See: Administration 24h/24. "le portail des démarches en ligne". http://www.administration24h24.gouv.fr.

## Plan RE/SO 2007

The Plan for a Digital Republic within the Information Society (Plan pour une République numérique dans la societé de l'information) was presented by the prime minister in 2002. Acknowledging the necessity and importance of information and communication technologies for French economic growth, employment, and overall "influence in the world", this plan aims at giving a new impetus to the information society by focusing on the efficient development and use of an ICT infrastructure. Specifically, it strives to simplify the rules governing the internet, to restore the trust of the users, and to clarify the responsibilities of all actors within the information society.[13]

## Defense and National Security Whitebook

In June 2008, French President Nicolas Sarkozy announced the most wide-ranging reform of the French armed forces since 1994. The Defense and National Security Whitebook (Défense et Sécurité nationale: Le Livre Blanc)[14] states that global terrorism poses the most virulent threat to the security of France and its citizens. The document outlines the French military strategy to face this challenge until 2020.[15] It not only anticipates a major reduction in the personnel strength of the armed forces, but also simultaneously foresees a substantial increase in their funding. Funding for military intelligence, for example, will be doubled. These funds are intended to be used to strengthen satellite surveillance and ICT in general in order to prevent cyber-attacks. France also plans to develop offensive means to prevent cyber-attacks. Under the terms outlined in the whitepaper, up to 10 000 troops will be dedicated to the prevention of pandemics induced by chemical and biological attacks, and of cyber-attacks. The Defense and National

[13] http://www.internet.gouv.fr/informations/information/plan_reso2007.

[14] Défense et Sécurité nationale LE LIVRE BLANC. Odile Jacob. La Documentation Française: Paris (June 2008).

[15] Neue Zürcher Zeitung. "Weniger Personal, mehr Geld für militärische Raumfahrt. Frankreichs Präsident Sarkozy präsentiert Pläne für den Umbau der Armee" (16 June 2008). http://www.nzz.ch/nachrichten/international/frankreich_sarkozy_armee_plaene_1.760795.html.

Security Whitebook is scheduled to be discussed in the French parliament in June 2008.[16]

## Organizational Overview

In France, the secretary-general of national defense (SGDN),[17] a secretary attached to the Prime Minister's Office, bears complete responsibility for organizing CIP.

Furthermore, within the Ministry of Defense, the key organizations responsible for CIP/CIIP are the Central Directorate for Information Systems Security (DCSSI),[18] the Inter-Ministerial Commission for the Security of Information Systems (CISSI),[19] and the Advisory Office, whereas the Central Office for the Fight Against Hi-Tech Crime plays a leading role within the Ministry of the Interior.

As a public-private partnership, the Strategic Advisory Board on Information Technologies (CSTI) strives to bring together government officials, business and industry executives, and representative of the research and development community.

### Public Agencies

#### Secretariat-General for National Defense (SGDN)

The secretary-general for national defense (SGDN) deals with national and international security affairs. The organization was first called into action with regard to information security for Y2K. A specific network of contacts among different bodies from the public and private sectors became involved under the

[16] Neue Zürcher Zeitung. "Frankreich fürchtet sich vor Cyber-Attacken. Aufklärung laut Verteidigungs-Weissbuch wichtigster Budgetposten" (17 June 2008). http://www.nzz.ch/nachrichten/international/frankreich_fuerchtet_sich_vor_cyber-attacken_1.761740.html.

[17] Secrétariat Général de la Défense Nationale: http://www.sgdn.gouv.fr/sommaire_en.php.

[18] Direction centrale de la sécurité des systèmes d'information (DCSSI).

[19] Commission Interministérielle pour la Sécurité des Systèmes d'Information (CISSI).

coordination of the SGDN. The SGDN is directly subordinated to the French prime minister and assists the prime minister's office in the co-ordination of the preparation, implementation, and follow-up of the government's decisions regarding defense and security policy, including the security of information systems.

The SGDN also promotes and co-ordinates the activities between ministries involved in CIIP. This includes responsibility for the security of information systems (since 1996) and chairing the CISSI, as well as responsibility for the protection of classified and sensitive military information. The SGDN deals with the impact of the scientific and technical revolution on defense and security policy, focusing on securitization of information and communication technology relating to military as well as civilian matters. In this area, the SGDN works closely together with DCSSI.

## Central Directorate for Information Systems Security (DCSSI)

The DCSSI was instituted by Decree No. 2001-693 of 31 July 2001[20] under the authority of the SGDN. It succeeded the Central Information Systems Security Division as the state's focal center for Information Systems Security.

The DCSSI has two main objectives: To guarantee the security of the information systems of the French state (including critical infrastructures in times of crisis); and to create a trusted environment to promote and facilitate the development of the information society. The DCSSI's principal missions are:[21]

- To contribute to interdepartmental and international definitions of governmental policy as regards information security;
- To serve as a national regulatory authority for information security by issuing approvals, guarantees, and certificates for national information systems, encryption processes, and products used by public bodies and services;

[20] http://www.ssi.gouv.fr/fr/dcssi/decretdcssicissi.html.

[21] http://www.cases.public.lu/fr/documentation/documents_de_reference/technique/index.html#1.

and by controlling information technology security evaluation centers (CESTI);
- To assist public services in information security (consult, audit, issue warnings, and conduct incident management, including crisis management);
- To develop scientific and technical expertise in the field of information security for the benefit of the administration and public services;
- To run training courses and increase awareness in information security (Information Systems Security Training Centre / CFSSI).

The DCSSI also administers the Security of Information Systems (SSI) website[22] and co-ordinates its activities. The SSI website comprises information on the Computer Emergency Response Team (CERTA),[23] information on regulation, certification, authorization, electronic signatures, and cryptography, and provides technical advice.

### Information Systems Security Training Center (CFSSI)

Attached to DCSSI, the Information Systems Security Training Center's (CFSSI)[24] objectives are to increase awareness on information systems security and to train experts capable of designing, evaluating, and making recommendations on the following aspects of information systems security:

- Communications security,
- Protection against compromising viruses,
- Computer security.

The CFSSI continues training actions undertaken by the CESSSI (Center for Training and Advanced Studies on Information Systems Security) since 1986.

[22] Sécurité de Systèmes d'Information: http://www.ssi.gouv.fr/en/index.html.

[23] Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques Informatiques. http://www.ssi.gouv.fr/fr/index.html.

[24] Centre de formation à la sécurité des systèmes d'information. http://www.ssi.gouv.fr/en/formation.html.

It will become the central player in a network designed to increase awareness on information systems security problems and provide training in the various aspects of this area, for the benefit of all government authorities.

The CFSSI also develops partnerships with higher education and further training centers. The activities of the CFSSI and the education it provides are controlled and monitored by an improvement committee chaired by the secretary-general for national defense and composed of civil servants and military staff.

## Operational Center (COSSI)

In order to defend governmental networks and information systems, the SGDN runs the Information System Security Operation center (COSSI) which, in addition to its general preventive tasks, coordinates the action of ministries and draws up protection and reaction measures. The centre also prepares and implements the Vigipirate plan against terrorist threats. COSSI operates around the clock, 365 days a year.[25]

## Central Office for the Fight Against Hi-Tech Crime

In May 2000, the Ministry of the Interior opened the Central Office for the Fight against Cyber-Crime.[26] It co-operates with Interpol and deals with unauthorized intrusions and crime in the field of information and communication technologies and supports legal investigations in this field. The Central Office has nationwide jurisdiction in this matter and works closely together with the national police as well as the private sector. It provides assistance to all agencies responsible for fighting computer crime, such as the police and gendarmerie, and sensitizes the actors.

[25] Information provided by an expert.

[26] Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (L'O.C.L.C.T.I.C.). http://www.securiteinfo.com/legal/OCLCTIC.shtml. See also: http://www.interieur.gouv.fr/sections/contact/police/questions-cybercriminalite/view.

## Public-Private Partnerships

### Strategic Advisory Board on Information Technologies (CSTI)

The Strategic Advisory Board on Information Technologies (CSTI)[27] was created in July 2000 at a meeting of the government committee on the Information Society. It is chaired by the French prime minister. The CSTI is composed of business and industry executives and leading representatives of the research and development community. It is responsible for recommendations to government concerning CIIP topics and the French contribution to the 6th European Framework Research and Development Program. The CSTI, in particular, has the following duties:[28]

- To communicate opinions and recommendations to the government on the studies and documents commissioned;
- To maintain a permanent dialog with representatives of industry and to improve co-ordination between private and public researchers (and the industry);
- To define national priorities and to select areas where more action is required;
- To provide general monitoring and warning services in the area of CIIP.

# Early Warning and Public Outreach

## Computer Emergency Response Teams (CERTs)

In France, there are three different Computer Emergency Response Teams (CERTs), and each of them addresses a different constituency: CERT-RENATER, CERTA, and CERT-IST.

[27] Conseil Stratégique des Technologies de l'Information: http://www.csti.pm.gouv.fr/.

[28] http://www.csti.pm.gouv.fr/uk/enbref.html.

- CERT-RENATER,[29] founded in 1993, specifically addresses research centers and academic institutions. CERT-RENATER gathers and provides information about information security and is dedicated to the membership of GIP[30] RENATER, the National Network of Telecommunications for Technology, Education, and Research;
- The Computer Emergency Response Team CERTA[31] has been hosted by DCSSI since 2000. CERTA deals in particular with the French administration services. As a center of expertise, it evaluates CIIP threats and gives advice, issues warnings, and provides information on how to prevent, respond to, and handle an attack against information systems. High-level staff, mainly engineers, work at CERTA. The CERTA is part of the Central Directorate for the Security of Information Systems (DCSSI) and acts as the technical cell of the permanent operational center (ITSOC) operating around the clock, seven days a week. CERTA is also the expertise cell from COSSI;[32]
- CERT-IST (CERT-Industry, Services, and Tertiary) was launched in 1999 by Alcatel (a telecom company), CNES (the French Space Agency), France Telecom, and the TotalFinaElf energy group. It serves France's private sector as a contact point for security incident response. CERT-IST provides alerts and means of protection against computer attacks aimed at French enterprises. It also helps the association members with incident handling.[33] CERT-IST interacts with the French national security organizations SGDN and DCSSI, in conjunction with CERT-RENATER and CERTA.[34]

[29] Réseau National de Télécommunications pour la Technologie, l'Enseignement et la Recherche. http://www.renater.fr, For CERT-Renater in particular, see: http://www.renater.fr/spip.php?rubrique19.

[30] Groupement d'Intérêt Publique (Public Interest Group).

[31] Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques Informatiques. http://www.certa.ssi.gouv.fr/.

[32] Information provided by an expert.

[33] http://www.cert-ist.com/.

[34] RAND Europe. Dependability Development Support Initiative (DDSI). "National Dependability Policy Environments, France" (November 2002), p. 7, http://www.ddsi.org/htdocs/Documents/final%20docs/DDSI_Country_Reports_Final_France.pdf.

### Web portal for citizens and SMEs

In the wake of a prime ministerial decision to bring security to citizens and small and medium enterprises, the DCSSI has built a web portal dedicated to enduser computer security.[35]

The prime minister's decision, which the portal serves to promote, consists of four main points:

- To coordinate the existing initiatives such as "internet sans crainte" (internet without fear);
- To keep citizens and SMEs informed about risks, recommendations, workarounds, and best practices;
- To alert citizens and SMEs when needed, and to provide timely and relevant information;
- To build and foster a contact network around the country.

## Law and Legislation

### Penal Code 2004

Amended as Law no.2004-575 of 21 June 2004, entered into force on 23 June 2004.

- Article 323-1: Fraudulent accessing or remaining within all or part of an automated data processing system is punishable by a sentence not exceeding two years' imprisonment and a fine. Where this behavior causes the suppression or modification of data contained in that system, or any alteration of the functioning of that system, the sentence shall not exceed three years' imprisonment and a fine.

[35] http://www.securite-informatique.gouv.fr.

- Article 323-2: Obstruction or interference with the functioning of an automated data processing system is punished by a sentence not exceeding five years' imprisonment and a fine.
- Article 323-3: The fraudulent introduction of data into an automated data processing system or the fraudulent suppression or modification of the data that it contains is punished by a sentence not exceeding five years imprisonment and a fine.
- Article 323-3-1: Fraudulently, and without legitimate motive, importing, holding, offering, selling or making available any equipment, tool, computer program or any data designed or particularly adapted to commit one or more offences provided for by articles 323-1 to 323-3, is punishable by the sentences prescribed for offences in preparation or the one that carries the heaviest penalty.[36]

Moreover, France ratified the Council of Europe Convention on Cybercrime on 10 January 2006.

[36] http://www.cybercrimelaw.net/laws/countries/france.html.

# Germany

## Critical Sectors

The main assumption underlying CIP/CIIP in Germany is that both the government and society as a whole depend heavily on a secure infrastructure. Organizations or facilities whose failure or impairment would cause a sustained storage of supplies, significant disruptions of public order, or other dramatic consequences for large parts of the population are defined as critical. According to the German constitution, it is the state's task to guarantee public security and order and to ensure that the population is provided with essential goods.

The following are the infrastructure sectors defined as critical in Germany:[1]

- Transportation and Traffic,
- Energy,
- Hazardous Materials,

* The Country Survey of Germany 2008 was reviewed by Susanne Jantsch, consultant, and Monika John-Koch Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK).

[1] http://www.bsi.bund.de/english/topics/kritis/kritis_e.htm, and http://www.bbk.bund.de/cln_027/nn_1048112/EN/02__themes/05__critical-infrastructures/01__sectors-start/sectors__node.html__nnn=true.

- Telecommunications and Information Technology,
- Financial, monetary and insurance systems,
- Supply (including water supply, food supply, healthcare, emergency and rescue services),
- Government Agencies, Administration, and Justice,
- Media, research facilities, cultural property.

## Past and Present Initiatives and Policies

In the past ten years, many activities have been undertaken that were directly or indirectly related to the issue of critical infrastructure protection. They emerged from inter-ministerial activities begun in 1997 at the initiative of the Federal Minister of the Interior, motivated in part by the study produced by the US President's Commission on Critical Infrastructure Protection (PCCIP). The events of 11 September 2001 added urgency to ongoing efforts and, as part of the campaign against terrorism, contributed to widening the scope of national activities and intensifying the international dialog.

In 2005, two key documents were presented:

- The National Plan for Information Infrastructure Protection (NPSI),[2] enacted by a cabinet decision of the federal government, and

[2] Federal Ministry of the Interior. "National Plan for Information Infrastructure Protection" (Berlin, 2005). http://www.bmi.bund.de/cln_012/nn_148138/Internet/Content/Common/Anlagen/Nachrichten/Pressemitteilungen/2005/08/National__Plan__for__Information__Infrastructure__Protection,templateId=raw,property=publicationFile.pdf/National_Plan_for_Information_Infrastructure_Protection.

- The Protection of Critical Infrastructures – Baseline Protection Concept[3], followed by the Protecting Critical Infrastructures – Risk and Crisis Management. A Guide for Companies and Government Authorities[4] in 2008.

These documents can be considered as initial milestones for a number of activities for establishing both CIIP and CIP processes throughout the country.

## AG KRITIS

Initiated by the PCCIP report in the US, an inter-ministerial working group on critical infrastructures (AG KRITIS) was established in 1997 by the Federal Minister of the Interior. It consisted of the ministerial representatives, a steering committee, and a permanent office at the Federal Office for Information Security (BSI). The mandate of AG KRITIS was to:

- Describe possible threat scenarios for Germany;
- Conduct a vulnerability analysis of Germany's crucial sectors;
- Suggest countermeasures;
- Sketch an early-warning system.

The work of AG KRITIS[5] was an important basis for all further activities of public agencies in Germany.

[3] Federal Ministry of the Interior. "Protection of Critical Infrastructures – Baseline Protection Concept" (Berlin, 2005). http://www.bmi.bund.de/nn_121894/Internet/Content/Common/Anlagen/Broschueren/2007/Basisschutzkonzept__kritische__Infrastrukturen__en,templateId=raw,property=publicationFile.pdf/Basisschutzkonzept_kritische_Infrastrukturen_en.pdf.

[4] Federal Ministry of the Interior. "Protecting Critical Infrastructures – Risk and Crisis Management. A Guide for Companies and Government Authorities" (Berlin, 2008). http://www.bmi.bund.de/Internet/Content/Common/Anlagen/Broschueren/2008/Leitfaden__Schutz__kritischer__Infrastrukturen__en,templateId=raw,property=publicationFile.pdf/Leitfaden_Schutz_kritische r_Infrastrukturen_en.pdf.

[5] The report of AG KRITIS was, however, never published. A draft version in German can be found at. http://userpage.fu-berlin.de/~bendrath/Kritis-12-1999.html.

## Situational Analysis of Threats and Hazards / CIP-Initiatives

CIP/CIIP activities were intensified after the events of 11 September 2001. The need for more coordinated CIP efforts was underpinned by lessons identified after the floods of the Danube, Oder, and Elbe rivers in the following years. The following sections provide summaries of CIP-related reports, recommendations, and activities. CIIP-related initiatives and reports are described in the next section.

### Comprehensive Report on Threats and Hazards

In March 2006, the Ministry of the Interior published a second comprehensive threat analysis for Germany.[6] The IT section in this report is founded on previous reports and continues to answer questions identified by the AG KRITIS work. Together with other national assets, information security is defined as crucial for the security of the German society and for the success of its economy.

### Kirchbach Report

The Kirchbach Commission, established in Saxony after the devastating flood of 2002, analyzed the overall structure of the German emergency protection system. Besides the focus on the flood disaster, the Kirchbach report provided a comprehensive analysis of existing facilities and recommendations for future capacities to secure information and communications technology in cases of emergency.[7] This disaster and the conclusions of the Kirchbach report triggered a broad range of measures in several ministries and agencies.

[6] Federal Ministry of the Interior. "Dritter Gefahrenbericht der Schutzkommission beim Bundesminister des Innern. Bericht über mögliche Gefahren für die Bevölkerung bei Großkatastrophen und im Verteidigungsfall" (Bonn, 2006). English summary: http://www.bbk.bund.de/cln_027/nn_529818/Schutzkommission/DE/03__Publikationen/01__Gefahrenberichte/Summary_203._20GB_20englisch.html.

[7] Bericht der Unabhängigen Kommission der Sächsischen Staatsregierung. Flutkatastrophe 2002 (2nd ed., 2003). http://home.arcor.de/schlaudi/Kirchbachbericht.pdf.

### Critical Infrastructure Protection – Baseline Protection Concept

The CIP baseline protection concept was developed in close cooperation between the Federal Ministry of the Interior (BMI), the Federal Office of Civil Protection and Disaster Assistance (BBK), the Federal Criminal Police Agency (BKA), and the private sector. It provides guidance for the analysis of potential hazards such as terrorist attacks, criminal acts, and natural disasters, as well as recommendations for companies on adequate protective measures.[8]

### Protecting Critical Infrastructures – Risk and Crisis Management. A Guide for Companies and Government Authorities

The CIP baseline protection concept was complemented by a guideline Protecting Critical Infrastructures – Risk and Crisis Management. A Guide for Companies and Government Authorities,[9] which was published in December 2007 and presented in January 2008. This guideline provides methods to support the implementation of risk management and crisis management in enterprises and government organizations and offers checklists and examples.

## CIIP Initiatives

As already mentioned, the attacks in the US on 11 September 2001 lead to a considerable intensifying of activities in the area of CIIP as well.

[8] Federal Ministry of the Interior. "Protection of Critical Infrastructures – Baseline Protection Concept", op. cit.

[9] Federal Ministry of the Interior. "Protecting Critical Infrastructures – Risk and Crisis Management. A Guide for Companies and Government Authorities", op.cit.

## CIIP at the BSI

After 2001, several departments at the Federal Office for Information Security (BSI) were expanded and given additional tasks to support critical information infrastructure protection.

On its website, the BSI regularly updates information and practical advice on critical infrastructures.[10]

In mid-2002, BMI and BSI commissioned a series of systematic infrastructure analysis studies on the influence of ICT on the CI sectors. The results of these studies, though unpublished, induced a number of further activities both in intensifying the dialog between public and private sectors and in developing and implementing CIIP-related strategies and policies, as described in the following subsections.

## National Plan for Information Infrastructure Protection (NPSI)

The National Plan for the Protection of Information Infrastructures (NPSI), issued in 2005, is the federal government's umbrella strategy for a comprehensive approach to the protection of ICT and ICT-dependent assets.[11] It aims at strengthening IT security in the nation's IT-dependent infrastructures and at enabling swift responses to IT-related crises.

The NPSI pursues three strategic objectives:

- Prevention – protecting information infrastructures adequately;
- Preparedness – responding effectively to IT security incidents;
- Sustainability – enhancing German competence in IT security and setting international standards.

[10] http://www.bsi.bund.de/fachthem/kritis/index.htm (German) and http://www.bsi.bund.de/english/topics/kritis/kritis_e.htm (English).

[11] Federal Ministry of the Interior. "National Plan for Information Infrastructure Protection", op. cit.

This strategy addresses public authorities as well as businesses and individuals. The NPSI announced two implementation plans, one for the federal administration and one for critical infrastructures, both of which were finalized in 2007.[12] By cabinet decision, the implementation plan for the federal administration presents a mandatory IT security guideline. Implementing the designated measures will ensure a high level of IT security throughout the federal administration in a mid- to long-term perspective.

## CIP Implementation Plan

The CIP implementation plan[13] was prepared in close cooperation between representatives of critical infrastructure operators and service providers as well as experts from the federal administration. The plan aims at implementing measures that make it possible to bring the goals of operators in the private industry in line with the higher-level (safeguarding) interests of the community.

The plan addresses the need for measures that meet security requirements extending beyond the security and business continuity responsibilities within the enterprises, as well as the aim of encouraging industries to scrutinize their own security and risk management approaches.

This implementation plan also introduces a roadmap to the future: the following topics will be pursued in direct follow-up activities:

- Emergency and crisis exercises;
- Crisis response and management;
- Maintaining critical infrastructure services;
- National and international cooperation.

[12] See press release (in German): http://www.bmi.bund.de/cln_012/nn_122688/sid_805F7477F227F34F95AFF8D45906FAD9/Internet/Content/Nachrichten/Pressemitteilungen/2007/09/IT__Sicherheit.html.

[13] Federal Ministry of the Interior. "Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen" (Berlin 2007). http://www.bmi.bund.de/cln_012/nn_122688/Internet/Content/Broschueren/2007/Kritis.html, currently only available in German, English version in preparation.

In future there will be regular reporting on progress and results, as well as updates of the implementation plan in response to progress and changes in the IT and threat environment.

### IT and Internet Security Situation in Germany

In order to provide general information on the IT security and internet security situation in Germany, the BSI started to publish a report on the IT Security Situation in Germany in 2005 (with a second edition following in 2007), which provides a survey of current threats to information and information systems, of the challenges to be met in order to secure information infrastructures, and of trends related to new information technologies and evolving threats. Furthermore, the BSI has started to issue a quarterly summary of the internet threat situation in 2007.[14]

### IT Security Guidelines

The IT Security Guidelines published by the BSI are intended to satisfy the needs of small and medium-sized businesses, summarizing the most important IT security measures in a compact overview that is intelligible to the non-expert. The focus is on organizational safeguards and on illustrating threats through practical examples.[15]

## E-Government Initiatives

The German e-Government initiative[16] aims to use modern information and communications technologies consistently in order to make administrative processes more efficient, and to facilitate an exchange between the business community, the public, and the administration. In short: e-Government should ensure that

[14] See http://www.bsi.bund.de/literat/lagebericht/index.htm.

[15] Federal Office for Information Security (BSI). "IT Security Guidelines: IT Baseline Protection in Brief" (Bonn: 2004). http://www.bsi.bund.de/english/gshb/guidelines/guidelines.pdf.

[16] http://www.kbst.bund.de/nn_836956/Content/Egov/egov.html__nnn=true.

each agency within the federal administration  is just one mouse click away for the citizen.

The BundOnline 2005 initiative – to make all suitable government services of the federal administration available to the public through the internet – was successfully concluded in August 2005.[17] The BSI had been tasked with developing the basic IT security components and with setting up the data security competence center. The BSI also published the e-Government Manual[18] covering all aspects of secure e-Government and presenting pragmatic approaches. In September 2006, the federal government initiated the E-Government 2.0 program for the further enhancement of e-Government services until 2010.[19]

As a related activity, Germany Online is the national e-government strategy pursued by the federal government, governments of federal states, and municipal administrations, initiated in 2003.[20] The goal was to establish a secure communications network for the entire German administration, and particularly for communication between the different state levels, i.e., the municipalities, the states, and the federal government. In June 2006, Chancellor Angela Merkel, together with the heads of the federal states' governments, adopted the Action Plan Germany Online, which was extended in June 2007.[21] Among the six prioritized projects, the establishment of the communications infrastructure is the most relevant one from a CIIP perspective.21

[17] For the final report, see http://www.kbst.bund.de/cln_012/nn_945224/SharedDocs/Publikationen/Oeffentlichkeitsarbeit/Umsetzungsplan/current_20status_20and_20outlook__2006,templateId=raw,property=publicationFile.pdf/current%20status%20and%20outlook_2006.pdf.

[18] http://www.e-government-manual.de.

[19] http://www.kbst.bund.de/cln_012/nn_836958/Content/Egov/Initiativen/EGov2/EGov2.html__nnn=true.

[20] http://www.kbst.bund.de/cln_028/nn_839178/Content/Egov/Initiativen/D__online/d__online.html__nnn=true and http://www.deutschland-online.de/DOL_en_Internet/broker.jsp.

[21] See download section under http://www.deutschland-online.de/DOL_en_Internet/broker.jsp.

## International Collaboration

A joint initiative of the German Ministry of the Interior[22] and the US Department of Homeland Security[23] at the ministerial level in 2003 laid the groundwork for cooperation in several CIIP-related activities.[24] Among others, both parties agreed to foster regular consultations in international organizations in order to enhance multilateral cooperation. This bilateral initiative complements the already ongoing counter-terrorism efforts. As a mid-term result, the International Watch and Warning Network (IWWN) has been established, currently involving 15 participants from all continents.

Multilateral conferences such as the International Watch, Warning and Incident Response Workshop held in Berlin in October 2004, the International Watch and Warning Network Conference in Washington, D.C. in June 2006 (both co-hosted by the US and Germany), or the European IT security conference Innovation and Responsibility in Berlin during the German EU presidency 2007, with one of the six tracks dedicated to CIIP, have contributed to the development and improvement of methods for multinational cooperation. Furthermore, Germany is actively participating in efforts aimed at bringing forward the European Programme for Critical Infrastructure Protection (EPCIP).[25] Germany's international CIIP activities also include participation in CIIP-relevant projects and working groups, such as the European SCADA and Control Systems Information Exchange (E-SCSIE).[26]

Moreover, Germany participates in efforts to identify, develop, and share CIIP good practice recommendations, e.g., the "Best Practices for Improving CIIP in Collaboration of Governmental Bodies with Operators of Critical Information Infrastructures" currently being discussed by the G8 High-Tech Crime Subgroup (HTCSG).

[22] http://www.bmi.bund.de.

[23] http://www.dhs.gov/index.shtm.

[24] Federal Ministry of the Interior (BMI). Schily und Ridge vereinbaren Kooperation beim Schutz von Computersystemen. (13 June 2003). http://www.bmi.bund.de/cln_028/nn_122688/Internet/Content/Nachrichten/Archiv/Pressemitteilungen/2003/06/Schily__und__Ridge__vereinbaren__Kooperation__Id__92348__de.html.

[25] See http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm.

[26] https://espace.cern.ch/EuroSCSIE/default.aspx.

## Organizational Overview

Overall responsibility for, and coordination of, major CIP- and CIIP-related activities rests with the Federal Ministry of the Interior (BMI), together with several of its subordinated agencies, such as the Federal Office for Information Security (BSI),[27] the Federal Office of Civil Protection and Disaster Assistance (BBK),[28] the Federal Criminal Police Agency (BKA),[29] and the Federal Police (BPOL).[30] For coordination within the ministry and the subordinated agencies, a task force for critical infrastructure protection (AG KRITIS) was established at the BMI in 2002. Strategy development and implementation are also coordinated with other federal ministries, especially the Federal Ministry of Economics and Technology,[31] the Federal Chancellery,[32] the Federal Ministry of Justice, the Federal Ministry of Foreign Affairs, the Federal Ministry of Defense, and other relevant agencies, such as the Federal Network Agency.[33] Furthermore, strategic partners from the private sector are consulted.

### Public Agencies

#### Federal Ministry of the Interior (BMI)

As the government agency responsible for ensuring Germany's internal security, the Federal Ministry of the Interior (BMI) is closely involved with CIP/CIIP. This agency deals with and coordinates the relevant topics, such as physical protection within the context of civil protection and disaster response, threat prevention within the context of law enforcement, and all areas of IT and IT dependence. The authority in charge of IT-related issues with regard to CIIP is

[27] "Bundesamt für Sicherheit in der Informationstechnik". http://www.bsi.bund.de.

[28] "Bundesamt für Bevölkerungsschutz und Katastrophenhilfe". http://www.bbk.bund.de.

[29] "Bundeskriminalamt". http://www.bka.de.

[30] "Bundespolizei". http://www.bundespolizei.de/cln_049/DE/Home/home__node.html?__nnn=true.

[31] http://www.bmwi.de/English/Navigation/root.html.

[32] "Bundeskanzleramt". http://www.bundeskanzlerin.de/Webs/BK/DE/Homepage/home.html.

[33] "Bundesnetzagentur". http://www.bundesnetzagentur.de/enid/6c28cf7e908c093de1d8973191d1ed59,0/xn.html.

Division IT 3 (Information Technology Security) under the Federal Ministry of the Interior's Chief Information Officer.[34] Responsibility for CIP resides with Division KM 4 (Critical Infrastructure Protection).[35]

## The Federal Office for Information Security (BSI)

The Federal Office for Information Security (BSI), one of the agencies under the Federal Ministry of the Interior, plays an especially important role in CIIP. The BSI deals with all areas related to security in cyberspace and takes preventive action by analyzing IT weaknesses and developing protective measures, including the following:

- Security of applications and critical infrastructures,
- Security of networks (including CERT Bund, IT situation center, and IT crisis management center, and early warning systems),
- Cryptographic technology,
- New technologies (e.g., biometrics, RFID).

The BSI investigates security risks associated with the use of IT and develops preventive security measures. It provides information on risks and threats relating to the use of information technology and develops appropriate solutions. This work includes IT security testing and assessment of IT systems, including their development, in co-operation with industry. It also analyses developments and trends in information technology. The BSI's services address a broad audience: the federal administration as well as manufacturers, distributors, and private users of information technology.[36]

Of special relevance in the CIIP context is the CERT-Bund 24-h on-call availability for the federal administration, and the operation of the IT situation center, where the IT threat situation is assessed on a continuous basis.[37]

[34] http://www.bmi.bund.de/Internet/Content/Ministerium/Organigramm__Neu/Referate/it-stab__engl.html.

[35] http://www.bmi.bund.de/Internet/Content/Ministerium/Organigramm__Neu/Referate/abteilung__km__engl.html.

[36] http://www.bsi.de/english/functions.htm.

[37] See also the chapter on Early Warning and Public Outreach.

## Federal Office of Civil Protection and Disaster Assistance (BBK)

The Federal Office of Civil Protection and Disaster Assistance (BBK) was established on 1 May 2004 under the Federal Ministry of the Interior.[38] One of the main functions of this agency is information-sharing and resource allocation between the different levels of public authority in case of emergencies.

The BBK has a special focus on CIP.[39] It operates in close cooperation with the BSI and the Federal Network Agency (Bundesnetzagentur) in the field of CIIP. Moreover, contingency plans and appropriate measures are being developed according to case studies.[40]

The BBK established the German Emergency Preparedness Information System (deNIS) as a special service for public authorities, emergency responders, and the general public.[41] For the public, deNIS provides general information about organizations and potential emergencies, and offers web links on emergency precaution and preparedness. For a closed user group of emergency responders and crisis management professionals, a secure and classified system called deNIS IIplus has been established.[42]

Furthermore, on 1 October 2002, the Joint Reporting and Situation Center (Gemeinsames Melde- und Lagezentrum, GMLZ) took up operation with the objective of enhancing cooperation between federal, state, and local authorities as well as national, international, and supranational organizations in situations of severe damage and hazards. The tasks include continuous situation assessment; the receipt, acquisition, analysis, processing, coordination, and dissemination of information; and forecasts of damage progression in case of events.

[38] http://www.bbk.bund.de/cln_007/nn_402322/EN/00__Home/homepage__node.html__nnn=true.

[39] The BBK's main CIP-related output have been the publications on "Critical Infrastructure Protection – Baseline Protection Concept" and "Protecting Critical Infrastructures – Risk and Crisis Management. A Guide for companies and government authorities.

[40] http://www.bbk.bund.de/cln_027/nn_398882/DE/02__Themen/06__SchutzKritischerInfrastrukturen/01 __Themen/02__InformationstechnikundTelekommunikation/InformationstechnikundTelekommunikation__node.html__nnn=true.

[41] http://www.bbk.bund.de/cln_007/nn_398880/DE/02__Themen/05__Krisenmanagement/01__deNIS/deNIS __node.html__nnn=true, http://www.denis.bund.de.

[42] http://www.bbk.bund.de/cln_007/nn_401142/DE/02__Themen/05__Krisenmanagement/01__deNIS/02 __deNISII/deNISII__node.html__nnn=true.

International request for emergency support from Germany will be handled through GMLZ.

## The Federal Criminal Police Agency (BKA)

The Federal Criminal Police Agency (BKA)[43] is responsible in the first instance for prosecuting crimes against the internal or external security of the Federal Republic of Germany and crimes involving damage to or the destruction of critical infrastructures that could result in a serious threat to life, health, or the functioning of society. Further, the BKA is the central agency for investigating crimes involving information and communications technology.

## Federal Ministry of Economics and Technology (BMWi)

With roughly 85 per cent of Germany's critical infrastructure being privately owned, the Federal Ministry of Economics and Technology (BMWi)[44] also plays a role, as its brief includes economic policy on the one hand, but also oversight over several CI sectors on the other (through the Federal Network Agency, see below). With regard to the energy sector, one of the BMWi's tasks is developing the framework for securing the energy supply. According to Article 87f of the German constitution, the BMWi is also responsible for ensuring the availability of adequate telecommunications infrastructure and services.

## Federal Network Agency

In July 2005, the Regulatory Authority for Telecommunications and Posts was renamed the Federal Network Agency for Electricity, Gas, Telecommunications, Post, and Railway. The Federal Network Agency is a higher federal authority within the scope of business of the Federal Ministry of Economics and Technology. The Federal Network Agency's task is to provide, by liberalization and deregulation, for the further development of the electricity, gas, telecommunica-

[43] http://www.bka.de.

[44] http://www.bmwi.de.

tions, and postal markets and, as of January 2006, of the railway infrastructure market as well.[45]

### Other ministries involved

The Federal Ministry of Justice (BMJ)[46] is responsible for relevant legislation, in particular for ensuring that national laws comply with relevant EU legislation such as the EU Council Framework Decision on attacks against information systems.[47].

The Federal Ministry of Defense (BMVg)[48] is involved in the context of its responsibility for national defense and for maintaining troop readiness and performance.

The Federal Chancellery plays a coordinating role at the ministerial level. Additional ministries with specific areas of responsibility are also involved in CIP.

Responsibilities are also shared among the agencies within the remit of the various ministries. The Federal Intelligence Service (Bundesnachrichtendienst, BND) and the Federal Office for the Protection of the Constitution (Bundesamt für Verfassungsschutz, BfV) provide important information regarding the threat situation and possible domestic targets.

## Public-Private Partnerships

### CIP Implementation Plan

The latest example of public-private cooperation was the development of the CIP implementation plan (see chapter on Past and Present Initiatives and Policies), followed by a set of ongoing activities to actually implement measures.

[45] http://www.bundesnetzagentur.de/enid/0a888f9d9a85f3748b2d8fb635f752e7,0/xn.html.

[46] http://www.bmj.bund.de/enid/4e02aa38526e9a3069072ac5fa5dbc01,0/aktuelles_13h.html.

[47] Official Journal of the European Union, L 69/67-71, 16 March 2005, http://eur-lex.europa.eu/JOHtml.do?uri=OJ:L:2005:069:SOM:en:html.

[48] http://www.bmvg.de/portal/a/bmvg.

## Germany Secure in the Web Campaign

The campaign Germany Secure in the Web (Deutschland sicher im Netz, DsiN)[49] is an initiative undertaken under the auspices of the Federal Minister of the Interior. Members include private enterprises as well as associations and non-profit organizations. Its main objective is to improve the security of both private and commercial IT users, to provide private users and small and medium-sized enterprises with a sound basis of information that encourages the use of, and confidence in, the internet and internet-based services, and to raise awareness of all relevant IT security issues. The association also targets children and adolescents specifically, with the objective of raising their awareness and that of their parents of IT-security related issues, but also to protect them from, and prevent them from accessing, criminal and abusive contents.

## Initiative D21

Launched in 1999, Initiative D21[50] is the largest public-private partnership in Germany. This economic initiative also deals with information security. Initiative D21 is a neutral platform, independent of party allegiance and of individual industrial sectors. D21 has more than 200 participants from enterprises, associations, parties, political institutions, and other organizations. Initiative D21 pursues a steadily growing number of projects. Initiative D21 is organized into three subject areas (steering groups):

- Digital Integration,
- Digital Competence,
- Digital Excellence.[51]

[49] https://www.sicher-im-netz.de/default.aspx?.
[50] http://www.initiatived21.de/en/English.104.0.html.
[51] Ibid.

## Early Warning and Public Outreach

### CERT-Bund

The CERT-Bund unit was established on 1 September 2001 at the Federal Office for Information Security (BSI). CERT-Bund is a central contact point charged with protecting the security of data processes and networks of the federal public administration. CERT-Bund also offers some of its services to clients from the private sector. However, several services are only available to the federal administration (e.g., incident response).[52] CERT-Bund's main tasks include warning and information-sharing, data collection, analysis and processing of information, documentation and dissemination, sensitization of IT decisionmakers, and cooperation with existing CERTs.[53]

### CERT-Network

The CERT-Verbund (CERT Network) is an alliance of German security and computer emergency teams.[54] The alliance provides a common base for cooperation between the teams and also allows the pursuit of the overarching objectives, namely to ensure the protection of national IT networks or to prepare for swift and coordinated reaction in case of larger IT security incidents.

### IT Situation Center

The IT Situation Center collects, assesses, and summarizes information on the IT situation in Germany as a continuously updated situational picture. The processes of gathering information and establishing an information exchange in cooperation with relevant partners, e.g., from critical infrastructures, are constantly being further developed. Procedures are emerging to share assessment

[52] Günther Ennen. "CERT-Bund – eine neue Aufgabe des BSI". In: KES Zeitschrift für Kommunikations- und EDV-Sicherheit. Bundesamt für Sicherheit in der Informationstechnik (BSI), (Bonn, June 2001), p. 35. See also http://www.bsi.bund.de/certbund/index.htm.

[53] Ennen, "CERT-Bund – eine neue Aufgabe des BSI", op. cit., p. 35.

[54] http://www.cert-verbund.de/index.html.

results, including alerts and warnings, in a target-oriented way with a variety of audiences, including government agencies, critical infrastructure operators, and the general public.[55]

## IT Crisis Response Center

To be prepared for national crisis situations affecting information infrastructures, Germany has established an IT Crisis Response Center as a non-standing organization located at the BSI, closely related to the IT situation center. Situational crisis indicators will activate IT crisis response functions to warn and alarm potentially affected parties and to develop countermeasures. Moreover, the center supports a coordination board for the IT security of the federal ministries in organizing timely responses to minimize and to contain damage, and to return swiftly to the safe and secure operation of affected information infrastructures.[56]

## Services for Citizens and SMEs

### Citizens' CERT (Bürger-CERT)

The Citizens' CERT[57] project aims at informing and warning citizens and small enterprises of the threats stemming from worms, viruses, and security loopholes in IT systems not only rapidly and competently, but also from an explicitly neutral perspective and at no cost. The Citizens' CERT project was initiated jointly by the BSI and Mcert[58] in 2006. Since June 2007, Citizens' CERT has been maintained exclusively by the BSI. Every citizen can subscribe to the services of the Citizens' CERT project, which include technical warnings, a bi-weekly newsletter, and special editions of the newsletter. Thus, the project aims to make as many people as possible aware of the issues the importance of IT security.[59]

[55] Information provided by an expert.

[56] See "The IT Security Situation in Germany 2007", op. cit., section 7.3.

[57] https://www.buerger-cert.de.

[58] Mcert began as a CERT for SMEs in 2003 and suspended its services in June 2007, with key tasks being continued by Citizens' CERT and the initiative "Germany Secure in the Web" (see above).

[59] http://www.buerger-cert.de/ueberuns.aspx.

For general information on IT security, there is a direct link to the website "BSI for the Citizen".

### BSI for the Citizen

The internet service "BSI for the citizen"[60] aims at providing easy-to-understand background information on IT security and the internet. The service offers guidance on how to surf the internet and use internet-based applications securely. For up-to-date warnings on new internet threats and a newsletter, users can follow a direct link to the Citizens' CERT webpage, which serves as a warning and information service for citizens.

## Law and Legislation

### Telecommunications Act

First enacted in 1996, this act was revised in 2004 and last amended in 2007.[61] Its purpose is to provide legal provisions for the liberalization and deregulation of the telecommunications market.

### Telecommunications and Media Act 2007

The Information and Telecommunications Services Act (Informations- und Kommunikationsdienste-Gesetz, IuKDG) of 1997[62] was the starting point for the liberalization of the German telecommunications market.[63] The IuKDG and

[60] Ibid.

[61] http://www.gesetze-im-internet.de/tkg_2004/BJNR119000004.html.

[62] Informations- und Kommunikationsdienste Gesetz (IuKDG). http://www.artikel5.de/gesetze/iukdg.html#fn.

[63] Interview with a representative of the consulting company Industrieanlagen-Betriebsgesellschaft (IABG), May 2002.

all related acts expired in 2007 with the enacting of the Telecommunications and Media Act (Telemediengesetz, TMG).[64]

## Electronic Signature Act 2001

In May 2001, this act (which conforms to EU regulations) replaced the existing pioneer Digital Signature Act of 1997. The main purpose of the act is to define a framework for the handling of electronic signatures.[65] The act was last amended on 26 February 2007.

## Penal Code[66]

To implement the EU Council Framework decision on 2005/222/JHA of 24 February 2005 on attacks against information systems, the German penal code was amended on 7 August 2007, affecting §202a on data espionage, §202b on data interception, §202c on the preparation of data espionage and interception, §303a on alteration of data, and §303b on computer sabotage.[67]

[64] http://bundesrecht.juris.de/tmg/BJNR017910007.html.

[65] Bundesministerium der Justiz. Gesetz über Rahmenbedingunge für elektronische Signaturen (Signaturgesetz – SigG). http://www.gesetze-im-internet.de/sigg_2001/BJNR087610001.html.

[66] See: Cybercrimelaw. Country Survey Germany. http://www.cybercrimelaw.net/countries/germany.html; and Bundesministerium der Justiz. German Penal Code (Strafgesetzbuch). http://www.gesetze-im-internet.de/stgb/index.html.

[67] Bundesgesetzblatt Jahrgang 2007 Teil I Nr. 38, ausgegeben zu Bonn am 10. August 2007, 1786-1787. http://www.computerundrecht.de/6758.html.

# Hungary

## Critical Sectors

In 2005, Hungary welcomed the EU program for Critical Infrastructure Protection (EPCIP). Even though some policies in the field of CIP had already been implemented before, the EU program highly influenced the further development of Hungary's CIP and CIIP policies. Accordingly, the Hungarian definition of the concept of critical infrastructure corresponds to the definitions of the EU as formulated in the Green Paper of the EU Commission.[1] Critical Infrastructures, according to the Hungarian Green Book, are defined as interconnected, interactive, and interdependent infrastructure elements, establishments, services, and systems that are vital for the operation of the national economy and public utilities to maintain an acceptable level of security for the nation, individual lives, and private property, as well as concerning the maintenance of the economy, the public health services, and the environment.[2] The CI sectors in the Green Book include the following:

[*] The Country Survey of Hungary 2008 was reviewed by Bence Birkás and Ferenc Suba from CERT-Hungary (with support from Barbara Locher, Ministry of Economics and Transport; Peter Csokany, National Communication Authority; and Csaba Sandor, Electronic Government Center); and Lajos Muha, Dennis Gabor College, Budapest.

[1] Commission of the European Communities. "Green Paper on a European Program for Critical Infrastructure Protection", Brussels, 2005. Cf. the chapter on the EU in this Volume.

[2] Information provided by an expert.

- Information and Telecommunication Systems,
- Energy,
- Water Supply,
- Transport,
- Public Health,
- Food-Products Supply,
- Banking and Financial Sector,
- Industry,
- Government Institutions,
- Public Security and Homeland Defense.[3]

In addition, a legal definition has been agreed that includes e-communications and postal services among the nation's critical infrastructures. According to article 2, no. 11 of ministerial decree no. 27/2004 of the Ministry of Informatics and Communications on the National Alert Service of the Postal and Communications Sector and the Tasks of the Designated Service Providers, a critical information infrastructure can be "any object or service, including e-communications and informatics systems, of which inoperability or destruction can severely impair, either separately or in conjunction with other inoperable or destroyed critical infrastructure, national security, the life and property of citizens, the proper functioning of national economy and public services."[4]

## Past and Present Initiatives and Policy

The increasing importance of ICT in the Hungarian economy has prompted the government to increase its commitment to the security of information systems and networks in general and of CIIP in particular. These efforts were fostered by

[3] Ibid.

[4] Ibid.

the EU, which has implemented various programs to strengthen the information society in its member states. Thus, Hungary has initiated different initiatives and policies aiming to promote the information society in recent years. This section presents the most important initiatives and policies with regard to CIIP and information security.

## The National Security Strategy of the Republic of Hungary

The protection of important information systems and critical information infrastructures is an integral part of the National Security Strategy of the Republic of Hungary. The challenges of the information society and the vulnerabilities of the new communication technologies are explicitly mentioned as risk factors for the country.[5]

The National Security Strategy also clearly points out the need for collaboration with international and private partners in the field of protection of information systems: "Successful protection [of information systems] requires close co-ordination with allies, as well as information and telecommunication providers and research centers."[6]

On 18 December 2007 the National Security Cabinet of the government decided to establish a new Information Security Inspectorate (ISI), into whose jurisdiction CIIP will also fall, to issue new regulation on ISI, and to set up a coordination body for information security and CIIP. These tasks are to be fulfilled until the end of 2008.

## The Hungarian Information Society Strategy

Despite of the rapid evolvement in the last years,[7] internet penetration in Hungary is still relatively low, and the number of "digital illiterates" is considered to be too

[5] Government of Hungary. "The National Security Strategy of the Republic of Hungary", Chapter II.1.6: Challenges of the Information Society.

[6] Ibid., Chapter III.3.7.

[7] Ákos Detreköi. "Information Society in Hungary", (2006). http://www.agile2006.hu/papers/detrekoi_agile_welcome.pdf.

high. Hence, the focus of the strategy is the development of a modern society and a competitive economy based on a widespread usage of information and communication technologies.

The Information Society Strategy consists of two pillars: the introduction of information technologies into (economic) processes, and the implementation of public electronic services.

Information security and the protection of privacy are seen as essential parts of the development towards an information society, since the extent to with ICT is used is determined by the extent to which people trust new technology. The strategy therefore identifies IT security as a field of governmental intervention and highlights the necessity of regulatory, organizational, and technological measures.

## The National Information Infrastructure Development Program (NIIF)

The National Information Infrastructure Development Program[8] was initiated to operate and advance the network of research bodies in Hungary. The program, which has been running since 1986, is the oldest and best established program for information and communication technology in Hungary. As a research program, the NIIF is essential for the development of the information society. By providing up-to-date information infrastructure for the academic and research community, the program introduces advanced network technology in Hungary.

The technical expertise of the NIIF and its broad network of national and international contacts are important for CIIP. The NIIF also operates a Computer Incident Response Team (CSIRT, see chapter on Early Warning and Public Outreach), and cooperates closely with other institutions involved in research on network security.

[8] http://www.niif.hu/en.

## Security Evaluation and Certification Scheme

Based on international standards like the Common Criteria and the Common Evaluation Methodology,[9] the Ministry of Informatics and Communications launched the Hungarian Information Security Evaluation and Certification Scheme (MIBETS).[10] MIBETS assists in evaluating and testing the security of software.

In addition, the ministry introduced the Information Security Management Framework (MIBIK), which aims to evaluate security measures at the organizational level.

The current government scheme includes an updated version of the MIBETS and MIBIK, now jointly abbreviated as MIBA. Government IT systems must be in compliance with the recommendations of the scheme, and a supervisory body will begin operating within the Prime Minister's Office Electronic Government Center from the first half of 2008.

## Organizational Overview

After the parliamentary elections of April-May 2006, the organization of the government was restructured. With regard to CIIP and the development of the information society, the most important change was the integration of the Ministry of Informatics and Communication – which was the central body for questions related to information and communication technology – into the Ministry of Economy and Transport and the Prime Minister's Office. The major tasks of CIIP are now mainly allocated in different ministries:

- Ministry of Economy and Transport:[11] As the ministry responsible for the maintenance and development of economic infrastructure – including

[9] cf. http://www.commoncriteriaportal.org/.

[10] Ferenc Suba and János Drencsán. "Hungary's National NIS Projects". In: ENISA Quarterly no. 12 (2005), pp. 16ff.

[11] http://www.gkm.gov.hu.

the information infrastructure – the Ministry of Economy and Transport coordinates the various efforts in the field of CIP and CIIP;

- Prime Minister's Office:[12] Through the Electronic Government Center,[13] the Prime Minister's Office coordinates the efforts with regard to e-Government, as well as other CIIP-related issues;
- Ministry of Defense:[14] This ministry is responsible for national security, including the security of information. In particular, it is responsible for protecting state secrets and public data;
- Ministry of Justice and Law Enforcement:[15] The duties and responsibilities of this ministry include crime prevention and data protection. It controls the Public Administration and Central Electronic Public Services Office, which is the central body for all tasks relating to the provision of e-government services and the management of electronic records and documents.

Since information security and CIIP is a horizontal issue that cuts across the responsibilities of individual government departments, Hungary has established a number of inter-ministerial bodies dealing with these tasks. In addition, Theodore Puskás Foundation, which works as a public-private partnership, plays an important role in CIIP, since it operates the national Computer Emergency Response Team (CERT-Hungary).

## Public Agencies

### The National Communications Authority (NCA)

Based on the Electronic Communications Act of 2003, the National Communications Authority was established in 2004 as an independent regulatory body for communications. The NCA's main task is to support the development of the communications market and to ensure that every citizen has access to affordable and reliable communications services. The NCA constantly analyzes

[12] http://www.meh.hu/english.
[13] http://www.ekk.gov.hu.
[14] http://www.honvedelem.hu.
[15] http://irm.gov.hu/?lang=en.

the market and exchanges information with national and international experts, and adapts its capabilities, methods, and operations accordingly.

The NCA is also responsible for the National Alert Service (NAS) in the postal and communication sectors, the operation of which has been outsourced to the CERT-Hungary Center of the Theodore Puskás Foundation (see chapter on Early Warning and Public Outreach). The NAS is based upon the co-operation of designated service providers who report the incidents affecting their services to the NAS. The main task of NAS is to gather and distribute these reports and to co-ordinate among service providers in case of emergency in affected regions, most frequently in case of spring floods in North-Eastern Hungary.[16]

## The National Board for Communications and Information Technology[17]

The National Frequency Allocation Board – the legal predecessor of the National Board for Communications and Information Technology – was established in 1993 by the government as an independent consulting and recommendation-making body for the allocation of radio and television frequencies. Over the years, its jurisdiction has been expanded, and today, the board is engaged in the fields of information technology, telecommunication, and media.

Some of the members of the board are appointed by the government (e.g., the chairman, who is appointed by the president of the republic), but there are also members appointed by scientific institutions and by the lobbies of the telecommunication companies. This heterogeneous composition ensures that the most important interests are represented, so that the board's recommendations are well-balanced.

The board elaborates drafts of laws and decrees related to IT or telecommunication and aims to foster the development of the information infrastructure.

[16] Information provided by the Hungarian experts involved.
[17] http://en.nhit.hu/start.

## Public-Private Partnerships

### Theodore Puskás Foundation

The Theodore Puskás Foundation[18] was established in 1992. It was co-founded by the government of Hungary and several distinguished institutions and businesses. It operates as a non-profit, public benefit organization. Its main objective is the dissemination of advanced technologies in Hungary. The foundation's activities include scientific research, consultations, and instruction in the field of information technologies.

In 2004, the Ministry of Informatics and Communication contracted the foundation to operate the national Computer Emergency Response Team (CERT-Hungary, see below), in consideration of its good reputation of the foundation and its research experiences in the field of information technology.

# Early Warning and Public Outreach

## Computer Emergency Response Teams (CERTs)

In Hungary, there are three important CERTs. Each of them serves a different constituency.

### CERT-Hungary

CERT-Hungary[19] is the governmental and national CERT. It is operated by the Theodore Puskás Foundation and was established in 2005. In its function as governmental CERT, it aims to improve information security of public agencies and is responsible for the technical aspects of CIIP. In order to combat high-tech crime efficiently, CERT-Hungary has developed direct communication channels to the national police force, and closely collaborates with all other

[18] http://www.neti.hu/pta/en/index.

[19] http://www.cert-hungary.hu.

agencies involved in CIIP.[20] CERT-Hungary is an accredited member of all main CERT forums, and acts as a National Contact Point for incident-handling and CIIP-related issues.

Furthermore, CERT-Hungary offers also some free services for the public, in particular warnings about emerging threats and new vulnerabilities, and provides chargeable services for private companies, e.g., intrusion detection, security audits, or malware analysis. Finally, CERT-Hungary coordinates a SCADA working group, which is organized jointly by government agencies and the operators of SCADA networks.[21]

## Hun-CERT

Hun-CERT[22] is operated by the Computer and Automation Research Institute of the Hungarian Academy of Sciences (MTA SZAKI).[23] It is sponsored by the Council of Hungarian Internet Service Providers (ISZT)[24] and mainly serves the interests of the members of the council. However, it is the intention of Hun-CERT to disseminate information on network security information among the general public.

Hun-CERT deals with all kinds of computer security incidents affecting Hungarian internet service providers. It supports system administrators in tackling these incidents. The level of support given varies according to the type and severity of the incident, the available resources of Hun-CERT, and the size of the affected community).

## NIIF-CERT

The NIIF-CSIRT (Computer Security Incidents Response Team of the National Information Infrastructure Development Program)[25] helps the members of the

[20] Suba, Ferenc and János Drencsán. "Hungary's National NIS Projects". In: ENISA Quarterly no. 12 (2005), pp. 16ff.

[21] Information provided by the Hungarian experts involved.

[22] http://www.cert.hu/index.php?option=com_content&task=view&id=16&Itemid=36.

[23] http://www.sztaki.hu/?en.

[24] http://www.iszt.hu/iszt/English/.

[25] http://www.niif.hu/en/csirt.

academic networks (NIIF and HUNGARNET) to handle all kinds of security incidents. The NIIF-CSIRT also disseminates important security-related information and warnings to its members.

## Hungarian Financal Services ISAC

In 2007, with the coordination of CERT-Hungary, the Hungarian Financial Services ISAC (Information Sharing and Analysis Center) was formed, involving law enforcement, the Hungarian banking association, the Hungarian Financial Regulatory Authority, and individual banks, including the biggest commercial banks. The cooperation between the parties resulted in several exercises, an incident handling directory, and cooperation on a recommendation about IT security in online banking.[26]

## Awareness Raising Programs

The www.biztonsagosinternet.hu project ("biztonsagos" means "safe") was launched by CERT-Hungary in May 2006 in order to provide a website for the general public with information on IT security in an easy understandable manner. The project is an adaptation of the German awareness-raising-program BSI für Bürger,[27] where the structure of the German model was adopted, and the texts were fitted to the Hungarian circumstances. The website gives advice for internet usage in general, and for e-shopping and e-banking in particular; it provides information on spam, viruses, and other threats to information security, and demonstrates how users can protect their privacy (with a special focus on child protection). Other awareness-raising programs include www.internethotline.hu and www.baratsagosinternet.hu. Both initiatives came into being as part of the Safer Internet Program – the first operating as an internet hotline for reporting harmful and illegal content, the other being the awareness node of Hungary.

[26] Information provided by the Hungarian experts involved.
[27] Cf. Country Survey Germany (in this volume).

The "e-Inclusion, be part of it!"[28] campaign was launched in December 2007. It aims to urge European governments and associations to give disabled people access to the advantages that the internet and information and communication technologies provide. The EU has issued three official calls since 2006 urging European governments to promote the advantages and digital opportunities of ICT for senior citizens, ill or disabled people, women (including those on maternity leave), minorities, or people living in rural areas of Hungary. Not only is Hungary's effort scant as far as the issue of inclusion in the information society is concerned. The majority of the Hungarian population are not aware of the advantages of the internet. The EU aims to change this situation by reducing the ratio of 'digital analphabetism' by half by 2010.

The Forum of Hungarian IT Organizations for Information Society (Inforum), together with other associations and firms, has announced plans to join the EU's initiative and is in the process of launching the e-Inclusion Year 2008, Hungary movement.

## Law and Legislation

### Penal Code

The Hungarian Penal Code includes several sections that are of relevance with regard to CIIP.[29] Particularly important are Articles 300/C and 300/E.

- Article 300/C: Criminal Conduct for Breaching Computer Systems and Computer Data: This article states that any person who gains unauthorized entry to a computer system shall be punished by imprisonment or community service. The punishment shall be more severe if the person alters, damages, or deletes data without permission, and particularly if the act is committed for financial gain.

[28] http://einclusion.hu.

[29] For an overview on the cybercrime legislation of Hungary, see: Council of Europe. "Project on Cybercrime, Cybercrime Legislation – Country Profile: Hungary". http://www.coe.int/cybercrime.

- Article 300/E: Compromising or Defrauding the Integrity of the Computer Protection System of Device: This article prohibits the creation, obtaining, and distribution of software, passwords, entry codes, or other data that can be used to gain access to a computer system or network illegally.

## Act on Protection of Personal Data and Disclosure of Data of Public Interest

Enacted in 1992, the Personal Data Protection Act (Act LXIII, Article 10)[30] sets rules and safeguards regarding the processing of personal data by public and private bodies. Its application is controlled by the Parliamentary Commissioner for Data Protection and Freedom of Information.

## Act on Electronic Commerce and Information Society Services

Adopted in 2001, this act implements an EU directive on electronic commerce. In doing so, it not only integrates the EU directive, but also makes use of the regulatory solutions included in the German (TDDSG, Mediendienststaatsvertrag) and US (Digital Millenium Copyright Act) legislation, especially in the sections relating to the liability of Information Service Providers (ISPs) and the notice-and-takedown procedure. The act governs the legal relationships of individuals, legal persons, and organizations for the purposes of e-commerce, in cases where the service is provided for or from the territory of Hungary.[31]

## Act on Electronic Signature

The Act on Electronic Signature[32] was adopted on 29 May 2001 and entered into force on 1 September 2001. It provides for legal recognition of electronic

[30] European Commission. "EGovernment in Hungary, Legal Framework", p.10. http://ec.europa.eu/egov.

[31] Ibid.

[32] http://www.epractice.eu/document/3374.

signatures (e-signatures) and electronic documents. Electronic documents and e-signatures are presumed to be admissible evidence in court and may not be challenged successfully based on the mere fact of their electronic form. An electronic document signed with an e-signature is deemed to be in compliance with a statutory requirement for a handwritten signature on a paper document. However, the act excludes family-related documents (e.g., marriage certificates and divorce decrees), and those documents must continue to be in paper form to have legal validity. Also, consumers are not obliged to accept the electronic format; if a consumer objects, a business firm must use paper documents. Hungarian government departments may elect to issue or accept electronic documents. Although all types of e-signatures are recognized, the digital signature enjoys most-favored status because it utilizes cryptographic methods resulting in a heightened degree of reliability and security.

## Further Regulations with Regard to CIIP and Information Security

In addition to the acts mentioned above, there are several further acts and decrees referring to CIIP and information security to some extent:

- Act no. CXII of 1996 on financial institutions and enterprises has a separate section in §13B on the security requirements of IT systems within financial institutions and enterprises;
- Act no. LXXXV of 1998 on the establishment of the National Security Supervision Office (NSSO): The NSSO is to provide advice on security for personal, physical, document and information, and industrial purposes. The office is also in compliance with the security measures promulgated within NATO, with regard to classified information;
- Government Decree 180/2003 on the rules of procedures of NSSO. Chapter IV regulates the detailed procedures of electronic security supervision;
- Ministerial Decrees 24/2004 and 27/2004 of the Ministry of Informatics and Communications on the National Alert Service in the Postal and Communications Sector and the Designated Service Providers: Ministerial

Decree 24/2004 obliges service providers to co-operate in the National Alert Service (NAS) of the Postal and Communication Sector. Decree 27/2004 sets the rules for the organization and operation of the NAS and gives a thorough list of definitions for CIIP (e.g., critical infrastructure, network security);

- Government Decree 84/2007 on the security measures of the Central Electronic Service System and adjoining systems: This decree states that the same security measures have to apply to all systems of the Central Electronic Service System (CESS), which include the government backbone, the government portal, the client portal, and all the services available through these gateways. The decree lists the uniform requirements of IT security for the CESS and includes the IT catastrophe recovery plan. The Prime Minister's Office is the operator of the Central Electronic Service System.[33]

[33] Information provided  by an expert.

# India

## Critical Sectors

In India, the following sectors are considered critical:

- Banking and Finance,
- Insurance,
- Civil Aviation,
- Telecommunications,
- Atomic Energy,
- Power,
- Ports,
- Railways,

[*] The Country Survey of India 2006 was reviewed by Subimal Bhattacharjee, Argus Integrated Systems. Luthra & Luthra Law Offices reviewed and contributed substantially to the section on Law and Legislative Action of the 2006 CIIP Handbook edition. For this edition, the authors have thoroughly updated the Indian country survey by referring to open-source material.

- Space,
- Petroleum and Natural Gas,
- Defense,
- Law Enforcement Agencies.

These 12 critical sectors were identified by the National Task Force on Y2K a few years ago, taking into account the extent of penetration of information technology in these sectors and the impact that a disruption of any of these sectors would have.[1]

## Past and Present Initiatives and Policies

In India, many efforts in the field of CIIP were triggered by the government's goal of making the country a leading knowledge-driven global economy by boosting IT and e-business. In 1998, the prime minister of India announced a drive to make India an IT superpower and one of the largest producers and exporters of software in the world within the next ten years. The government of India has recognized the potential of IT for rapid national development.[2] Therefore, it has established a National Task Force on Information Technology and Software Development[3] and a Department of Information Technology (DIT) within the Ministry of Communications and Information Technology, also dealing with CIIP.[4]

[1] Mishra Vineeta. "Critical sectors to be Y2K ready in time: govt report". In: India Times, 19 October 1999. http://www.apnic.net/mailing-lists/s-asia-it/archive/1999/10/msg00050.html.

[2] Government of India. National Task Force on Information Technology and Software Development. "Information Technology Action Plan, (Preamble)", 4 July 1998. http://it-taskforce.nic.in/infplan.htm#aa.

[3] http://it-taskforce.nic.in.

[4] http://mit.gov.in.

## National Task Force on Information Technology and Software Development and Information Technology Action Plan

The Indian government has given top priority to developing an appropriate action plan for the country to emerge as a global leader in the field of IT. As a first step, the National Task Force on IT and Software Development[5] was set up by the then Prime Minister Atal Behari Vajpayee on 22 May 1998, under the chairmanship of the deputy chairman of the planning commission. This task force had a mandate to formulate the draft of a National Informatics Policy, including:[6]

- To recommend an appropriate institutional mechanism to implement this policy as a national mission with the participation of the central and state governments, industry, academic institutions, and society at large;
- To prepare a vision statement that will excite and energize the people of India, creating a faith in IT for personal and national growth. The task force will also suggest a strategy for the effective articulation and dissemination of that vision, so as to create an ethos, an ambiance, a mindset, and a work culture that is consistent with the needs of the emerging knowledge-driven global civilization;
- To prepare a blueprint for the nationwide adoption of information technology, with a network of task forces at all governmental and non-governmental levels.

The IT Task Force submitted its first report in the form of an Information Technology Action Plan to the prime minister on 4 July 1998. The report contained a special section on IT for all by Year 2008, the centerpiece of which is a major

[5] http://it-taskforce.nic.in.

[6] http://informatics.nic.in/archive/inf98jul/cover.htm.

national campaign called Operation Knowledge, focusing on spreading IT and IT-based education at all levels.[7]

The establishment of the Task Force is a clear indication that IT is an area where India wants to achieve global pre-eminence. It is hoped that IT, fostered by these government policies, will prove immensely useful in all areas of national economy – especially industry, trade, and services – and will contribute significantly to making India a global economic power.[8]

## National e-Governance Plan (NeGP)

The government of India approved the National e-Governance Plan[9] (NeGP) on 18 May 2006. The plan lays the foundation and provides the impetus for long-term growth of e-governance within the country. The plan is intended to create the right government and institutional mechanisms, to set up the core infrastructure and policies, and to make the public administration more responsive to the needs of citizens and businesses.

The NeGP has started to realize three important elements of the e-Governance Plan that form the core infrastructure for effective service delivery: Data processing centers, State Wide Area Networks (SWANs), and Common Services Centres (CSCs). In addition, the government announced in 2006 that it would enhance its efforts to bring a number of services online. Subsumed under the label 'E-District', these services are provided at the district level and serve as the primary interface between citizens and the government.[10]

[7] The IT Action Plan included, among others, the following measures: Ministries and departments to earmark 1-3 per cent of their budget for IT; IT literacy requirement for government/public-sector employment; software and IT to be treated as a priority sector by banks; zero tax on all IT products by 2002; internet access through cable TV; early introduction of IT legislation; networking of all engineering/medical colleges and universities before 2000. http://it-taskforce.nic.in/index.html.

[8] Ibid.

[9] http://mit.gov.in/default.aspx?id=836.

[10] Government of India. Ministry of Communications and Information Technology. Department of Information Technology. "Annual Report 2006–2007", p. 4. http://mit.gov.in/download/annualreport2006-07.pdf.

## Core Group on Standards for e-Governance

Under the NeGP, standards for e-governance are crucial to ensure integration and interoperability of data and electronic applications. The Department of Information Technology (DIT) has therefore constituted a Core Group on Standards for e-Governance[11] to develop an institutional mechanism and processes, and to recommend key areas for standardization. Some of the priority areas for standardization are:

- Technical standards,
- Localization standards,
- Quality and documentation,
- Security standards,
- Metadata and data standards for various application domains.

An apex body has been constituted under the chairmanship of the secretary of the DIT with senior representatives from the government, the National Association of Software and Service Companies (NASSCOM),[12] the Bureau of Indian Standards (BIS), and others with a mandate to approve, deliver notification of, and enforce the standards formulated by various working groups and to ensure that they are in accordance with international practices.

The National Informatics Centre (NIC)[13] publishes whitepapers on all the desired standards, which serve as discussion papers for the working groups that develop the standards. The working groups with representatives of the DIT, associations, industry, academia, and central and state governments, etc., are constituted with the approval of the DIT.

[11] http://egov.mit.gov.in.

[12] http://www.nasscom.org.

[13] The National Informatics Centre (NIC) of the Department of Information Technology provides network backbone and e-governance support to the central government, state governments, administrations, districts, and other government bodies. It offers a wide range of ICT services, including a nationwide communication network for decentralized planning, improvement in government services, and greater transparency of national and local governments. The NIC collaborates closely with central and state governments in implementing IT projects. See http://home.nic.in.

The standards approved by the apex body are released on the web by the Standardization Testing and Quality Certification (STQC) Directorate, an office attached to the DIT. The STQC further ensures conformance and certification (where required) of these standards. The e-Governance Division of the NIC and the STQC function in tandem with the e-Governance Programme Management Unit at DIT.[14]

## Organizational Overview

In the Indian government, the National Information Board (NIB) is at the very top of the national information security structure. Directly linked to the NIB are the National Technology Research Organization (Technical Cybersecurity) and the National Information Security Coordination Cell (NISCC), which is part of the National Security Council Secretariat (NSCS). The NIB has instructed the NSCS to coordinate cyber-security activities across the country. The NISCC provides input for the consideration of the NIB. It works through the Sectoral Cyber Security Officers (SCOs).

Directly below the NIB are the Information Infrastructure Protection Centre (IIPC), followed by state cyber-police stations; and the Computer Emergency Response Team India (CERT-In), followed by state- and sectoral-level CERTs. Various ministerial coordinators of special functions are also situated at this level, as is the Development and Promotional Section of the Ministry of Communications and Information Technology (MOC).

As a public-private partnership initiative, the Indo-US Cyber Security Forum strives to discuss and implement increasing cooperation in high-technology between the two countries.

[14] Information provided by an expert.

## Public Agencies

### National Information Board (NIB)

The establishment of the National Information Board (NIB) was recommended by a group of ministers. It consists of 21 members. The national security advisor is the chairman of the board, while the deputy national security adviser serves as its member secretary. The NIB acts as the highest policy formulation body at the national level and periodically reports to the Cabinet Committee on Security of the Government of India, headed by the prime minister. The NIB is at the very top of the information security structure.[15]

### National Information Security Coordination Cell (NISCC)

The NIB has charged the National Security Council Secretariat (NSCS) with coordinating cyber-security activities across the country, covering both the public and the private sectors. NISCC provides input to NIB for its consideration. It works through the Sectoral Cyber Security Officers (SCOs). There are 20 such SCOs in various ministries, where the senior officer holds the rank of a joint secretary or director. The NISCC deals with the following topics: CERT functions, research and development, encryption, laws, interception and early warning, cyber-crime, training, and international cooperation. It represents the government in international forums for cyber-security and issues related to large scale cyber-related incidents.[16]

### Ministry of Communications and Information Technology (MOC): Department of Information Technologies (DIT)

The Department of Information Technologies (DIT),[17] part of the Ministry of Communications and Information Technology (MOC),[18] was established

[15] Presentation by Commander Mukesh Saini of the National Security Council, India, at the Indo-US Cyber Security Forum in Washington, D.C., on 9–10 November 2004.

[16] Information provided by an expert.

[17] http://www.mit.gov.in.

[18] http://www.moc.gov.in.

with the purpose of making India a leading IT nation by 2008. Through the DIT organization, the Indian government has undertaken several initiatives and strategies:

- The promotion of the internet and provision of IT infrastructure;
- The development of legislation;
- The support of IT education and development;
- The promotion of standardization, testing, and quality in IT;
- The establishment of an Information Security Technology Deve-lopment Council (ISTDC);
- The creation of a National Information Security Assurance Framework;
- The establishment of Inter Ministerial Working Groups.[19]

The Indian Computer Emergency Response Team (CERT-In) and the Controller of Certifying Authorities (CCA) are also DIT organizations. The Standardisation, Testing, and Quality Certification (STQC) Directorate and the National Informatics Centre (NIC) are also attached offices of the DIT.[20]

The DIT has set up the following Inter Ministerial Working Groups on:

- Cyber-Security Education and Research;
- Cyber-Security Assurance and Awareness;
- Encryption Policy and PKI;
- Legislation and Forensics in Cyberspace;
- Critical Infrastructure Protection.[21]

[19] http://www.mit.gov.in/default.aspx?id=9. Cf. presentation by Shri R. Chandrashekhar. "On The National E-Governance Plan – Approach & Key Components". National e Governance Plan – Workshop with States and UTs, (New Delhi, 11–12 March 2005). http://www.mit.gov.in/default.aspx?id=115.

[20] http://www.mit.gov.in/default.aspx?id=12.

[21] Presentation by Shri R. Chandrashekhar, op. cit.

## Standardization, Testing and Quality Certification (STQC) Directorate

The Standardization, Testing, and Quality Certification (STQC) Directorate is an office attached to the DIT. The STQC provides quality and security assurance services that meet international standards to Indian companies and users. The STQC program has been in place for over three decades, and the STQC has positioned itself as a prime provider of assurance services to both the hardware and the software industry, as well as for users. The recent focus of the DIT on IT security, software testing and certification, and the assignment of a national assurance framework, has further raised the responsibility of the STQC as well as the expectations it must meet.[22] The STQC worked together with the US National Institute of Standards and Technology (NIST) to create a US standard for controls of Information Security, SP-800-53.

## Information Security Technology Development Council (ISTDC)

The main objective of the Information Security Technology Development Council (ISTDC) is to facilitate, coordinate, and promote technological advancements, and to respond to information security incidents, threats, and attacks at the national level. ISTDC was established for the following functions:[23]

- To evaluate cyber-security project proposals, and to provide recommendations for further processing by DIT;
- To review on-going projects through monitoring committees and recommend any modification in scope, funding, duration, additional input, termination, and transfer of technology;
- To recommend follow-up action on completed projects concerning transfer of technology and the initiation of subsequent phases;
- To form project review and steering groups of projects approved and funded by the DIT.

[22] http://www.stqc.nic.in.

[23] http://www.nasscom.org//download/india.pdf.

## Public-Private Partnerships

### Indo-US Cyber Security Forum

In pursuance of the Indo-US Cyberterrorism Initiative announced by Indian Prime Minister Atal Behari Vajpayee and US President George Bush in Washington in November 2001, the first plenary session of the Indo-US Cyber Security Forum was held at the National Security Council Secretariat (NSCS) in India in April 2002. The second plenary meeting was held in Washington, D.C. in November 2004. This meeting resulted in the creation of five working groups on legal issues and law enforcement, research and development, emergency response and watch and warning, defense cooperation, and standardization. In 2005, the NSCS organized five seminars and a workshop with the help of the Confederation of Indian Industry (CII). There has also been some exchange of experts. In 2006, the third Plenary of the Indo-US Cyber Security Forum was held. The Confederation of Indian Industry, in consultation with its US counterpart, decided to set up an India Information Sharing and Analysis Center and an India Anti-Bot Alliance to raise awareness about emerging threats in cyberspace. CERT-In and the US national Cyber Security Division agreed to share expertise in artifact analysis, network traffic analysis, and exchange of information. The research and development group concentrates on hard problems of cyber-security, cyber-forensics, and anti-spam research.[24]

The Indo-US Cyber Security Forum is a part of the Indo-US High Technology Group, a public-private partnership between India and the US established to discuss and implement ways and means of increasing cooperation between the two countries in high-technology areas.

[24] http://www.indlawnews.com/FABDE8B21DAB06E51E383AACA2D3FF36.

## Early Warning and Public Outreach

### Indian Computer Emergency Response Team (CERT-In)

The Indian Computer Emergency Response Team (CERT-In)[25] was established in January 2004 by the Department of Information Technologies (DIT) as part of the international CERT community. It has a mandate to respond to computer security incidents reported by the national computer and networking community as well as to create security awareness among Indian IT users. The main CERT is located in New Delhi, with backup in Bangalore. It has reactive as well as proactive functions.[26] CERT-In aims to become India's most trusted agency for responding to computer security incidents. In addition, CERT-In will also assist Indian IT users in implementing proactive measures to reduce the risks of security incidents.

Another five sector-specific CERTs have been set up: three for the army, air force, and navy; one for banking, known as FinCERT; and one for railways, known as RailCERT. It is anticipated that more CERTs will be established for the telecom and the power sectors.

CERT-In recently appointed a panel of IT security auditors, whose tasks will include vulnerability assessment and penetration testing of the computer systems and networks of various organizations of the government, critical infrastructure organizations, and in other sectors of Indian economy.[27] The auditors will assist CERT-In in assessing the information security risks. They will determine the effectiveness of information security controls over information resources and assets that support operations in the auditor organizations at their request.[28]

[25] http://www.cert-in.org.in.

[26] http://www.cert-in.org.in/roles.htm.

[27] http://www.cert-in.org.in/audit-background.htm.

[28] Ibid.

## Law and Legislation

In the year 2000, the government of India enacted the Information Technology Act (IT Act) to provide a framework for the legal recognition of electronic commerce in India. The IT Act provides for the establishment of a public-key infrastructure in India and addresses issues of cyber-crime and the admissibility of digital evidence. It achieves this through various provisions and by way of amendments to other statutes, such as the Indian Penal Code 1860, the Indian Evidence Act of 1872, the Bankers' Books Evidence Act of 1891, and the Reserve Bank of India Act of 1934. The amendments relate to the inclusion of electronic records and other such computerized data alongside the traditional forms of documents.

### Information Technology Act 2000 (IT Act)

The IT Act comprises 13 chapters, divided into 94 sections. The chapters relevant to the present discussion are: Chapter V (Secure Electronic Records and Secure Digital Signatures), Chapter VII (Digital Signature Certificates), Chapter IX (Penalties and Adjudication), Chapter XI (Offences), and Chapter XII (Network Service Providers Not To Be Liable In Certain Cases).

The IT Act provides a much-needed legal framework for electronic transactions in India. The National Association of Software and Service Companies (NASSCOM), the leading trade body and the chamber of commerce of the IT software and services industry in India, summarizes some of its key progressive features as follows:[29]

- From the perspective of e-commerce in India, the IT Act 2000 and its provisions contain many positive aspects. First of all, these provisions have approved e-mail as a valid and legal form of communication in India that can be duly produced and approved in a court of law;
- Companies are now able to carry out electronic commerce using the legal infrastructure provided by the act;

[29] http://www.nasscom.org/artdisplay.asp?cat_id=852.

- The act bestows legal validity and sanction on digital signatures;
- The act allows companies to become certifying authorities that may issue digital signature certificates;
- The act allows the government to issue legal notifications on the internet, a first step towards e-governance;
- The act enables companies to file any form, application, or other document with any office, authority, body, or agency owned or controlled by the government in such electronic formats as may be prescribed by the government;
- The IT Act also addresses important issues of security that are critical for the success of electronic transactions. The act includes a legal definition of the concept of secure digital signatures that must undergo a security procedure as stipulated thereunder;
- The act offers companies a statutory remedy in case anyone should break into their computer systems or network and cause damages or copy data. The remedy provided by the act is in the form of monetary damages not exceeding 10 million rupees.

In order to resolve IT-related disputes in a focused and timely manner, the IT Act provides for the constitution of a Cyber Appellate Tribunal, which acts as a forum for original jurisdiction on issues arising under the IT Act. Appeals from the tribunal can be made to the relevant state high courts.

Section 79 of the IT Act declares that network service providers shall not be liable for any third-party information or data made available by them if they prove that the offense or contravention was committed without their knowledge or that they had exercised all due diligence to prevent the commission of such an offense. This provision is crucial, as it is the only one under which a network service provider can claim a defense under the provisions of the act.

In order to further strengthen the scope and ambit of the IT Act, a committee has been set up comprising several experts in cyber-law and data protection who will review the act and make necessary changes to ensure that the existing lacunae in the law can be filled. These amendments are likely to deal with provisions concerning third-party liability, issues of privacy and data protection security, and the replacement of written signatures with digital signatures, among others.

## IT Related Offenses Under the IT Act

Section 43 of the IT Act specifies acts committed without the permission of the owner or person in charge of a computer, computer system, or computer network that may cause damage by destruction, alteration, deletion, addition, modification, or rearranging of any computer resource. The offenses relate specifically to: (a) accessing or securing access to a computer, computer system, or computer network; (b) downloading, extracting, or copying of data or information from such computers, computer systems, or computer networks; (c) introducing or causing the introduction of any virus or computer contaminant; (d) disrupting or causing disruption to computers, computer systems, or computer networks; (e) damaging or causing to be damaged any computer, computer system, or computer network or any programs residing therein; (f) denying or causing denial of access by any person authorized to use the computer system or computer network; (g) assisting a person in contravention of the IT Act; (h) manipulating a computer for financial benefit.

Sections 65 through 74 of the IT Act contain provisions relating to various cyber-crimes.[30]

### Hacking and Tampering with Computer Source Code

The popular and notorious offense of hacking is dealt with under Section 66 of the IT Act. Hacking is defined as the act of destroying, altering, deleting, diminishing in value, or injuriously affecting the information residing in a computer resource, by any means. An essential element of this offense is the intention or knowledge on the part of the perpetrator of causing the wrongful loss. This provision is often viewed as a "catch-all" provision because of its broad wording, which could be potentially used to cover any IT crimes that are not covered by any other provision of the IT Act.

[30] Information provided by an expert.

Tampering with computer source code has been made an offense under Section 65 of the act. This provision applies to offenders who alter, conceal, or destroy computer source codes.

The maximum punishment for both hacking and tampering with computer source code is three years' imprisonment and/or a fine of up to 200,000 rupees, or both.

### Breach of Confidentiality and Privacy

Section 72 of the IT Act deals with the penalty for breach of privacy and confidentiality. It applies to situations where individuals who have gained access to any electronic record, book, register, information, document, or other material by virtue of powers conferred to them under the IT Act or related legislation make an unauthorized disclosure of the same.

Offenses relating to digital signatures, which include misrepresentation or suppression of material facts from the Digital Signature Certificate and publishing a digital signature for fraudulent purposes, are also covered under this section.

## IT-Related Offenses under the Indian Penal Code

The Indian Penal Code of 1860 (IPC) is the statute governing criminal jurisprudence in India. With the enactment of the IT Act, specific provisions of the IPC dealing with offenses relating to documents and paper-based transactions were amended to include crimes conducted using electronic devices.

The amendments made to the IPC refer to the sections dealing with forgery, extortion, criminal breach of trust, criminal intimidation, and fraud.

### Forgery

The offense of forgery is covered by Section 463 of the IPC. It is defined as an act of creating false documents or electronic records for the purpose of causing damage or injury to the public or any person, or to commit fraud. A "forged document or electronic record" is defined under Section 470 as a document or electronic record that is false and has been forged either entirely or in part. The general offense of forgery is further classified into a range of individual offenses. These include forgery for the purpose of cheating or defaming another party; making, using, or possessing forged documents; and counterfeiting authentication marks and designs.

## Extortion

Such an offense involves one person dishonestly inducing another to deliver any property or valuable security by intentionally putting fear of injury in that person's mind. This offense is dealt with by the IPC under Section 383. When such crimes are committed electronically, they would be included within the purview of this section as well. Web-jacking and threatening e-mails are examples of extortion committed by an electronic medium.

## Criminal Breach of Trust

Section 405 of the IPC defines "criminal breach of trust" as any act whereby a person who has been entrusted with property, or with any power over any property, dishonestly misappropriates the property, makes wrongful use of the property, dishonestly disposes of that property, or induces any other person to do so.

## Criminal Intimidation

When a person threatens another or someone in whom such other person is interested with injury to their physical well-being, reputation, or property and causes them to commit or desist from actions against their free will in order to avoid the execution of such threats, this constitutes criminal intimidation. When such threats or intimidation occur through e-mails or other electronic means of communication, they are punishable under Section 503 of the Indian Penal Code. Threats of denial-of-service attacks, e-mail bombing, virus attacks, cyber-stalking, etc., can be used to intimidate a person and amount to criminal intimidation.

### Cheating

Section 420 of the Indian Penal Code deals with fraud cases. Under the section, whoever cheats and consequently dishonestly induces a person to deliver any property (to any other person), or to alter or destroy the whole or any part of a valuable security, shall be punished. When fraud is committed with the use of a computer, as in the case of credit card fraud, money-laundering, or e-mail spoofing, it is punishable under the IPC.

## Further Issues

### Data Protection

The only provision of the IT Act that currently addresses the issues of data protection and confidentiality is Section 72. To address the issue of misuse of personal information and data, India is currently in the process of reviewing the various clauses of the IT Act. In the absence of a specific law on data protection, appropriate principles, safeguards, and liquidated damages for breach would need to be built into a contract between relevant parties to ensure adequate remedies for data protection.

The Indian Contract Act of 1872 (Contract Act) codifies the way one enters into a contract, the execution of a contract, the implementation of its provisions, and the effects of breach of such contract. Contracts are among the best ways for foreign firms to protect their data and intellectual property while subcontracting work to India. The Indian Contract Act provides adequate safeguards to foreign companies, provided that both firms (Indian and foreign) agree to the contract. The companies subcontracting their work to India need to enter an exhaustive Service Level Agreement (SLA) with their vendor that covers various aspects of data security and confidentiality. This will help companies to safeguard against any fraud or misconduct.

### Copyright

The Indian Copyright Act of 1957 was amended in 1994–1995 to include penalties for any person who knowingly makes use of an illegal copy of a computer program.

Such an act is punishable with a minimum imprisonment of seven days, although a sentence of up to three years can be imposed. The act further provides for fines of 50,000 to 2,000,000 rupees, a jail term up to three years, or both.

# Italy

## Critical Sectors

Since information and communication technologies (ICTs) play an important role in a number of critical sectors, the protection of critical information infrastructures is crucial for the well-functioning of the Italian society. In consequence, there are several strategy and policy papers with regard to CIP and CIIP (see the section on Past and Present Initiatives and Policies). These documents define the critical sectors consistently, so that it is possible to specify the sectors that are deemed to be critical, even if there is no official register of the critical infrastructures of Italy:

- Banking and Finance,
- Public Safety and Order,
- (Tele-) Communication,

[*] The Country Survey of Italy 2008 was reviewed by Roberto Setola, Complex Systems and Security Laboratory, Università Campus Bio-Medico; and Tommaso Palumbo, Postal and Communication Police Service.

- Emergency Services,
- Energy Production, Transportation, and Distribution,
- Public Administration,
- Health Care Systems,
- Transportation and Logistics (Air, Rail, Maritime, Surface),
- Water (Drinking Water, Waste Water Management),
- Information Services and the Media,
- Food supply.

## Past and Present Initiatives and Policies

There is no central unit in Italy devoted to defining CIP and CIIP policies and strategies: Various activities are assigned to ministries and public bodies in charge of the different critical sectors, as well as those responsible for public safety and security. In addition, a variety of coordination efforts have been undertaken:

- In order to create an inter-sectoral forum and to improve awareness on CIIP, a Working Group on Critical Information Infrastructure Protection was set up in March 2003 at the Department for Innovation and Technologies of the Presidency of the Council of Ministers. All ministries involved in the management of critical infrastructures are represented in the group, together with many Italian infrastructure operators and owners as well as various research institutes. The working group ended its activities after publishing the Report on Critical Information Infrastructure Protection: The Case of Italy in 2004;
- The Ministry of Communication has established a special working group to analyze the responsibilities and security requirements that CIIP imposes on communication infrastructure operators, and to analyze the dependencies of the latter on other critical infrastructures. This working group has issued the following guidelines with regard to CIIP: The Network Security of Critical Infrastructures (2005); Network Security: From Risk Analysis

to Protection Strategies (2005); Guideline on Managing Local Emergencies (2006). With the publication of these guidelines, the working group ended its activities;

- In July 2005, to coordinate activities better and improve the protection of CII with respect to cyber-attacks, the Postal and Communications Police was identified as the unit responsible for law enforcement initiatives in this area;
- In 2006, a new body for the coordination of all ministries and agencies involved in CIP was established. This body, named Tavolo interministeriale di coordinamento ed indirizzo nel settore della protezione delle infrastrutture critiche (Tavolo PIC)[1] is chaired by the Military Advisor to the President of the Minister's Council. Tavolo PIC is charged with coordinating all activities in the field of CIP and CIIP. It also serves as an international contact point;
- To improve the protection of critical information infrastructure against cyber-threats, the Ministry of the Interior established the National Anti-Cybercrime Center for the Protection of Critical Infrastructures (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche, CNAIPIC) in 2008.

## Report on Critical Information Infrastructure Protection: The Case of Italy

The Working Group on Critical Information Infrastructure, established as part of the Prime Minister's Office in 2003 to address CIIP, released the report Protezione delle Infrastrutture Critiche Informatizzate – La Realtà Italiana (Critical Information Infrastructures Protection: The Case of Italy)[2] in March 2004, offering a synthesis of its efforts. The document describes many elements of the Italian infrastructure, emphasizes their interdependencies, and suggests CIIP

[1] Interministerial Coordination Platform and Contact Point for the Sector of Critical Infrastructure Protection.

[2] Working Group for the Protection of Critical Infomration Infrastructure Protection. "Protezione delle Infrastrutture Critiche Informatizzate – La realtà Italiana", March 2004.

policy strategies. In particular, the Working Group suggests that full responsibility for the correct implementation of a survivability policy should remain with the individual owners and operators of critical infrastructure, while the government should be responsible for the definition of an overall policy to minimize interdependencies and cascading failures.

## Guidelines for the Protection of Critical Information Infrastructures

The Institute for Information and Communication Technologies (ISCOM) of the Ministry for Communication has published several guidelines with regard to the security of ICT and the protection of critical information infrastructures. The guidelines are elaborated in close collaboration with various private organizations, most notably with the owners and operators of critical infrastructures. The following two guidelines directly address the security of information in critical infrastructures:

- The guideline The Network Security in Critical Infrastructures[3] highlights the importance of information infrastructures in Italy and identifies and analyzes the vulnerabilities and interdependencies of critical information infrastructures. The document also proposes best practices for the protection of critical infrastructures (e.g., certification of secure services), as well as organizational measures such as the creation of a crisis management group where stakeholders of all the critical infrastructures can be represented.
- The guideline Network Security: from Risk Analysis to Protection Strategies[4] describes the features of the information and communication network and its importance for contemporary society. In particular, the document addresses the topic of risk analysis and risk management with regard to ICT.

[3] http://www.isticom.it/documenti/news/pub_003_eng.pdf.

[4] http://www.isticom.it/documenti/news/pub_002_eng.pdf.

Other documents issued by the Ministry of Communication also deal with information security and risk analysis. They encompass analyses on the quality of communication networks; analyses on outsourcing in the field of information security; guidelines for local crisis management; and studies on the certification of secure ICT.[5]

## Organizational Overview

The main Italian government bodies dealing with CIIP are the Ministry of the Interior (Postal and Communications Police) and the Ministry of Innovation and Technologies. The Ministry of Communication is also involved in various activities to improve the security of information and communication networks.

In order to improve CIIP at all levels, the public agencies also collaborate closely with the private sector. The most important Public-Private Partnership in the field of CIP is the Association of Italian Experts for Critical Infrastructures (Associazione Italiana Esperti in Infrastrutture Critiche, AIIC),[6] an expert group of practitioners from both the public and the private sectors.

### Public Agencies

#### Ministry of Communication

The Ministry of Communication supervises postal and telecommunications services, acting as a regulator as well as implementing a policy of coordination, supervision, and control.[7] It is involved in the definition of security policies for communication. In 2004, ISCOM established a working group to analyze the different aspects of security in communication networks and the security requirements required in communication networks to guarantee an adequate

[5] For an overview on the documents issued by ISCOM, see: http://www.isticom.it/index.php?option=com_frontpage&Itemid=1.

[6] http://www.infrastrutturecritiche.it.

[7] http://www.comunicazioni.it/english_version.

level of services for critical infrastructures. The working group ended its activities in 2006.[8]

## Permanent Working Group on Network Security and Communications Protection

The Ministries of Communication, the Interior, and Justice established the Permanent Working Group on Network Security and Communications Protection in 1998 with a focus on criminal, legal, and economical aspects of communication services, such as the duration for which a provider should store communication data. Within this group, the Internet Subgroup deals with investigative and judicial matters related to the internet.

## Postal and Communications Police

In 1992, the Ministry of the Interior issued a directive assigning to the state police specific responsibilities for IT and telecommunications security that are in fact carried out by the Postal and Communications Police. The Postal and Communications Police is a flexible organization with a staff of around 2,000 highly trained officers, and placed at the peak of a structure involving 19 regional departments and 76 territorial sections. The Postal and Communications Police reviews communications regulations, studies new technical investigative strategies to fight computer crime, and coordinates operations and investigations for other offices. This police force also collaborates with other institutions – in particular, with the Ministry of Communication and the Privacy Authority – and with private operators who deal with communications. As the Italian contact point for the G8's computer crime offices, it is available at all times. This particular organizational aspect guarantees a quick, qualified, and efficient response[9] in the event of a threat or computer attack originating nationally or internationally.

The Postal and Communication Police Service also hosts and manages an emergency center at both the national and regional levels, in order better to deal

[8] Information provided by an expert.

[9] http://www.poliziadistato.it/pds/english/specialist.htm.

with computer crimes against critical infrastructure and to conduct preventive monitoring activities on a technical and operational level. The center serves as a focal point for the evaluation of threats, thus providing adequate countermeasures to face such situations.

Article 7 bis of the Law n.155/2005 assigns the task of protecting national information infrastructures against cyber-crime attacks to the Postal and Communication Police Service. In order to perform this task, the aforementioned Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC) was established as a special unit of the Postal and Communication Police Service.[10]

## Ministry for Innovation and Technologies (MIT)

The Ministry for Innovation and Technologies[11] has been delegated to act on behalf of the prime minister in the areas of technological innovation, the development of the Information Society, and related innovations for government, citizens, and businesses. This ministry has particular responsibility for network structures, technologies, and services, the development and use of information and communication technologies, and the fostering of IT and digital awareness and literacy, including through links with international and EU bodies that are active in the sector. The MIT has also been delegated to chair the Committee of Ministers for the Information Society and the Committee of Ministers for Joint Satellite Navigation Initiatives.

The Department for Innovation and Technologies (DIT) is the department of the Presidency of the Council of Ministers that provides support to the minister of innovation and technologies. It serves to coordinate ministerial policies for the development of the Information Society and to promote innovation in public offices and among citizens and businesses.[12]

[10] Information provided by an Italian expert.

[11] http://www.innovazione.gov.it.

[12] http://www.innovazione.gov.it.

## National Technical Committee for ICT Security in the Public Administration

On 16 October 2002, the Ministry for Innovation and Technologies and the Ministry of Communication created the National Technical Committee for ICT Security in the Public Administration. The establishment of this new committee followed from the Directive on ICT Security for the Public Administration, which enacts EU recommendations with the important initial aim of achieving compliance with a set of minimum security standards. The Technical Committee can therefore be seen as the operative arm of the new national IT security policy.[13] It was constituted in July 2002 with support from the Ministry for Innovation and Technologies and the Ministry for Communications.[14]

The committee aims to attain a satisfactory security level in information systems and digital communications, in compliance with international standards, in order to guarantee the integrity and reliability of the information. It prepares strategy proposals concerning computer and telecommunications security for the public administration. In particular, it develops:

- The National Emergency Plan for the Security of Information and Communication Technologies in the Public Administration. The committee annually verifies its state of progress, and proposes corrective measures if required;
- The ICT security national organizational model for the public administration. The committee monitors its level of activation and application.

Furthermore, the committee formulates proposals for regulating certification and security assessment, as well as certification criteria and guidelines for ICT security certification in the public administration, on the basis of national, sectoral, and international norms of reference.

[13] http://www.innovazione.gov.it.

[14] Minister for Innovation and Technologies. "Government Guidelines for the Development of the Information Society" (13 February 2002). http://www.innovazione.gov.it/eng/intervento/allegati/docu_base130202.pdf.

Finally, the committee elaborates guidelines for agreements with the Ministry of Public Administration for training public employees in ICT security. Among other proposals, the group is tasked with establishing the Computer Emergency Response Team (CERT) for the Public Central Administration (CERT-PA, now GovCERT.it, which has also assumed the role of coordinating the CERTs of the other parts of the public administration). It will have a central Early-Warning System operating around the clock.

In March 2004, the National Technical Committee on ICT Security published a preliminary proposal for the National Security Plan and an organizational model. Guidelines were suggested for building an organizational infrastructure to coordinate and support public offices at the national level, and the most urgent areas of action for putting the process on track were identified.[15]

## National Center for Informatics in the Public Administration (CNIPA)

The Authority for IT in the Public Administration (AIPA), founded in 1993, was transformed into the National Center for Informatics in the Public Administration (CNIPA) in 2003.[16] CNIPA is supervised by the Ministry of Innovation and Technologies, and its head is nominated by the Council of Ministries. It addresses central and local administrations, especially the elements responsible for IT systems in the public administration. The main task of CNIPA is to promote modern information technologies in the Italian public administration, to establish standards and methods, to deal with security issues, and to make recommendations and technical regulations in the field of IT for public administration.[17] CNIPA published a comprehensive guide on the protection of personal data in 2001.

[15] http://www.innovazione.gov.it.

[16] http://www.cnipa.gov.it.

[17] http://www.cnipa.gov.it.

## Public-Private Partnerships

### Association of Italian Experts for Critical Infrastructures (AIIC)

The Association of Italian Experts for Critical Infrastructures[18] is a not-for-profit-organization that aims “to support an interdisciplinary and inter-sectoral culture for the development of strategies, methodologies, and technologies supporting the correct management of Critical Infrastructure during periods of crisis, in case of exceptional events, and during terrorist attacks or natural disasters.”[19] The AIIC comprises public as well as private members.

In order to raise awareness of information security and critical infrastructure protection, the association publishes periodical newsletters on national and international developments in the field of CIIP and provides information on strategies and policies as well as on recent scientific findings on its website.

## Early Warning and Public Outreach

A variety of Computer Emergency Response Teams (CERTs) is currently active in Italy. They are all devoted to the development of IT security and to supporting organizations in increasing their level of security with respect to cyber-threats.

- CERT-IT: The Italian Computer Emergency Response Team was founded in 1994 as a non-profit organization. It is mainly supported by the Department of Informatics and Communications (DICO) at the University of Milan.[20] CERT-IT is a member of the Forum of Incident Response and Security Teams (FIRST). It promotes research and development activities in security systems, provides information about computer security, and has an expert team for handling computer incidents;[21]

[18] http://www.infrastrutturecritiche.it.

[19] http://www.infrastrutturecritiche.it/jml/index.php?option=com_frontpage&Itemid=1.

[20] http://security.dsi.unimi.it.

[21] http://idea.sec.dsi.unimi.it/activities.en.html.

- GovCERT.it:[22] This initiative was planned by the National Technical Committee on Computer and Telecommunications Security to help public administrations to improve their level of ICT security by providing an early-warning service on cyber-threats;
- GARR-CERT:[23] The GARR Network Computer Emergency Response Team assists the users of the GARR Network (Gestione Ampliamento Rete Ricerca – the Italian Academic and Research Network) in implementing proactive measures to reduce the risk of computer security incidents and in responding to such incidents when they occur;
- CERT Difesa:[24] The CERT of the Ministry of Defense assists its users in protecting ICT networks and disseminates information about ICT security.

The Ministry of the Interior, together with the Postal and Communication Police, is also active in early-warning activities. These agencies continuously monitor cyberspace to discover criminal or malicious behavior in order to provide adequate countermeasures. Moreover, specific protocols have been established to prevent incidents and to manage and share information as well as criminal evidence.

## Law and Legislation

Italy has specific laws and ministerial decrees devoted to CIP and CIIP. In the early 1990s, a new law related to computer crimes was introduced (Law 547 of 23 December 1993) that gave more power to investigators in the evidence-collection phase and allowed computer and telecommunication intercepts. Italy was one of the first European countries to adopt such legislation, mainly due to the incidence of new crimes in the areas of computer fraud, forgery, data corruption, computer misuse, unauthorized interceptions of computer communications, and

[22] http://www.cnipa.gov.it/site/it-it/Attivit%C3%A0/Servizi_per_la_PA/Govcert.it/.
[23] http://www.cert.garr.it/index-en.html.
[24] http://www.difesa.it/SMD/Staff/Reparti/II-reparto/CERT/default.htm.

sabotage. The great attention given to such crimes is underscored by the fact that computer intrusions are treated as domestic property violations.

The innovative concept of High-Tech Crime, which had already enjoyed currency in the Italian penal legislation for different types of offenses, was introduced with Law 547. According to Article 420 of the Italian Penal Code (attempt to damage public utilities systems), actual damage or destruction to the systems are not required for such activities to constitute an offense; the mere intention suffices. Such cases will be prosecuted even if the attempt was unsuccessful.

Other relevant laws include:

- Legislative Decree 518, enacted on 29 December 1992 and modified by Law 248 (18 August 2000), a legislative decree against illicit ICT piracy;
- Law 547, enacted on 23 December 1993, a comprehensive and integrated law against ICT crimes;
- Law 675, enacted on 31 December 1996, a law governing personal data protection, integrated by subsequent legislation (DPR 318/1999, Law 325/2000, Legislative Decree 467/2001, and Legislative Decree 196/2003);
- Legislative Decree 374/2001, changed into Law 438/2001, a law devoted to improving law-enforcement instruments and to combating terrorism. Law 374/2001 was transformed into Law 438/2001 after 11 September 2001, so that now, crimes committed in Italy are liable to prosecution even if they are directed against a foreign state or against a multilateral institution.
- Article 7 bis of Law 155/2005 defines the authority of the Postal and Communication Police Service to carry out undercover investigations and preemptive interceptions both for the protection of critical infrastructures and for countering terrorist acts committed by means of new technologies.

## Privacy Law

Part of Article 15 of Law 675/96[25] (the Privacy Law) deals with the organizational issues that the use of IT systems raises. By establishing a duty to store data in a way that minimizes the risk of loss and prevents unauthorized access (includ-

[25] http://www.innovazione.gov.it/ita/privacy/legge675_96.rtf.

ing access inconsistent with the reasons given for the original acquisition and processing of such data), Article 15 requires data holders to update their security to keep up with technical advances and changes in the methods of infiltration.

Consequently, not only should the minimum measures established by Presidential Decree 318/99 be strictly implemented and observed, but all appropriate additional measures should also be taken and regularly updated to match technical progress.

A New Privacy Code, which contains specific requirements for the protection of personal data online, has been in force since July 2003.[26]

## Italian Penal Code

Penal Code Article 615 ter: Unauthorized Access to Computers or Telecommunication Systems: Any person who enters a computer or telecommunication system protected by security measures without authorization, or remains in it against the expressed or implied will of the authority that has the right to exclude them, shall be sentenced to imprisonment not exceeding three years.

The imprisonment is from one until five years:

1) if the crime is committed by a public official or by an officer of a public service, through abuse of power or in violation of the duties concerning the function or the service, or by a person who practices – even without a license – the profession of a private investigator, or by abusing the authority of a system operator;
2) if, in order to commit the crime, the culprits use violence against assets or people or if they are manifestly armed;
3) if the deed causes the destruction or damage of the system or the partial or total interruption of its operability, or the destruction or damage of the data, information, or programs contained in it.

[26] http://www.innovazione.gov.it/eng/egovernment/infrastrutture/sicurezza_privacy.shtml.

If the crimes listed in the first and second paragraphs concern computer or telecommunication systems of military importance, or of importance to public order or public security, or civil defense, or any public interest whatsoever, the penalty is one to five years and three to eight years of imprisonment, respectively. In the case provided for in the first paragraph, the crime is only liable to prosecution after an action by the plaintiff; the other cases are prosecuted ex officio.

Penal Code Article 615 quater: Illegal Possession and Diffusion of Access Codes to Computer or Telecommunication Systems:

Whoever, in order to obtain a profit for themselves or for another or to cause damage to others, illegally gets hold of, reproduces, propagates, transmits, or delivers codes, key-words, or other means for accessing a computer or telecommunication system protected by safety measures, or whoever provides information or instructions for the above purpose, will be punished by imprisonment not exceeding one year and a fine.

Penal Code Article 615 quinquies: Diffusion of Programs Intended to Damage or to Disrupt a Computer System:

Whoever propagates, transmits, or delivers a computer program – written by themselves or by another party – with the aim and the effect of damaging a computer or telecommunication system, the data or the programs contained therein or pertinent to it, or achieving the partial or total interruption or an alteration in its working, will be punished by imprisonment not exceeding two years and a fine.[27]

[27] http://www.cybercrimelaw.net/laws/countries/italy.html.

# Japan

## Critical Sectors

The critical infrastructures of Japan are defined in the Action Plan on Information Security Measures for Critical Infrastructures that was issued by the Information Security Policy Council in 2005: "Critical infrastructures are formed by business entities providing highly irreplaceable services and are essential for people's social lives and economic activities. If an infrastructure's function is suspended, reduced or unavailable, people's social lives and economic activities will be greatly disrupted."[1] The paper lists the following ten sectors that are deemed to be critical:

[*] The Country Survey of Japan 2008 was reviewed by Toshihiko Suguri and Yoshihiro Sato of the National Information Security Center (NISC), Tohru Nakao and Tomoko Makino of the Ministry of Internal Affairs and Communications (MIC), and Mika Shimizu of the East-West Centre.

[1] Information Security Policy Council. "Action Plan on Information Security Measures for Critical Infrastructures", p.2. http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng.pdf.

- (Tele-) Communication,
- Government and Administrative Services,
- Finance,
- Civil Aviation,
- Railways,
- Logistics,
- Electricity,
- Gas,
- Medical Services,
- Water.

## Past and Present Initiatives and Policies

The government of Japan, based on the Action Plan of the Basic Guidelines Toward the Promotion of an Advanced Information and Telecommunications Society of 1998[2], has been steadily promoting policies contributing to the advancement of information technology and telecommunications in Japan.[3]

The Comprehensive Strategy on Information Security, released in 2003 by the Ministry of Economy, Trade, and Industry (METI) was the next step of the policy development process. In this document, ICT-related risks and threats confronting the Japanese society were explicitly considered from a national-security perspective.[4]

[2] Decision of the Advanced Information and Telecommunications Society Promotion Headquarters (9 November 1998).

[3] "Outline of the First Follow-up of the Action Plan of the Basic Guidelines Toward the Promotion of an Advanced Information and Telecommunications Society" (19 May 2000). http://www.kantei.go.jp/foreign/it/2000/0706outline.html.

[4] "Comprehensive Strategy on Information Security: Executive Summary." Chapter 1.2: "New Dimensions of Risks Confronting Society as a Whole" (no date). http://www.meti.go.jp/english/information/downloadfiles/cInfo031216e.pdf.

In 2005, the First National Strategy on Information Security was issued. This is now the most important policy paper and provides the basis for all other guidelines and action plans related to CIIP and information security.[5]

## The First National Strategy on Information Security

In October 2003, the Information Security Committee of the METI published the Comprehensive Strategy on Information Security.[6] This document was the starting point for the development of a national strategy on information security, because it highlighted the need for a comprehensive approach to bring about and improve a highly reliable Information Society in Japan. Most importantly, the Comprehensive Strategy called for a clear definition of responsibilities within the government and promoted the development of a dedicated organization for information security within the Cabinet Secretariat.

In 2005, the propositions of the Comprehensive Strategy were implemented. A council and an organization were established within the Cabinet Secretariat (the Information Security Policy Council (ISPC) and the National Information Security Center (NISC)), and a new national strategy was elaborated. This strategy, called The First National Strategy on Information Security – Towards the Realization of a Trustworthy Society,[7] is a mid- and long-term strategy formulating clear goals for the years 2006–2008. The Information Security Policy Council issued separate implementation plans for each of these three years.[8]

In general, the strategy aims to make Japan an advanced nation in the field of information security. Most importantly, the strategy aims to establish a new public-private partnership model to improve information security. Thus, the strategy defines the roles of government, critical infrastructures, businesses, and individuals, and the measures that need to be implemented by these actors:

[5] "Japanese Government's Efforts to Address Information Security Issues". http://www.nisc.go.jp/eng/pdf/overview_eng.pdf.

[6] http://www.meti.go.jp/policy/netsecurity/downloadfiles/strategy_summary_English.pdf.

[7] http://www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf.

[8] "Secure Japan 2006: First Step Towards a Trustworthy Society". http://www.nisc.go.jp/eng/pdf/sj2006_eng.pdf, and "Secure Japan 2007: upgrading of information security measures in order to create an environment in which people can use IT safely and securely". http://www.nisc.go.jp/eng/pdf/sj2007_eng.pdf.

- Central and local governments are required to define best practices for information security and implement these practices in their agencies. By defining and implementing standards for information security, the government shall increase the overall ability to respond to emergencies, including cyber-attacks;
- Critical infrastructures must ensure stable provision of their services. The major step to prevent disruptions of critical infrastructures is the development of so-called Capabilities for Engineering of Protection, Technical Operations, Analyses, and Response (CEPTOAR; for more detail, see the chapter on Organizational Overview) for each major sector. The Action Plan on Information Security Measures for Critical Infrastructures defines the strategy for critical infrastructures in more detail;
- Businesses need to implement information security standards and measures that are promoted by government agencies. Security audits and third-party evaluation systems shall be promoted;
- Individuals: the government aims to raise awareness of information security among users of IT services by improving information security education and by promoting user-friendly services.

The second version of the Comprehensive Strategy is being discussed as of March 2008.[9]

[9] Information provided by an expert.

## Action Plan on Information Security Measures for Critical Infrastructures

In 2000, the Cabinet Secretariat released a Special Action Plan on Countermeasures to Cyber-Terrorism of Critical Infrastructure[10], which was replaced in December 2005 by the Action Plan on Security Measures for Critical Infrastructures[11], published by the ISPC as an amendment of The First National Strategy on Information Security.

The new plan includes definitions of critical infrastructure elements and threats, safety standards for information security, information-sharing systems in public-private partnerships (PPP), interdependency analyses, and exercises. In particular, the plan emphasizes the importance of PPPs. The plan therefore aims to establish within each critical sector so-called Capabilities for Engineering of Protection, Technical Operation, Analysis, and Response (CEPTOAR, see the chapter on Organizational Overview).

In addition, the Action Plan provides for analyses of interdependencies and cross-sectoral status assessments of the critical infrastructures. For this purpose, various cross-sectoral exercises are projected. Such exercises shall be implemented in every fiscal year, based on concrete threat scenarios corresponding to the assumed threats.

## Standards for Information Security Measures for the Central Government Computer Systems

In order to achieve a sector plan for improving the information security level of the whole government, the ISPC has issued the Standards for Information Security Measures for the Central Government Computer Systems. The standards formulated by the ISPC represent the nominal level of information security in

[10] "Special Action Plan on Countermeasures to Cyber-terrorism of critical infrastructure".,(15 December 2000), provisional translation. http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN009986.pdf, and "Special Action Plan on Countermeasures to Cyber-Terrorism of Critical Infrastructure", Summary, provisional translation, (no date). http://www.kantei.go.jp/foreign/it/security/2001/cyber_terror_sum.html.

[11] http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng.pdf.

government agencies. The NISC inspects and evaluates the actual levels and compares them with the standards. In that way, it is possible to formulate recommendations for each government agency.[12]

## Organizational Overview

Within the Japanese government, the Cabinet Secretariat is the main actor in the field of CIIP and information security in general. In 2005, thr ISPC and the NISC were established within the Cabinet Secretariat. These two organizations are now the focus of CIIP policies in Japan.

In addition, the METI, the National Police Agency (NPA), and the Ministry of Internal Affairs and Communications (MIC) assist the Cabinet Secretariat and play major roles in the field of CIIP.

As a private-public partnership initiative, the so-called CEPTOAR (Capabilities for Engineering of Protection, Technical Operation, Analysis, and Response) are designed to serve the purpose of information-sharing between government and the private sector.

### Public Agencies

#### Cabinet Secretariat and IT Strategic Headquarters

The IT Strategic Headquarters, which includes all ministers and private-sector experts, was established in July 2000 within the cabinet in order to promote comprehensive measures for making Japan an internationally competitive IT nation. At the same time, the IT Strategy Council, consisting of 20 opinion leaders, was established in order to study the issue strategically and by combining private-public

[12] National Information Security Center (NISC). "Japanese Government's Efforts to Address Information Security Issues – Focusing on the Cabinet Secretariat's Efforts." Chapter 3.1. "Standards for Information Security Measures for the Central Government Computer Systems". http://www.nisc.go.jp/eng/pdf/overview_eng.pdf, p. 23ff.

partnerships.[13] In January 2001, the Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society (IT Strategic Headquarters) was launched under the provisions of the Basic Law on the Formation of an Advanced Information and Telecommunications Network Society (IT Basic Law), with the prime minister as its director-general, and including all cabinet members and opinion leaders from the private sector as members, to serve as a new base for joint government and private-sector promotion of IT policies.[14]

## Information Security Policy Council (ISPC)

The ISPC, set up in May 2005, is chaired by the chief cabinet secretary and forms part of the IT Strategic Headquarters with members from various ministries as well as private-sector experts. It plays a central role in developing and reviewing the information security strategies and policies. Thus, the ISPC has the following tasks:

- To develop and review strategies with regard to information security;
- To undertake proactive and retrospective assessments of information security policy, based on the basic strategy;
- To develop safety guidelines for information security that are uniform throughout government;
- To recommend information security policies based on the government-wide safety guidelines.

## The National Information Security Center (NISC)

The NISC was launched in April 2005 as Japan's central implementing body for IT security issues. It collaborates closely with the ISPC and pursues the following tasks:

[13] E-Japan Priority Policy Program. http://www.kantei.go.jp/foreign/it/network/priority-all/1.html.

[14] Basic Law on the Formation of an Advanced Information Telecommunication Network Society. http://www.kantei.go.jp/foreign/it/network/0626_e.html.

- Planning government-wide fundamental strategies for information security policy;
- Promoting comprehensive measures on information security concerning government organizations;
- Supporting these government organizations in an appropriate way when information security incidents occur;
- Strengthening the information security of critical infrastructures;
- Reinforcing information-sharing systems;
- Implementing cross-sector cyberspace exercises;
- Creating an international strategy and promoting relationships with other countries.

## Ministry of Economy, Trade and Industry (METI)

The METI is responsible for planning and implementing various information policies under the guidance of the IT Strategic Headquarters. In particular, METI deals with e-commerce, e-government, data protection, and research and development related to IT.[15] In order to enhance the IT industry competitiveness in Japan, METI promotes policies that improve information security in companies.

## National Police Agency (NPA)

The NPA[16] has long been committed to maintaining computer and network security and investigating cyber-crimes. Traditionally, it has done this via its High-Tech Crime Prevention Department. In 1999, a new program was established to help fight high-tech crime. The High-Tech Crime Technology Division (HTCTD) was set up in the Information-Communications Bureau, and a National Police Agency Technology Center was created as the technical heart of the division. In April of 2004, the National Police Agency established

[15] http://www.meti.go.jp/english/policy/index_information_policy.html.

[16] http://www.cyberpolice.go.jp/english/action01_e.html.

the HTCTD in each Prefectural Information-Communications Department in order to enhance the capacity for technological support.[17]

Additionally, the National Police Agency is committed to creating a monitoring and emergency response service to prevent and minimize the spread of large scale cyber-related incidents, as well as to arrest so-called cyber-terrorists. One branch of this service consists of mobile technical teams, or Cyber Forces. These technical computer-security teams are stationed throughout Japan, and the Cyber Force Center acts as their command center. It monitors internet security around the clock and collects and analyzes relevant information. It is also equipped with facilities for a wide range of research and development, as well as for personnel education and training.

## Ministry of Internal Affairs and Communications (MIC)

The MIC[18] is responsible for creating the fundamental national infrastructure of Japan, including information and communications. In order to realize "secure and safe" communications as a social infrastructure, MIC promotes various policies that reinforce information security in the three categories of "Network", "Terminal System and Equipment", and "Person".

The MIC publishes an annual White Paper on Information and Communications in Japan.[19] In each edition, a special chapter deals with privacy protection as well as information security. The aim is to strengthen public-private partnership cooperation to ensure information security. Moreover, the MIC conducts research related to fundamental technologies related to measures against cyber-attacks and other network security issues and to the protection of personal information in the field of ICT, and carries out measures to upgrade emergency information functions in the telecommunications area.

The 2007 White Paper deals with ways to achieve a ubiquitous network society (u-Japan) by 2010 that allows connection to networks anytime, anywhere, by anyone, and enables an easy exchange of information. The MIC outlined the

[17] http://www.npa.go.jp/english/kokusai/pdf/Poj2007-52.pdf.

[18] http://www.soumu.go.jp/english/index.html.

[19] http://www.soumu.go.jp/joho_tsusin/eng/whitepaper.html.

future of such a society and summarized the necessary policies as the u-Japan Policy, which is based on the four principles "ubiquitous", "universal", "user-oriented", and "unique". Among these, "ubiquitous" (connects everyone and everything) plays the key role.[20]

## Public-Private Partnerships

### Capabilities for Engineering of Protection, Technical Operation, Analysis, and Response (CEPTOAR)

Public-private partnerships are an important part of CIIP policies in Japan. The Comprehensive Strategy on Information Security of 2003 already contained suggestions for cooperation between the national government and private enterprises.[21] The First National Strategy on Information Security and the Action Plan on Security Measures for Critical Infrastructures substantiated this requirement. They formulate the need for implementation of CEPTOAR within each critical infrastructure sector.

The latter serve the purpose of information-sharing between the government and the private sector. The CEPTOAR receive information from the Cabinet Secretariat (via the presiding ministries and agencies) and provide this information to their corporate members that operate critical infrastructures.[22]

In order to enable information sharing between government agencies and private companies, the NIPC issued a "traffic light" protocol for information sharing: information can be classified as red (not to be disseminated), amber (need-to-know restriction), green (can be shared among all persons concerned), or white (can be made public).[23]

[20] Ministry of Internal Affairs and Communications, Information and Communications in Japan. "2007 Report on the Current Status of Information and Communications". http://www.johotsusintokei.soumu.go.jp/whitepaper/eng/WP2007/contents.pdf.

[21] Comprehensive Strategy on Information Security (executive summary), op. cit. http://www.meti.go.jp/english/information/downloadfiles/cInfo031216e.pdf.

[22] http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng.pdf.

[23] http://www.nisc.go.jp/eng/pdf/overview_eng.pdf, p. 51.

## Early Warning and Public Outreach

### National Incident Response Team (NIRT)

The National Incident Response Team (NIRT) has been part of the IT Security Office of the Cabinet Secretariat since April 2002[24], and is in charge of the first response to cyber-incidents as the Japanese government CERT. Based on the Action Plan for Ensuring e-Government's IT Security (adopted on 10 October 2001 by the IT Security Promotion Committee), NIRT comprises 17 computer security experts from both the government and the private sector and has the following tasks:[25]

- To understand incidents correctly: To collect and analyze the related information or intelligence and make forecasts on possible future damage;
- To develop technical countermeasures for mitigation and recovery, and to prevent reoccurrence: To analyze countermeasures and to organize concrete remedies to be implemented by the ministries and agencies;
- To assist in response: To provide help-desk service for ministries and agencies, as well as response support when required;
- To collect and analyze information or intelligence in order to make predictions and provide effective incident response;
- To supply expertise, knowledge, and information to government organizations;
- To improve the necessary expertise.

### Japan Computer Emergency Response Team Coordination Center (JPCERT/CC)

JPCERT/CC[26] is an independent non-profit organization acting as a national point of contact for the other Computer Security Incident Response Teams

[24] http://www.nisc.go.jp/en/sisaku/h1310action.html.
[25] http://www.nisc.go.jp/en/shoukai/nirt.
[26] http://www.jpcert.or.jp/english.

(CSIRTs) in Japan. Since its establishment in 1992, the center has been gathering information on computer incidents and vulnerabilities, issuing security alerts and advisories, and providing incident responses as well as education and training to raise awareness of security issues. JPCERT/CC coordinates with network service providers, security vendors, government agencies, and industry associations, and is a member of the Forum of Incident Response and Security Teams (FIRST; see the survey on FIRST in this volume).

## Asia Pacific Computer Incident (Emergency) Response Team (AP-CIRT/APCERT)

The aim of the Asia Pacific Security Incident Response Coordination (AP-CIRT) is to foster close collaborations among the CIRTs (Computer Incident Response Teams) in the region.[27] In February 2003, its name was changed to Asia Pacific Computer Emergency Response Team (APCERT), and it continues to carry out its mission, which is to maintain a trusted contact network of computer security experts to improve the region's awareness and competency in relation to computer security incidents.[28]

## Telecom Information Sharing and Analysis Center Japan (Telecom-ISAC Japan)

Telecom-ISAC Japan[29] is an independent organization established as Japan's first ISAC (Information Sharing and Analysis Center) in July 2002. Telecom-ISAC Japan works to improve information security by various means such as collecting, analyzing, and sharing incident information, providing timely countermeasures and best practices, and coordinating/collaborating with related organizations, based on mutual cooperation between a wide variety of members in the information and telecommunications industry, such as ISPs, carriers, and manufacturers.

[27] See the membership list: http://www.apcert.org/about/structure/members.html.

[28] http://www.apcert.org/about/mission/index.html.

[29] https://www.telecom-isac.jp/index.html.Information provided by an expert.

## Cyber Force

The Cyber Force, a section within the police, gathers data on the internet around the clock and looks for evidence of cyber-crime. When the Cyber Force detects an unusual phenomenon, it provides critical infrastructure operators with security information to prevent cyber-terrorism and conducts vulnerability tests. Additionally, the Cyber Force will give operators of critical infrastructures advice on how to limit the damage from such an incident and how to recover their services safely, and to find the cause of the incident.[30]

## @police

The National Police Agency has a security portal site, @police, whose purpose is to prevent large-scale cyber-related incidents or keep them from spreading by quickly providing information gathered by the police on information security. Moreover, @police makes efforts to increase security awareness among internet users. Therefore, it provides a wealth of diverse content in order to help as many people as possible improve their security. Special online security courses, examples of internet crimes and how to avoid them, quick security checks, and information on security holes are provided for the benefit of private PC users as well as server administrators.[31]

## Ministry of Economy, Trade and Industry (METI)

METI has responded to security breaches in cooperation with JPCERT/CC and the Information Technology Promotion Agency (IPA) since 1990. Around that time, it also began releasing reports on computer viruses and unauthorized access and started to gather information about damage caused by computer viruses and disseminating it to the public immediately after the incident.[32]

[30] http://www.cyberpolice.go.jp/english/action02_e.html.

[31] http://www.cyberpolice.go.jp/english.

[32] Yutaka Hayami. “Realizing a World-Class Highly Reliable Society”. http://www.aavar.org/2004web/AVAR2004/Presentations/ps011.ppt.

## Law and Legislation

### Unauthorized Computer Access Law 1999

The Unauthorized Computer Access Law No. 128 of 1999 prohibits acts of unauthorized computer access (Article 3) as well as acts that facilitate unauthorized computer access (Article 4).

Article 3 covers acts such as:

- Facilitating a specific use that is restricted by an access control function, by entering via a telecommunications line another person's identification code into a specific computer that controls access;[33]
- Facilitating a specific use that is restricted by an access control function, by entering via a telecommunications line any information (excluding an identification code) or command that can evade the restrictions of that access control function for that specific purpose;
- Facilitating a specific use that is restricted by an access control function, by operating a computer whose specific use is restricted by an access control function installed on another specific computer that is connected, via a telecommunication line, to that specific computer, by entering via a telecommunications line any information or command that can evade the restriction concerned.

Article 4 makes it illegal to provide another person's identification code relating to an access control function to a person other than the access administrator for that access control function, or to the authorized user for that identification code, while indicating that it is the identification code for a specific computer's specific use, except where such acts are conducted by the access administrator, or with the approval of that access administrator or of the authorized user.

[33] To exclude such acts conducted by the access administrator who has added the access control function concerned, or conducted with the approval of the access administrator concerned or of the authorized user for that identification code.

Moreover, the Japanese Penal Code, Article 258, makes it illegal to damage documents or electronic-magnetic records in public or private use.[34]

## Act on Electronic Signatures and Certification Business 2000

The Act on Electronic Signatures and Certification Business No. 102 of 2000 aims to promote the distribution of information by electromagnetic forms and information processing by ensuring easy use of electronic signatures, and thereby to contribute to the improvement of citizens' quality of life and the sound development of the national economy, by providing the presumption of authentic establishment of electromagnetic records, the accreditation system for designated certification businesses and other necessary matters, with respect to electronic signatures.[35]

## Basic Law on Formation of an Advanced Information and Telecommunication Network Society 2001

The purpose of the IT Basic Law, which entered into force on 6 January 2001, is to promote measures for forming an advanced information and telecommunications network society where citizens can enjoy the benefits of ICT. Its measures include (Articles 16–24) the formation and expansion of advanced ICT networks; the promotion of fair competition; increasing IT user skills and development of expert human resources; reform of regulations and facilitation of e-commerce through appropriate protection; promotion of e-government and digitalization of administration; assuring security and reliability for networks and the protection of personal data; promotion of creative research and development; and international cooperation.[36]

[34] http://www.cybercrimelaw.net/laws/countries/japan.html.

[35] http://www.cas.go.jp/jp/seisaku/hourei/data/aescb.pdf.

[36] http://www.kantei.go.jp/foreign/it/it_basiclaw/it_basiclaw.html.

# Republic of Korea

## Critical Sectors

The critical information and communication infrastructure plays a crucial role in providing public safety and stable services that are essential for everyday life. In Korea, the following sectors are counted among the critical infrastructures that are heavily dependent on information and telecommunication technologies.

- E-Government and National Government Administration,
- National security,
- Emergency/Disaster Recovery Services,
- National Defense,
- Media Service, e.g., Broadcasting Facilities,
- Financial Service,
- Gas and Energy, e.g., Power Plants,

* The Country Survey of the Republic of Korea 2008 was reviewed by Heung Youl Youm, Professor at the Department of Information Security Engineering of Soonchunhyang University.

- Transportation, e.g., Subways and Airports,
- Telecommunication.[2]

## Past and Present Initiatives and Policies

### Report on the Status of the Critical Information Infrastructure

In 2001, the Korean Information Security Agency (KISA) published a Report on the Status of the Critical Information Infrastructure. The scope of the research was:

- To provide technical consulting for critical information infrastructure management agencies to perform a risk assessment and establish safeguards;
- To evaluate the security and confidentiality of internet data centers;
- To assign information-security consultants for information infrastructure.

These efforts resulted in a model and guidelines for vulnerability analysis and assessment of critical information infrastructures, including a protection guide and protection measures; a vulnerability analysis and assessment model; a guide to risk computation; asset classification; threat classification; and vulnerability analysis. In addition, technical consulting was provided for the former Ministry of Information and Communication[3] now the Korea Communications Commission.

[2] Lim Chaeho. "Creating Trust in Critical Network Infrastructures: Korean Case Study", 20 May 2002 (slides). http://www.itu.int/osg/spu/ni/security/workshop/presentations/cni.14.pdf. Cf. also Lim Chaeho. "Creating Trust in Critical Network Infrastructures: Korean Case Study", p. 4. Paper presented at the ITU Workshop on Creating Trust in Critical Network Infrastructures, (Seoul, 20–22 May 2002). http://www.itu.int/osg/spu/ni/security/docs/cni.05.doc.

[3] Korean Information Security Agency (KISA). "Report on the status of the Critical Information Infrastructure", 12 January 2001. http://www.kisa.or.kr/index.jsp.

## e-Korea Vision 2006

In April 2002, the Ministry of Information and Communication published its third master plan for Informatization Promotion for the years 2002–2006, called e-Korea Vision 2006,[4] in consultation with the Korean Informatization Promotion Committee[5] It followed the first master plan of informatization promotion devised in 1996 and the second, called Cyber Korea 21, drawn up in 1999. e-Korea Vision focuses on "Ensuring Safety and Reliability of Cyberspace" to strengthen the security of the critical information infrastructures. Government policies relevant to the vision paper include the following:

- Identifying critical information infrastructures that are important for national security and the economy, systematic analysis of vulnerabilities and preparation for protective plans, and establishment of cooperation between the public and private sectors in order to prevent cyber-attacks and intensify response measures;
- Reinforcement of real-time warning systems to fight against hacking and viruses and strengthening international cooperation, because cyber-terrorism is intrinsically transnational;
- Developing information security technologies and training new information security experts to meet the changing needs of the information security environment;
- Strengthening cooperation between the government and the private sector for a sound and healthy cyberspace;
- Devising plans to establish information ethics that enable a secure cyberspace, and encouraging voluntary regulation of the private sector in terms of online information circulation.

[4] http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN008975.pdf.

[5] Ministry of Information and Communication. "e-Korea Vision 2006. The Third Master Plan for Informatization Promotion" (2002–2006), (April 2002). http://www.nca.or.kr/homepage/ehome/ehome.nsf/0/4f84e7068921413ec9256ce80024c20a/$FILE/e-Korea%20Vision%202006.pdf.

With the designation of major information and communication facilities as critical to the national defense and the economy, the government plans to conduct a systematic analysis of their weaknesses and implement strong security measures to protect these facilities. The government has established an Information Sharing and Analysis Centre (ISAC) for each area of the government and the financial and information sectors. In addition, standards have been developed for information security technologies, together with an evaluation methodology for information security systems. [6]

## Basic Strategy for Ubiquitous Information Security

The downside of the information revolution is seen in the growing number of cyber-attacks on the internet, infringement of private information, and spam. According to a vision called u-Korea, based on the four principles "ubiquitous" (connects everyone and everything), "universal", "user-oriented", and "unique", the resulting damage would not be limited to individuals, but would affect the whole society and its economy, and even pose a threat to the life and property of its citizens. Therefore, a new framework of information protection is required that takes the new virtual ubiquitous environment into account.

In May 2005, the Ministry of Information and Communication issued a report on the Mid- to Long-Term Roadmap for Information Protection dealing with the security of high-technology infrastructures and the establishment of reliable systems for new IT services. In particular, the report presents a phased roadmap from 2005 to 2008 for the prevention of attacks on the internet, advanced response measures, reinforced protection of privacy, improvement of the legal system regarding information protection, and the training of a specialized force.[7]

In December 2006, the Ministry of Information and Communication established the Basic Strategy for Ubiquitous Information Security. The strategy aims to strengthen the global competitiveness of Korean industries; improving the

[6] http://www.ipc.go.kr/ipceng/policy/vision_ground.jsp?num=1.

[7] http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN027266.pdf.

existing legal and regulatory system, and promoting research and development in the field of ICT. It defines four specific policy goals:[8]

- Secure infrastructures: developing a more efficient incident response system, minimizing threats, protecting critical infrastructures from cyber-attacks;
- Privacy Protection of users: privacy protection of location information, protection of biometric and healthcare information, protection of personal information and personally identifiable information;
- Trusted IT services and devices: developing authentication and ID management systems, developing techniques for making IT services secure, providing a base for secure electronic transactions;
- Clean internet environment: preventing the dissemination of illegal and harmful traffic on the internet, spreading a culture of security, raising users' awareness.

## Organizational Overview

In general, all governmental organizations and their subsidiary organizations are in charge of CIIP.

The National Cyber Security Center (NCSC) coordinates the efforts of these departments and agencies. In the field of cyber-crime investigation and prevention, the Internet Crime Investigation Center (ICIC) under the authority of the Supreme Public Prosecutors' Office plays a central role. The Electronics & Telecommunications Research Institute has the leadership in developing technology and providing support to protect critical information infrastructure. The Ministry of Public Administration and Security, the Korea Communications Commission (the former Ministry of Information and Communication), and the Korea Internet Security Center (KISC; KrCERT/CC) within the Korean

[8] Heung Youl Youm. "Countermeasures for Combating Cyber Attacks in Korea", p. 40, (2007). http://www.itsc.org.sg/pdf/6thmtg/Korea-Malaysia-Singapore-S.pdf. MIC; Basic plan for ubiquitous information security (in Korean). Information provided by an expert.

Information Security Agency (KISA) are undertaking efforts to foster a culture of safe internet and telecommunication networks.

In addition, the structure of government organization was changed in February 2008. According to new regime plan, the Ministry of Information and Communication was abolished, and its functions in the area of information security were transferred to several ministries: the Ministry of Public Administration and Security, the Ministry of Knowledge and Economy, and the Korea Communication Commission. Therefore, the Ministry of Public Administration and Security, the Korea Communications Commission, and the Ministry of Knowledge and Economy have begun sharing CIIP-related responsibilities in Korea.

As a public-private partnership, the national Information Security Alliance (NISA) strives to improve information security by fostering information exchange between governmental agencies, enterprises, and research institutes. The Financial Information Security Alliance has members from banks and insurance companies and strives to implement international information protection policies. The Information Security Practice Alliance is an initiative fostering information protection activities in the private sector, and the Korea Information Security Industry Association (KISIA) is an exchange platform for the information security industry.

## Public Agencies

### Ministry of Public Administration and Security (MOPAS)

As a result of the government restructuring, the Ministry of Public Administration and Security (MOPAS), a government department that is responsible for electronic-government and public administration services, began to play a primary role in information security tasks including CIIP-related missions in March 2008. The informatization strategy office, which is part of MOPAS, is responsible for information security matters in the private sector. It pursues the following tasks:

- Establishing an information security policy for private sector;

- Ensuring the protection of users' privacy;
- Dealing with electronic authentication;
- Cultivating a sound internet culture for the public and private sectors.[9]

## Korea Communications Commission (KCC)

As a result of the government restructuring in February 2008, the Korea Communications Commission (KCC), a government department that is responsible for establishing the policy for communications and digital broadcasting, began to play a primary role in tasks of the network security in March 2008. It pursues the following tasks:

- Establishing a network security policy;
- Ensuring the protection of internet users' privacy.[10]

## National Cyber Security Center (NCSC)

The government established the National Cyber Security Center (NCSC)[11] in February 2004. It not only coordinates the efforts of the Korean governmental departments and agencies in charge of CIIP, but is also a platform that brings together the private, public, and military sectors to fight cyber-threats. This is based on the understanding that cooperation among all sectors is crucial for the effective prevention of cyber-attacks as well as for the minimization of damage. The NCSC operates under the auspices of the National Intelligence Service (NIS) and is the central point of government for identifying, preventing, and responding to cyber-attacks and threats in Korea. NCSC performs the following tasks:

- Overall management of national cyber-security by working out plans and guidelines to improve national cyber-security systems, as well as providing support for strategic committee meetings;

[9] http://www.mopas.go.kr.
[10] http://www.kcc.go.kr.
[11] http://www.ncsc.go.kr.

- Publishing national cyber-security manuals, security guidelines, and analysis reports, and collecting, analyzing, and distributing information on cyber-threats;
- Detecting and responding to cyber-threats, issuing warnings and information on cyber-incidents, and developing cyber-security technology;
- Preventing the spread of cyber-attacks, providing support for recovery procedures, and establishing and managing pan-governmental working groups for prompt response measures;
- Promotion of cooperation among international and domestic IT security organizations;
- Education and public relations regarding cyber-security issues.
- In addition, NCSC operates early-warning services (see the chapter on Early Warning and Public Outreach).[12]

## Internet Crime Investigation Center (ICIC)

The Supreme Public Prosecutor's Office and the Seoul District Public Prosecutor's Office have established the Internet Crime Investigation Center (ICIC)[13] to deal more effectively with internet-related crimes. The ICIC monitors crime trends such as hacking, the spread of viruses, fraud in electronic commerce, and infringement of privacy. In doing so, it develops more effective response measures and new investigative methods to crack down on cyber-crimes. Moreover, to maximize its investigation capacity, it maintains close cooperation with international and domestic organizations. The ICIC is operated by a high-tech crime investigation team of the Central Investigation Department and performs the following tasks:

- Intensive and systematic monitoring of cyber-crime trends;
- Collecting reports on cyber-crimes;
- Developing effective investigation methods;

[12] http://ncsc.go.kr/eng/files/20080123112558_NCSC_M0801.pdf.

[13] http://www.icic.sppo.go.kr.

- Improving the legal system in the field of cyber-crime;
- Around-the clock monitoring system to respond to high-tech crime.

## Korea Information Security Agency (KISA)

The Korea Information Security Agency (KISA),[14] affiliated with the Korea Communications Commission (the former Ministry of Information and Communication), was established in 1996 to create a safe, reliable information environment in Korea by reacting effectively to various acts of electronic infringement and intrusion. KISA is devoted to enhancing the security and reliability of electronic transactions by developing and supplying cryptographic algorithms. In addition, KISA has supported the development of information security in Korea through evaluations of IT-security products, IT-security education, public awareness campaigns, information security policy, and research and standardization in support of the legislative framework. In January 1998, KISA became a member of the Forum of Incident Response and Security Teams (FIRST; for more information on FIRST, see the FIRST chapter in this volume).

KISA opened the Korea Certification Authority Central in 1999, and the Personal Information & Privacy Protection Center in 2000. In addition, the Korea Information Security Industry Support Center (KISIS) was established under KISA in 2001. The Korea Internet Security Center (KISC, KrCERT/CC)[15] was founded in 2003 (see the chapter on Early Warning and Public Outreach), the Korea Spam Response Center (KSRC) also in 2003, and the Korea IT Security Evaluation Center (KISEC)[16] began its work in 2004.

In accordance with the Information Infrastructure Protection Act and the Act on Promotion of Utilization of Information and Communication Network and Data Protection, which became effective as of July 2001, KISA acquired additional duties such as the analysis and evaluation of the vulnerabilities of the critical information infrastructure, and the certification of information security management systems.

[14] http://www.kisa.or.kr/index.jsp.

[15] http://www.certcc.or.kr/english/vision.htm.

[16] http://www.kisa.or.kr/kisae/kisec/jsp/kisec_6010.jsp.

KISA includes an Information Infrastructure Protection Division with a CIIP Planning Team, a Critical Infrastructure Security Management Team, and the Korea Certification Authority Central Team, providing:

- Vulnerability analysis and assessment, including technical consulting and vulnerability analysis for facilities designated as CII;
- Security technology service for CII, including technical consulting for CII management agencies to establish safeguards and help in computer system recovery;
- Certification for information security management systems, including certifying integrated information security management systems, as well as technical and physical safeguards.[17]

## Electronics and Telecommunications Research Institute (ETRI)

The Information Security Research Division, a part of the Electronics and Telecommunications Research Institute (ETRI),[18] is developing advanced technologies in the area of information security for the private sector in Korea and supporting rapid industrialization of those technologies to resolve impediments to the emergence of the Information Society such as malfunctions of the Broadband Convergence Network infrastructure, the exchange of unsound and harmful information, and leaking of personal information, all of which are obstacles to the creation of a knowledge-based society. It aims to establish leadership in information security technology in order to approach the ideal of a secure u-Korea (see the chapter on the Past and Present Initiatives and Policies). This division focuses on four major research areas: Network Security, Ubiquitous Security, Biosecurity, and Security Chipset Technology.

The National Security Research Institute (NSRI), an affiliated research institute of ETRI,[19] is managed by the Ministry of Science and Technology.[20]

[17] http://www.kisa.or.kr.

[18] http://www.etri.re.kr/eng.

[19] http://www.etri.re.kr/www_05/e_etri.

[20] http://www.most.go.kr.

NSRI contributes to the public welfare by developing technology for protecting critical information infrastructures and enables the government to exercise information sovereignty by providing national security technology and policies required to protect the country and public organizations from cyber-attacks. NSRI deals with:[21]

- Developing technology to deal with cyber-terror and cyber-attacks, and for evaluating information protection systems, as well as to ensure the reliability and viability of governmental and military critical information infrastructures;
- Raising awareness of CIIP and giving seminars;
- Analyzing weaknesses in the government, public, and military sectors;
- Supporting Korea's e-Government strategy for information protection;
- Demonstration projects in the area of information protection for governmental organizations.

## Information and Telecommunication Infrastructure Protection Committee

The Information and Telecommunication Infrastructure Protection Committee, which is chaired by the viceminister for State Affairs of the Prime Minister's Office[22] and whose members are appointed by the chiefs and chairpersons of central administrative organizations, reviews items related to critical information infrastructures. The chairperson of the Information and Telecommunication Infrastructure Protection Committee can set up the Joint Working Group for Security Incident Response in order to provide emergency measures, technological support, and recovery procedures in the case of a large-scale security incident.[23] This committee was established in accordance with Article 3 of the Critical Information Infrastructure Protection Act. However, the Ministry of

[21] http://www.nsri.re.kr/kor/index.html.

[22] http://www.opm.go.kr/warp/webapp/content/view?meta_id=english&id=1.

[23] Chaeho, op. cit., p. 4.

Public Administration and Security in May 2008 announced plans to abolish this committee.

## Public-Private Partnerships

### National Information Security Alliance (NISA)

The National Information Security Alliance (NISA) was established in September 2002 to improve information security by facilitating information exchange, presenting policies, and concentrating pan-governmental efforts. The alliance consists of 22 major governmental organizations, such as the Ministry of National Defense, the Ministry of Public Administration and Security, and the Korea Communications Commission, as well as information security officials from 17 public enterprises, communication network providers, the Korea Information Security Industry Association, research institutes, and experts from industry and academia. One main aspect of NISA's work is the executive meeting of chairpersons of the National Information Security Alliance, the Public Enterprise Information Security Alliance, and the Industrial-Educational-Research Information Security Alliance as a way of improving cooperation, while guaranteeing the autonomy of each of these actors within the alliance. [24]

### Financial Information Security Alliance

The Financial Information Security Alliance was established in October 2002 to protect financial information security systems from cyber-terror and hacking, and to implement changes in international information protection policies such as the Banking Industry Technology Secretariat (BITS). The alliance has 87 members (20 banks, 27 security corporations, 30 insurance companies, and ten non-bank financial institutions). The Financial Information Security Alliance develops information protection standards and policies for the financial sector, as well as assessments and certifications. It also performs research in the field of information security and provides education.[25]

[24] http://www.nisa.or.kr/link_2.php.

[25] Information provided by an expert.

### Information Security Practice Alliance

The Information Security Practice Alliance was set up in July 2002 as a way of voluntarily increasing information protection activities in the private sector, in cooperation with various security companies and associations and with the help of the KISA. KISA has introduced a variety of projects in order to promote information protection campaigns with voluntary efforts from the public.[26]

### Korea Information Security Industry Association (KISIA)

The KISIA was established in July 1998 as a platform for nurturing the information security industry (KISA has more than 150 members). Moreover, KISIA became a corporation in 2004 in accordance with Section 2 of Article 59 of the Act on Telecommunication Network Usage Promotion and Information Protection. It proposes measures to improve the legal system relevant to information security, trains specialized forces in the field, does joint research on innovative technology, analyzes market trends to understand the status of information security industry and to make plans, solves IT problems of the industry, reflects the opinions of members on governmental policies, promptly shares information with related authorities through an integrated system, provides support for participating in information security seminars or expositions, and promotes joint research with governmental or other related organizations.[27]

## Early Warning and Public Outreach

### National Cyber Security Center (NCSC)

The National Cyber Security Center (NCSC) takes preventive measures against cyber-threats. It also analyzes collected information on IT security, traffic, and capacity, using the service networks of numerous organizations, including govern-

[26] Ibid.

[27] http://www.kisia.or.kr/new.

ment high-speed networks. Moreover, NCSC issues color-coded cyber-threat warnings ("green", "blue", "yellow", "orange", and "red"). It also distributes various security guidelines and information on worms and viruses, security news, cyber-incidents, and security technology to the private, public, and military sectors.[28] Furthermore, if a cyber-incident takes place, NCSC staff is dispatched to the site to investigate its cause and swiftly restore the system. The NCSC staff also examines the security of systems to prevent similar incidents in advance. Besides, the security center has organized a response team alliance dealing with national cyber-attacks, and is installing an emergency contact system for affected organizations.[29]

## Korea Internet Security Center (KISC, KrCERT/CC)

The Korean Internet Security Center (KISC, also called the Korea Computer Emergency Response Team Coordination Center, or KrCERT/CC), established in 2003, aims at raising the technical capability for the protection of critical network infrastructure in order to create a safe internet and communication network. KISC develops effective countermeasures against hacking and viruses, such as cyber-attack countermeasure methodology and attack tools. KISC is organized into five major teams:

- Incident Analysis Team,
- Response Coordination Team,
- Hacking Response Team,
- Spam Response Team,
- Botnet Response Team,
- Network Monitoring Team.

KISC responds to threats against IT networks and has built cooperation systems with relevant organizations in order to immediately handle incidents. As a

[28] For example, the NCSC issues the "NCSC Monthly", which contains information about incidents, cyber-threat trends, response activities, and analysis results. http://www.ncsc.go.kr/eng.

[29] http://www.ncsc.go.kr/eng.

member of FIRST, KISC does its utmost to fulfill its duties in cooperation with international organizations. The tasks of KISC (KrCERT/CC) are as follows:

- Technological support to prevent cyber-incidents;
- Analysis of cyber-incidents, analysis of malicious codes and their destructive power, and development of response and recovery measures;
- Analysis of network traffic and the status of the internet, monitoring of vulnerabilities at the national and the international levels;
- Analysis of the latest hacking tools and development of response measures;
- Receiving reports on spam, making improvements to the legal system, and analyzing domestic as well as international trends;
- Reinforcing cooperation with international CERTs;
- Dealing with phishing, activating CERTs, and raising awareness in the private sector.[30]

## Information Sharing and Analysis Center (ISAC)

In 2001, the first Korean Information Sharing and Analysis Center (ISAC) was established, after regulations were enacted according to Article 16 of the National Information Infrastructure Protection Act. The aim of ISACs is to prevent cyber-attacks on critical information infrastructures by sharing information on incidents with other companies and with the authorities concerned.[31]

In Korea, there are three ISACs, each of them addressing businesses of a different sector:

- The KS-ISAC (Korean Security Information Sharing and Analysis Center) was the first ISAC in Korea. It offers a database on cyber-incidents,

[30] http://www.certcc.or.kr/english/vision.htm.

[31] The first ISACs were established in the US (see country survey on the United States in this volume).

vulnerabilities, and patches, shares information with relevant organizations outside the ISAC, and provides information online;[32]

- The KF-ISAC (Korea Financial Information Sharing and Analysis Center) was established in 2002 within the Korean Financial Telecommunication and Clearings Institute (KFTC). It provides various information security services to the participating members, especially customized for the Korean banking industry. The most important services are information security reports; real-time monitoring and warning services; information security checks for core systems; and education and training services;[33]
- The Korean Telecommunication ISAC was also established in 2002. It aims to provide its members with the opportunity to share proper information on incidents and to exchange experiences and insights. The ISAC gathers and disseminates information obtained from different sources, such as CERTs or other information-security associations.[34]

## Law and Legislation

### Information Security Promotion Systems

Information-security promotion systems in Korea can be divided into national cyber-security systems, e-Government security systems, critical information infrastructure systems, and private information security systems. With respect to the national cyber-security system, the National Cyber Security Management Regulation was issued by a presidential directive on 31 January 2005, which regulates cyber-security organizations such as the National Cyber Security Strategy Council or the National Cyber Security Center. Meanwhile, for e-Government security systems, the Act on Promotion of Electronic Administration for e-

[32] http://www.allbusiness.com/company-activities-management/management-benchmarking/6058179-1.html.

[33] http://www.kftc.or.kr/english/business/kf.html.

[34] https://www.isac.or.kr/english/e_intro.swf.

Government, enacted on 28 February 2001, regulates matters of information protection as well as e-Government.[35]

## Digital Signature Act 1997

The Digital Signature Act was enacted by Korea Parliament on July 1997 and revised on 31 December 2005[36]. The purpose of the Digital Signature Act is to endow electronic documents with an equal level of legal validity as paper documents and to regulate basic matters related to achieving reliability, protect consumer rights, and implement policies, and thus to promote electronic commerce, with a view to creating a legally predictable environment in which the private citizens can make secure transactions in the Information Age. It contains provisions on "definition of digital signature", "licensed certification authority", "public-key certificate", "security and trust for certification service", and "electronic certification policy", etc. Responsibility for implementing this act has resided with the Ministry of Public Administration and Security since March 2008.

## Act on Promotion of Utilization of Information and Communication Network and Information Protection 1999

The Act on Promotion of Utilization of Information and Communication Network and Information Protection was enacted on 1999 and revised on December 2007[37] The purpose of this act is to promote the use of information and communications networks, to protect users' personal information when they are using information and

[35] Information provided by an expert.

[36] Digital Signature Act (in Korean). http://www.klaw.go.kr/, Heung Youl Youm. "Countermeasures for Combating Cyber Attacks in Korea", p.40, 2007. http://www.itsc.org.sg/pdf/6thmtg/Korea-Malaysia-Singapore-S.pdf. MIC; Basic plan for ubiquitous information security (in Korean). Information provided by an expert.

[37] Act on Promotion of Utilization of Information and Communication Network and Information Protection (in Korean). http://www.klaw.go.kr/. Heung Youl Youm. "Countermeasures for Combating Cyber Attacks in Korea", p. 40, 2007. http://www.itsc.org.sg/pdf/6thmtg/Korea-Malaysia-Singapore-S.pdf. MIC. Basic plan for ubiquitous information security (in Korean). Information provided by an expert.

communications services, and to construct an environment within which users can safely use information and communications networks. It consists of many articles governing the utilization of digital documents through relay servers, protection of personal information, protection of juveniles in information and communication networks, securing the safety of information and communications networks, and other issues. Responsibility for implementing this act has been shared by the Ministry of Public Administration and Security, the Korea Communication Commission, and the Ministry of Knowledge and Economy since March 2008.

## Act on Private Information Protection of Public Organizations 1994

The Act on Personal Information Protection by Public Organization, enacted in 1994 and revised in 1998, aims to ensure the adequate performance of public duties and to protect the rights and interests of users by protecting personal information processed by computers.[38]

## Critical Information Infrastructure Protection Act 2001

The ministerial meeting on the prevention of large scale cyber-related incidents in February 2000 decided to pass a law covering comprehensive and systematic information infrastructure protection and countermeasures against so-called cyber-terrorism. The Critical Information Infrastructure Protection Act was enacted in January 2001 and revised in December 2007. It serves as a fundamental law protecting critical information infrastructure from various cyber-incidents. A critical information infrastructure was defined as a public or private network that carries information relevant to national security and safety or information of high financial value. The critical ICT infrastructure can also be defined physically as the whole network or a part of the network that exchanges information of high significance. This law consists of many articles defining the critical information

[38] Act on Private Information Protection of Public Organizations (in Korean). http://www.klaw.go.kr/. Information provided by an expert.

and communication infrastructure, outlining protective measures and responses against cyber incidents, defining the work of the information security consulting agency, and specifying legal responsibilities and penalties. It outlines the government framework for critical information infrastructure protection. It directs the affairs of the Critical Information Infrastructure Protection Committee, the Working Group for Security Incident Response, and other central administrative organizations. Moreover, protection measures, prevention and response, technical support, development of technologies, international cooperation, and penalties for cyber-crimes are addressed.[39] Responsibility for enforcing this act has rested with the Ministry of Public Administration and Security since March 2008.

In addition, the Act on Private Information Protection of Public Organizations, the Act on Promotion of Electronic Administration for e-Government, and the Resident Registration Act in the public sector, as well as the Act on Promotion of Utilization of Information and Communication Network and Information Protection in the private sector deal with private information security systems.[40]

## e-Commerce Framework

As electronic transactions and commerce across long distances become more common due to the development of ICT networks, a legal framework has been established regarding electronic signatures and their certification, in order to secure the safety and reliability of electronic documents that are drawn up by data processing systems and then transferred, received, or saved. The Digital Signature Act and the e-Commerce Framework Act regulate certification of electronic signatures, and the Act on Promotion of Electronic Administration for e-Government governs the use of digital signatures in the public administration.[41]

[39] Cha Yang-Shin. "Korea's Approach to Network Security", (21 May 2002). http://www.itu.int/osg/spu/ni/security/workshop/presentations/cni.21.pdf.

[40] Act on Private Information Protection of Public Organizations, the Act on Promotion of Electronic Administration for e-Government, and the Resident Registration Act in the public sector (in Korean): http://www.klaw.go.kr/. Information provided by an expert.

[41] The e-Commerce Framework Act (in Korean): http://www.klaw.go.kr/. Information provided by an expert.

## Protection of Telecommunication Networks and Information Systems

As attacks on telecommunication networks and information systems increase in the public and private sectors, the need for a systematic national-level protection system has become urgent. The Framework Act on Information Promotion, the Critical Information Infrastructure Protection Act, the Act on the Promotion of Utilization of Information and Communication Network Utilization and Information Protection, the e-Commerce Framework Act, the e-Government Act, the Act on Trade Automation Promotion, the Act on Industrial Infrastructure, and the Freight Distribution Promotion Act have been passed to protect telecommunication networks and information systems.[42]

## Cyber-Attacks

The following laws and regulations are applied in order to prevent national and social loss arising from hacking, viruses, denial-of-service (DoS) attacks on telecommunication networks as well as other information systems, and theft or forgery of information:

- Article 28 of the Critical Information Infrastructure Protection Act imposes a penalty for attacks on critical information infrastructures;
- Article 62 of the Act on the Promotion of Utilization of Information and Communication Network Utilization and Information Protection outlaws attacks on telecommunication networks and violations of a duty to protect secret information;
- Article 25 of the Act on Trade Automation Promotion, as well as Sections 2 and 4 of Article 54 of the Freight Distribution Promotion Act, may also apply.

In addition, there are provisions in the national criminal legislation dealing with computer crime.[43]

[42] http://www.klaw.go.kr.

[43] Ibid.

# Malaysia

## Critical Sectors

In Malaysia, the following sectors are regarded as making up the national critical infrastructure:[1]

- Financial Sector,
- Water and Sewerage,
- Communications and Media,
- Energy,
- Health and Emergency Services,
- Industry,
- Central Government,
- Government Services,
- Transportation,
- Military.

[1] Rahman Bistamam Siru Abdul (MCMC). Malaysia's Approach to Network Security. Presentation held at ITU Workshop on "Creating Trust in Critical Network Infrastructures", (Seoul, May 2002), slide 7. http://www.itu.int/osg/spu/ni/security/workshop/presentations/cni.19.pdf.

# Past and Present Initiatives and Policies

## National IT Agenda (NITA) and NITC Strategic Agenda

Malaysia launched the National IT Agenda (NITA) in 1996 as part of a major strategy to prepare the nation for the challenges of the information age. The agenda contains an outline for a national framework aimed at ensuring a balanced IT development for Malaysia, its infrastructure, and the applications found within. According to NITA, for this effort to succeed, Malaysia requires greater trust and faith in the use of information and communication technology (ICT), which can be fostered through enhanced ICT security.[2] The launch of NITA provided the foundation and framework for the utilization of information and communication technology to transform Malaysia into an information and knowledge society.

Besides NITA, the National Information Technology Council (NITC) (see the chapter on Organizational Overview) formulated the NITC Strategic Agenda, a strategy involving a more participatory governance structure with active partnership between the public, private, and community-interest sectors. The Strategic Agenda includes concepts such as e-Community, e-Public services, and e-Economy. It is based on the assumption that knowledge and information will be the most valuable assets in the new economy.[3]

## e-Secure Malaysia 2005 International Conference

A major information security event, e-Secure Malaysia 2005, took place in September 2005 in Kuala Lumpur. It consisted of two conferences and an exhibition targeted at security professionals, solution providers, policymakers, corporate decisionmakers, and government officials. The event was jointly organized by various government agencies such as the Ministry of Science, Technology and Innovation (MOSTI); the Ministry of Energy, Water and Communications

[2] http://www.cybersecurity.org.my/en/index.html.

[3] http://www.msctc.com.my/idb/B-1.htm.

(MEWC); the Malaysian Communications and Multimedia Commission (MCMC); the National ICT Security and Emergency Response Centre (NISER); and the Malaysian Administrative Modernisation and Management Planning Unit (MAMPU). The conference focused on the following topics: Computer Emergency Response Teams (CERTs) and incident response; critical infrastructure protection; network and application security; security management and strategy; and knowledge-sharing.[4]

## Organizational Overview

The Malaysian Communications and Multimedia Commission (MCMC) has a coordinating role. The Malaysian Administrative Modernization and Management Planning Unit (MAMPU) administers security issues in the public sector. The Police Cyber Crime Unit is responsible for investigation and prevention of commercial cyber-crime. The Ministry of Science, Technology and Innovation (MOSTI) holds wide-ranging responsibilities concerning national ICT policy and security, while it is the objective of the Ministry of Energy, Water and Communications (MEWC) to protect the infrastructure.

As a public-private partnership, the Information Sharing Forum (ISF) strives to bring together various ICT stakeholders in order to jointly address Malaysian information and network security issues.

### Public Agencies

#### Malaysian Communications and Multimedia Commission (MCMC)

The MCMC[5] is a statutory body established in 1998 in accordance with the national policy objectives set out in the Communications and Multimedia

[4] http://www.cybersecurity.org.my/en/knowledge_bank/news/2005/main/detail/891/index.html.

[5] http://www.mcmc.gov.my.

Commission Act[6] and in the Communications and Multimedia Act (CMA).[7] The MCMC oversees the new regulatory framework for the converging industries of telecommunications, broadcast, and online activities. This includes the development and enforcement of access codes and standards. The MCMC ensures information security and the integrity and reliability of the network of Malaysia, identified as one of the ten national policy objectives in the CMA. Together with the police, the MCMC has enforcement powers for offences relating to network security in the CMA. In June 2002, MCMC hosted a workshop on Information and Network Security and the Protection of Critical Infrastructure.[8] In response to a proposal by the Malaysian prime minister in 2005, an initiative called IMPACT (an International Multilateral Partnership Against Cyber-Terrorism, set up by the Malaysian government) was recently launched. The first inaugurating IMPACT summit took place in Kuala Lumpur in May 2008 under the auspices of MCMC.

## Malaysian Administrative Modernization and Management Planning Unit (MAMPU)

Security issues in the public sector are administered by the Malaysian Administrative Modernization and Management Planning Unit (MAMPU).[9] Within MAMPU, the ICT Security Division also operates as Computer Emergency Response Team (GCERT) for the government.[10] In the field of e-Government, MAMPU developed the ICT Strategic Plan in 2003 to provide citizens and businesses with enhanced access to government information and services. The Public Sector ICT Strategic Plan outlines the guidelines for implementing the public sector's ICT

[6] This act created a new regulatory body, the MCMC. Cf. http://www.mcmc.gov.my/about_us/roles.asp.

[7] This act set out a new regulatory licensing framework for a convergent communications and multimedia industry. For example, it covers fraudulent use of network facilities or services and interceptions of communications. http://www.mcmc.gov.my/about_us/roles.asp. See the chapter on Law and Legislation.

[8] Rahman Malaysia's Approach to Network Security, op. cit. http://www.itu.int/osg/spu/ni/security/workshop/presentations/cni.19.pdf.

[9] http://www.mampu.gov.my.

[10] http://www.mampu.gov.my/perkhidmatan/gcert.

requirements, frameworks, and the core areas to be strengthened.[11] The MAMPU is also the host of the Government ICT Security Command Center, a project designed to monitor cyber-threats to the network system and to public ICT. The aims of this project include the provision of periodic scanning of vulnerabilities and assets, the detection of security breaches, and forecasting and warning of cyber-attacks.[12]

The current information security measures provided by MAMPU fall under three categories:

- Proactive measures: providing ICT security documents such as an ICT security policy framework for the public sector; ICT incident reporting mechanisms; and best practices;
- Recovery measures: ensuring the continuous function of critical business in the event of disruption; advice on how to upgrade patches; and warnings of virus attacks;
- Continuous measures: monitoring, enforcement, policy review and improving ICT security management.

## Police Cyber Crime Unit

The Royal Malaysia Police has established a Technology Crime Investigation Unit under the Commercial Crime Investigation Division of the Criminal Investigation Department. The investigation officers in this unit investigate and take preventive action against commercial crime involving computers and internet-related crimes. The police has also established a forensic computer laboratory to assist officers investigating computer crime.[13]

[11] http://www.mampu.gov.my/perkhidmatan/isp.

[12] http://www.mampu.gov.my/perkhidmatan/prisma.

[13] http://mpk.rmp.gov.my/english/Eng_indexMail.htm.

## Ministry of Science, Technology and Innovation (MOSTI)

Under a recent restructuring, the Ministry of Science, Technology and Innovation (MOSTI) took over responsibility from the former Ministry of Energy, Communication and Multimedia (MECM) for the following areas:

- Formulation and implementation of national policy on ICT;
- Formulation and implementation of national information security policy;
- Encouraging research and development and commercialization of ICT;
- Development and promotion of ICT industries.[14]

Following the restructuring, the secretariat of the National Information Technology Council (NITC) (see the chapters on Past and Present Initiative and on Early Warning and Public Outreach) was transferred to MOSTI. The ICT Policy Division within MOSTI was established on 1 March 2005 with five units, namely the Policy and Strategic Unit, the ICT Technology Studies Unit, the Assessment and Monitoring Unit, the ICT Acculturation Unit, and the NITC Secretariat.[15]

At an NITC meeting in April 2006, agreement was reached on a Malaysian National Cyber Security Policy (NCSP), and the National ICT Security and Emergency Response Center (NISER) was assigned to carry out the function of the national cyber-security agency. In March 2007, NISER was given additional mandates and renamed CyberSecurity Malaysia. And in August 2007, CyberSecurity Malaysia was officially launched by the prime minister. It has been operating autonomously since then under the heading of the MOSTI[16] (see the chapter on Early Warning and Public Outreach).

## Ministry of Energy, Water and Communications (MEWC)

The Ministry of Energy, Water and Communications (MEWC) was established in March 2004 and manages the nation's energy, communications (infrastructure),

[14] http://www.mosti.gov.my/opencms/opencms/MostePortal/NITC/NITCIntro.html.

[15] http://www.mosti.gov.my/opencms/opencms/MostePortal/NITC/NITCIntro.html.

[16] http://www.cybersecurity.org.my/en/about_us/history/main/detail/734/index.html.

and postal services, as well as water supply. MEWC develops and formulates strategic and innovative policies, a self-regulatory framework, and an effective management system. One of its objectives is to ensure a secure and reliable supply and provision of energy, water, and communications services.[17]

### Public-Private Partnership

#### Information Sharing Forum (ISF)

The Information Sharing Forum (ISF) was formed in June 2004 by the Malaysian Communications and Multimedia Commission (MCMC). It brings together various Internet Service Providers (ISP) and other agencies – namely, CyberSecurity Malasyia, the ICT Security Division of MAMPU, and the Malaysian Technical Standards Committee – to address Malaysian information and network security issues. Apart from encouraging cooperation between different network owners, operators, and other agencies, this forum enables the sharing of experience and expertise for the benefit of the Malaysian network infrastructure. Moreover, it aims at elaborating guidelines and best practices. The ISF meets every month and is chaired by the MCMC. It also hosts a newsgroup where members interact and debate on issues before each ISF meeting.[18]

## Early Warning and Public Outreach

### Malaysian Computer Emergency Response Team (MyCERT)

In March 1997, the Malaysian Computer Emergency Response Team (MyCERT) was launched.[19] Over the years, MyCERT has provided assistance to many

[17] http://www.ktak.gov.my/template01.asp?contentid=280.

[18] Tho Swee Hoe, Malaysian Communications and Multimedia Commission. "Information and Network Security Issues in the Communications and Multimedia Industry", HackInTheBox Conference, 2004. http://packetstormsecurity.org/hitb04/hitb04-toh-swee-hoe.pdf.

[19] http://www.mycert.org.my/about.html.

Malaysians in handling ICT security incidents. During this period, there was an increase in national awareness of ICT – in particular, of the fact that ICT security issues encompass a much broader scope than previously envisaged. Purely technical measures, such as firewalls, are not sufficient for tackling security threats. The government of Malaysia realized that the growing number and variety of ICT applications and devices produced by suppliers lacking fundamental security precautions had created a strong need for a trusted ICT security center to support not only reactive measures, but also proactive measures in ICT security. To this end, MyCERT provides a point of reference for the internet community to deal with computer security incidents and methods of prevention. It strives to reduce the probability of successful attack and lowering the risk of consequential damage. MyCERT has the following functions:

- Providing an expert point of reference on network and security matters;
- Reporting security incidents and facilitating communication to resolve security incidents;
- Disseminating security information, including system vulnerabilities and defense strategies;
- Acting as a repository of security-related information, acquiring patches, tools, and techniques;
- Educating the public with regard to computer security in Malaysia.[20]

## From the National ICT Security and Emergency Response Center (NISER) to Cyber Security Malaysia

The National ICT Security and Emergency Response Center (NISER)[21] was formed by the National Information and Communication Technology Council (NITC) to address e-Security issues and to act as Malaysia's CERT. NISER evolved from what was originally the Malaysian Computer Emergency Response Team (MyCERT) in March 1997. As mentioned earlier (see the chapter on Organization Overview, section on MOSTI), the transformation process of

[20] http://www.mycert.org.my.

[21] http://www.cybersecurity.org.my/en/about_us/history/main/detail/734/index.html.

NISER into CyberSecurity Malaysia, through the adoption of the Malaysian National Cyber Security Policy, started in 2006. It was given additional mandates and officially launched by the prime minister in 2007.[22] Thus, NISER's role was elevated as it became CyberSecurity Malaysia. Today, CyberSecurity Malaysia exists as the national reference and specialist center for cyber-security under the purview of MOSTI. CyberSecurity Malaysia was formed as a one-stop coordination center for all national cyber-security initiatives with the aim to

- Reduce the vulnerability of ICT systems and networks;
- Nurture a culture of cyber-security among users and critical sectors;
- Strengthen Malaysian self-reliance in terms of technology and human resources.

With the advent of CyberSecurity Malaysia, the country has been striving towards overcoming cyber-threats and to build a safer and more secure cyberspace. The services offered by CyberSecurity Malaysia include computer emergency response, digital forensics, security assurance, security management and best practices, and training and outreach.[23] Therefore, CyberSecurity Malaysia offers services to private and public entities such as research in vulnerability detection, intrusion detection, and computer forensic technology. It is also a member of the Forum of Incident Response and Security Teams (FIRST) (see the chapter on FIRST in this volume) and APCERT (the Asia Pacific Computer Emergency Response Team). Through collaboration with other agencies, it provides specialized ICT security services and continuously identifies possible gaps that could be detrimental to national security.[24] CyberSecurity Malaysia fosters mutual co-operation, information-sharing, and expert assistance among the different government agencies involved. The integrative purpose of CyberSecurity Malaysia is to reduce the vulnerability of ICT systems and networks, to nurture a culture

[22] http://www.cybersecurity.org.my/en/about_us/history/main/detail/734/index.html.

[23] http://www.cybersecurity.org.my/en/about_us/brief_detail/main/detail/729/index.html.

[24] http://www.cybersecurity.org.my/en/about_us/operational_mode/main/detail/735/index.html.

of cyber-security amongst users and critical sectors, and to strengthen Malaysian self-reliance in terms of technology and human resources.[25]

## Laws and Legislation

The Malaysian government has passed a number of laws relating to cyberspace since 1997 to provide a comprehensive legal framework that encompasses the security of information and network integrity and reliability, for the benefit of society at large as well as the business sector in particular.

### Computer Crimes Act 1997

Part II, Offences

3 (1) A person shall be guilty of an offence if

(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer;

(b) the access he intends to secure is unauthorised; and

(c) he knows at the time when he causes the computer to perform the function that that is the case.

(2) The intent a person has to have to commit an offence under this section need not be directed at –

(a) any particular program or data;

(b) a program or data of any particular kind; or

(c) a program or data held in any particular computer.

(3) A person guilty of an offence under this section shall on conviction be liable to a fine or to imprisonment not exceeding five years or to both.[26]

[25] http://www.cybersecurity.org.my/en/about_us/establishment/main/detail/733/index.html.

[26] http://www.cybercrimelaw.net/laws/countries/malaysia.html.

## Communications and Multimedia Act (CMA) 1998

An Act to provide for and to regulate the converging communications and multimedia industries, and for incidental matters.

Part 1 – Preliminary Section 3.

Objects (1)

The objects of this Act are (a) to promote national policy objectives for the communications and multimedia industry; (b) to establish a licensing and regulatory framework in support of national policy objectives for the communications and multimedia industry; (c) to establish the powers and functions for the Malaysian Communications and Multimedia Commission; and (d) to establish powers and procedures for the administration of this Act.

(2) The national policy objectives for the communications and multimedia industry are - (a) to establish Malaysia as a major global centre and hub for communications and multimedia information and content services; (b) to promote a civil society where information-based services will provide the basis of continuing enhancements to quality of work and life; (c) to grow and nurture local information resources and cultural representation that facilitate the national identity and global diversity; (d) to regulate for the long-term benefit of the end user; (e) to promote a high level of consumer confidence in service delivery from the industry; (f) to ensure an equitable provision of affordable services over ubiquitous national infrastructure; (g) to create a robust applications environment for end users; (h) to facilitate the efficient allocation of resources such as skilled labour, capital, knowledge and national assets; (i) to promote the development of capabilities and skills within Malaysia's convergence industries; and (j) to ensure information security and network reliability and integrity.

(3) Nothing in this Act shall be construed as permitting the censorship of the Internet.[27]

[27] http://www.mcmc.gov.my/mcmc/the_law/ViewAct.asp?cc=4446055&lg=e&arid=900722.

# The Netherlands

## Critical Sectors

Using the so-called Quick Scan method[1] and in consultation with the industry and government, it was determined in 2002 that the Netherlands' critical infrastructure comprises 11 sectors and 31 critical products and services.[2] That result was adjusted in the ensuing risk analysis phase. Since April 2004, the list comprises 12 critical sectors and 33 critical products and services. Infrastructures are deemed critical if they constitute an essential, indispensable service for society, and if their disruption would rapidly bring about a state of emergency or could have adverse societal effects in the longer term. In the Netherlands, critical sectors (and products and services) include the following:[3]

[*] This chapter was reviewed by Eric Luiijf, TNO Defense, Security and Safety; Williët Brouwer, Programme Manager Critical Infrastructure Protection, Ministry of the Interior; and André Griffioen, Deputy Programme Manager Critical Infrastructure Protection, Ministry of the Interior.

[1] For more information on "Quick Scan", see the chapter on Past and Present Initiatives.

[2] Ministry of the Interior and Kingdom Relations. "Critical Infrastructure Protection in the Netherlands", (April 2003). http://cipp.gmu.edu/archive/NetherlandsCIreport_0403.pdf.

[3] Ministry of the Interior and Kingdom Relations. "Report on the Netherlands", September 2005: Critical Infrastructure Protection, September 2005, p. 72.

- Drinking Water Supply,
- Energy (Electricity, Natural Gas, and Oil),
- Financial Sector (Financial Services and the Financial Infrastructure, both Public and Private),
- Food (Food Supply and Food Safety),
- Health (Urgent Health Care/Hospitals, Sera and Vaccines, Nuclear Medicine),
- Legal Order (Administration of Justice and Detention, Law Enforcement),
- Public Order and Safety (Maintaining Public Order, Maintaining Public Safety),
- Retaining and Managing Surface Water (Management of Water Quality, Retaining and Managing Water Quantity),
- Telecommunications (Fixed Telecommunication Network Services, Mobile Telecommunication Services, Radio Communication and Navigation, Satellite Communication, Broadcast Services, Internet Access, Postal and Courier Services),
- Public Administration (Diplomatic Communication, Information Provision by the Government, Armed Forces and Defense, Decision-making by Public Administration),
- Transport (Mainport Schiphol, Mainport Rotterdam, Main Highways and Waterways, Rail Transport),
- Chemical and Nuclear Industry (transport, storage, and production/processing).

The Critical Information Infrastructure (CII) of the Netherlands consists mainly of the internal supporting infrastructure of critical sectors like the energy, transport, and financial sectors, and is supported by a set of services delivered by the telecommunications and energy sectors (fixed telecommunication, mobile telecommunication, internet access, electricity).

# Past and Present Initiatives and Policies

In the Netherlands, CIP/CIIP is perceived increasingly as a crucial issue of national security. Since the end of the 1990s, several efforts have been made to manage CIP/CIIP better. The early initiatives and policies were aimed at information security in general, because there was no clear definition of critical infrastructures. This changed with the Critical Infrastructure Protection Project, which started in 2001 and formulated dedicated policies for CIP and CIIP.

## Early Efforts to Protect Information and Communication Infrastructure

### The Digital Delta

The publication The Digital Delta of June 1999 offered a framework for a range of specific measures regarding government policy on information and communications technology (ICT) for the next three to five years.[4] This memorandum noted the increasing importance of ensuring the security of information systems and the communications infrastructure, and of mastering the growing complexities of advanced IT applications.[5]

### Defense Whitepaper 2000

Likewise, the increasing importance of ICT is also explicitly mentioned in the Dutch Defense Whitepaper 2000: "Given the armed forces' high level of dependence on information and communication technology, it cannot be ruled out that in the future attempts will be made to target the armed forces in precisely this area."[6]

[4] http://www.gbde.org.

[5] Eric Luiijf and Marieke Klaver. "In Bits and Pieces: Vulnerability of the Netherlands ICT-Infrastructure and Consequences for the Information Society", (Amsterdam, March 2000); translation of the Dutch Infodrome essay 'BITBREUK', de kwetsbaarheid van de ICT-infrastructuur en de gevolgen voor de informatiemaatschappij, p. 5.

[6] Ministerie van Defensie. "Defensienota 2000", (1999), p. 59.

## Infodrome Initiative & BITBREUK

In March 2000, the key essay BITBREUK (English version In Bits and Pieces) was published by the government-sponsored think-tank Infodrome[7] to stimulate the discussion on the need to protect CII. The essay offered an initial vulnerability analysis and postulated a number of hypotheses for further discussion and examination by the Dutch authorities in co-operation with the appropriate national public and commercial organizations.[8] In mid-2001, this document was used as a starting point for a so-called 24-hour cabinet session. This was a 24-hour workshop with a selected group of experts that created a manifesto on CI/CII issues (KWINT-manifest) with a set of recommendations for all political parties. These recommendations provided the basis for the KWINT program to improve information security.

## KWINT Report and KWINT Program

The report entitled Kwetsbaarheid op Internet – Samen werken aan meer veiligheid en betrouwbaarheid (KWINT),[9] written by Stratix Consulting/TNO[10] for the Ministry of Transport, Public Works, and Water Management (V&W), was completed in 2001. The report concluded that the Dutch internet infrastructure was extremely vulnerable. Final recommendations were made on policy measures with regard to awareness and education, coordination of incidents, protection, and security. The report concluded that the measures should be realized within

[7] Infodrome was a think-tank founded in 1999 and sponsored by the Dutch government that served a threefold objective: (1) to develop an understanding of the social implications of the information revolution (this requires the gathering of empirical, quantitative knowledge and data on IT-related developments, and a systematic analysis thereof), (2) to stimulate social awareness of the importance of having a government policy that meets the requirements of the information society, and (3) to examine the priorities given by parties and interest groups to activities (public or private) undertaken in relation to the information society. This requires an understanding of the political and social value of knowledge, experience, and insights. The Infodrome project ended in 2002.

[8] Luiijf/Klaver, op. cit.

[9] Vulnerability of the Internet – Working Together for Greater Security and Reliability.

[10] TNO is the Netherlands' Organization for Applied Scientific Research.

a public-private partnership framework, while the government should play a facilitating and coordinating role.[11]

The findings and recommendations of this report triggered the formation of an interdepartmental working group of members of the Ministries of Economic Affairs, Defence, Finance, the Interior, Justice, and Transport (Telecom and Post Directorate).[12] As a result, the KWINT government memorandum Vulnerability of the Internet was endorsed by the cabinet on 6 July 2001. It includes a set of recommendations for action. The government-wide computer emergency response team, GOVCERT.NL, was established, and a malware-alerting service for Small and Medium Enterprises (SMEs) and the public was set up.[13] Other KWINT tasks were given to the Platform Electronic Commerce in the Netherlands (ECP.NL), the public-private platform for e-commerce in the Netherlands.

The KWINT Program 2002–2005 was especially targeted towards the protection and safe use of the internet. The 2005 report to the Dutch parliament recognizes the need to address the security of ICT that is used across critical sectors. The dependency and vulnerability of Supervisory, Control, and Data Acquisition (SCADA), for instance, is a cross-sector ICT area that will be analyzed in detail.

## Veilige Elektronische Communicatie (VEC)

The successor of the KWINT program is called Veilige Elektronische Communicatie (VEC).[14] The program started in January 2006 and will run for at least three years. The program is designed as a public-private partnership under the responsibility of the Ministry of Economic Affairs. It aims to raise

[11] Ronald De Bruin. "From Research to Practice: A Public-Private Partnership Approach in the Netherlands on Information Infrastructure Dependability". Dependability Development Support Initiative (DDSI) Workshop (28 February 2002).

[12] The Telecom and Post Directorate (DGTP) became part of the Ministry of Economic Affairs as of 1 January 2003.

[13] http://www.waarschuwingsdienst.nl.

[14] Safe Electronic Communications.

general awareness of information security and will implement a pilot project to support SMEs in the fight against cybercrime.[15]

## The Critical Infrastructure Protection Project

In early 2002, the Dutch government initiated the critical infrastructure protection project Protection of the Dutch Critical Infrastructure,[16] with the objective of developing an integrated set of measures to protect the infrastructure of government and industry, including ICT.[17] The project includes four steps: 1) A quick-scan analysis of the Dutch critical infrastructure to identify products and services vital to the nation, the (inter-) dependencies of these products and services, and underlying essential processes; 2) stimulation of a public-private partnership; 3) threat and vulnerability analysis; and 4) a gap analysis of protection measures.

To identify sectors, products, and services comprising the national critical infrastructure, a Quick-Scan Questionnaire was developed. Dutch government departments used this questionnaire in early 2002 to make an inventory of all products and services that they regarded as vital, including the underlying processes and dependencies. In June 2002, an analysis of the collected information was presented in a working conference with key representatives of both the public and the private sectors. The initial results were augmented and refined in 17 workshops with the vital public and private sectors. In parallel, damage experts

[15] http://www.minez.nl/dsc?c=getobject&s=obj&objectid=136886&!dsnameEZInternet&isapidir=/gvisapi/ (in Dutch). Cf. also: Marjolijn Durinck and Willem Boersma. "Public-Private Partnership in Awareness Raising: Internet Safety Awareness in the Netherlands". http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_public_awareness_raising_in_the_netherland_boersma_durincks.pdf.

[16] Bescherming Vitale Infrastuctuur.

[17] Ministry of the Interior and Kingdom Relations. "Critical Infrastructure Protection in the Netherlands", (April 2003). http://cipp.gmu.edu/archive/NetherlandsCIreport_0403.pdf.

evaluated the potential damage impact of loss or disruption of vital products and services.[18]

In April 2003, the findings of the Quick Scan, performed in close collaboration with the Netherlands Organization for Applied Scientific Research (TNO), were published by the Ministry of the Interior and Kingdom Relations.[19] The following main conclusions were drawn from the Quick Scan results:

- The Dutch government and industry now have a clear understanding of the critical products and services that comprise the Netherlands' critical infrastructure, and of their (inter-) dependencies;
- The direct and indirect vitality of critical products and services has been elaborated;
- It became clear that actors responsible for critical products and services only have a limited understanding of other critical products and services that depend on them, and of the extent of this dependence.[20]

The next steps concerning the strengthening of the Netherlands' CIP/CIIP included pinpointing the vital nodes for each of the critical services, risk and vulnerability analyses for each critical sector, scenarios to test the effectiveness of CIP/CIIP measures, and an international exchange of CIP/CIIP information and coordination.[21] In addition, the CIP project has been established as a regular policy file under the responsibility of the Ministry of the Interior

[18] To determine the elements of the national critical infrastructure, the Dutch approach aims to distinguish between products and services vital to the nation and those that are "merely" very important. Under this method, a product or a service is defined as vital if it "provides an essential contribution to society in maintaining a defined minimum quality level of (1) national and international law and order, (2) public safety, (3) economy, (4) public health, (5) ecological environment, or (6) if loss or disruption impacts citizens or the government administration at a national scale." By measuring criticality according to a predefined minimum level of acceptable quality in vital services to society, the approach shifts the problem of defining "vital" or just "very important" elements to the political level. It is the government that must determine the level of damage impact that is acceptable to society. Eric Luiijf, Helen H. Burger, and Marieke H.A. Klaver, "Critical Infrastructure Protection in the Netherlands: A Quick-scan". In: Urs E. Gattiker, Pia Pedersen, and Karsten Petersen (eds.): EICAR Conference Best Paper Proceedings 2003.

[19] Ibid., p. 7.

[20] Ibid., p. 23.

[21] Ibid., p. 25.

and Kingdom Relations. In 2005, the ministry outlined the Report on Critical Infrastructure Protection for the attention of the Dutch parliament. The report contained a review of the achievements of the CIP Project and defined a new set of actions.[22]

- Intensifying critical infrastructure security policy: CIP is a collective task, and it is important that all relevant stakeholders pull together to improve the security of national infrastructures. Therefore, a Strategic Board for CIP (Strategisch Overleg Vitale Infrastructuur, SOVI) was created (for more information, see the chapter on Organizational Overview);
- Analyzing CIP dependency: fostering cross-critical sector communication is also the goal of the CIP Dependency project. Critical sectors must be able to get in touch with each other – not only to determine the extent of the crisis, but also to assess its likely duration. The project is underway and will determine whether the affected critical sectors will have to take additional measures in order to guarantee continuity;
- Improving protection of critical infrastructures against human threats: protection against willful disruptions of vital services is a high priority. Such attacks may be conducted by hackers, activists, frustrated employees, ordinary criminals (who are motivated by financial gains), and terrorists. In order to prevent such attacks, cooperation between law enforcement units, the intelligence services, CERTs, and private parties is indispensable. The National Advisory Centre Critical Infrastructures (NAVI)[23] provides a platform for mutual exchange among these organizations;
- Awareness-raising: Scenario exercises will be implemented involving distribution plans for CI products/services in the event of scarcity of supply, both at the national and regional levels.

Progress reports on these activities were published in 2006 and 2007.[24]

[22] House of Parliament (Tweede Kamer) 2005–2006, 26643 No. 75, 16 September 2005, and annex "Rapport ter Bescherming Vitale Infrastructuur", dated 1 September 2005.

[23] http://209.85.135.104/search?q=cache:ghBixn6L-noJ:www.fbiic.gov/reports/neth_2.pdf+%22govcert%22+%22aivd%22&hl=de&ct=clnk&cd=7&gl=ch.

[24] Kamerstuk 2006–2007, 26643, nr. 83, Tweede Kamer and Kamerstuk 2007–2008, 29668, nr. 18, Tweede Kamer.

## National Security Strategy and Work Programme 2007-2008

In order to cope with emerging risks, the Dutch cabinet has drawn up a National Security Strategy and Work Programme for the years 2007–2008.[25] The strategy defines the goals of Dutch security policy, analyzes and assesses threats and risks, and develops methods for strategic planning. The strategy pursues an all-hazard approach and aims to provide for a more coordinated and integrated approach to national security.[26]

Accordingly, the strategy will serve as a framework for the future protection policies for critical infrastructures.[27] The document states that there are many potential threats to the country and that each of these threats puts a strain on national security. National security is conceived as being under threat when vital interests of the Dutch state and society are harmed to the extent that society can become destabilized. These vital interests, and examples thereof, include the following:[28]

- Territorial security: the threat or occurrence of (terrorist) attacks on Dutch soil;
- Economic security: the breakdown of overseas trade or an ICT malfunction;
- Ecological safety: an environmental disaster or disruption of the drinking water supply;
- Physical safety: a dyke breach or epidemic;
- Social and political stability: tension between various ethnic groups.

[25] "National Security Strategy and Work Programme 2007–2008". http://www.minbzk.nl/aspx/download.aspx?file=/contents/pages/88474/natveiligh.bwdef.pdf.

[26] Dick Schoof. "National Security Strategy – The Netherlands", Presentation, 25 September 2007.
http://www.hightechconnections.org/files/HTC_homeland_security_Dick_Schoof.pdf.

[27] "National Security Strategy and Work Programme 2007–2008" op. cit., p. 18.

[28] http://www.minbzk.nl/bzk2006uk/subjects/public-safety/national-security.

In the Netherlands, national security encompasses both breaches of security by intentional human actions (security) and breaches due to disasters, system or process faults, human failure, or natural anomalies such as extreme weather (safety).

The new approach aims at allowing signals of potential threats to be identified at an earlier stage, by systematically linking information streams and cross-referencing developments (e.g., to what extent will energy requirements change if summers become warmer and more air conditioning and refrigerators are needed). The strategy formulates a method of weighing various interests and strives to prioritize among them.[29] Clearly, critical infrastructure protection is intimately linked with the National Security Strategy and planning. One of the capabilities named to be strengthened according to the national risk assessment (part of this programme) is business continuity.[30]

In 2008 one of the issues addressed within the National Security Strategy is ICT failure. A project called "ICT-verstoring" was initiated in which relevant private and public parties co-operate in a government-wide analysis and risk assessment of ICT. In this project, short, medium, and long-term ICT threats to the Netherlands are identified and analyzed in terms of their likelihood and potential impact. The insights gained from this process are used to assess whether preventative capabilities and preparation are sufficient to cope with these threats.

## Organizational Overview

Responsibility for the Dutch CI and CII lies with various actors and involves public and private sectors as well as several ministries, including the Ministry of the Interior and Kingdom Relations, the Ministry of Economic Affairs, the Ministry of Transport, Public Works, and Water Management, the Ministry of Housing, Spatial Planning, and the Environment, and the Ministry of Health,

[29] http://www.minbzk.nl/bzk2006uk/subjects/public-safety/national-security.

[30] http://www.minbzk.nl/onderwerpen/veiligheid/veilige-samenleving/nationale-veiligheid/publicaties/112985/item-112985.

Welfare and Sport. The General Intelligence and Security Service is also involved in protecting information security in the Netherlands.

Moreover, public-private partnerships play a crucial role in CIP and CIIP in the Netherlands. As mentioned above, the KWINT program and the Critical Infrastructure Protection Project are both based on public-private collaboration. The KWINT program led to a flurry of policy recommendations that are elaborated in further detail in the public-private partnership Platform Electronic Commerce in the Netherlands (ECP.NL). These recommendations refer to awareness-raising, research and development, alarm and incident response, and the integrity of information.

Public-private co-operation within the project Critical Infrastructure Protection Project gained further importance with the official establishment of the Strategic Board for CIP (SOVI). With regard to the protection of critical information infrastructures, the National Continuity Consultation Platform Telecommunication (NCO-T) is of special interest, because it enables public-private collaboration between the government and telecommunication companies on continuity planning and crisis response. Furthermore, the National Advisory Centre Critical Infrastructures is an initiative of the government striving to enhance information exchange on security issues between critical sectors, critical sector enterprises, and government agencies. Finally, the National Infrastructure against Cyber-Crime is a cyber-crime information-sharing model organized as a private-public partnership program.

## Public Agencies

### Ministry of the Interior and Kingdom Relations (BZK)

First of all, the Ministry of the Interior and Kingdom Relations (MoI) is responsible for the general C(I)IP policy, the co-ordination of the national activities across all sectors and responsible ministries, and international policy (e.g., EPCIP) and co-ordination. Additionally, the MoI is responsible for the protection of government information infrastructures (government CIIP), national emergency management, and the CIP aspects of emergency response services. The national emergency management includes the National Crisis Centre (NCC), which is in charge of co-ordination activities at the policy level in case of emergencies and disasters with a nation-wide impact.

### Ministry of Economic Affairs (EZ)

Some other key C(I)IP areas are the responsibility of the Ministry of Economic Affairs (EZ). EZ is responsible for C(I)IP coordination with the private sector in the areas of energy and telecommunications, including the internet.[31] Other parts of the same ministry are responsible for CIP/CIIP policies regarding the private industry, including SMEs.

### Ministry of Transport, Public Works, and Water Management (V&W)

The Ministry of Transport, Public Works, and Water Management (V&W)[32] is responsible for the public-private C(I)IP co-ordination for the critical infrastructures related to transport (road, rail, air, harbors, and inland shipping) and water management as well as the biochemical quality of the surface water.

### Ministry of Housing, Spatial Planning, and the Environment (VROM)

The Ministry of Housing, Spatial Planning, and the Environment (VROM)[33] is responsible for public-private co-ordination of the C(I)IP activities of the chemical and nuclear industries, as well as the potable water infrastructure.

[31] http://www.minez.nl/content.jsp?objectid=140727.

[32] http://www.verkeerenwaterstaat.nl/english.

[33] http://international.vrom.nl/pagina.html?id=5450.

### Ministry of Health, Welfare and Sport (VWS)

The Ministry of Health, Welfare, and Sport (VWS)[34] is responsible for the public-private coordination of the C(I)IP activities of the health sector.

### General Intelligence and Security Service (AIVD)

The General Intelligence and Security Service (AIVD)[35] is a division of the Ministry of the Interior and Kingdom Relations and is tasked with protecting the information security and vital sectors of Dutch society.[36] The AIVDs focus shifts in accordance with social and political changes. One of its tasks is to uncover forms of improper competition, such as economic espionage, that could harm Dutch economic interests. Another task is foreign intelligence. In the interests of national security, it will carry out investigations abroad, though only in the non-military sphere. The AIVD is responsible for analyzing potential and likely threats to the Dutch CI sectors.

## Public-Private Partnerships

### Platform Electronic Commerce in the Netherlands (ECP.NL)

The Platform Electronic Commerce in the Netherlands (ECP.NL)[37] has been tasked by the Ministry of Economic Affairs with setting up a public-private partnership program to implement the action guidelines of the KWINT Memorandum.

The objective of the KWINT program focused on the following aspects: continuity of the internet infrastructure in the Netherlands, viruses, denial-of-service attacks, hacking, transparency of internet services, integrity and confidentiality of information, and misuse by personnel. As the KWINT program expired in

[34] http://www.minvws.nl/en.

[35] Algemene Inlichtingen- en Veiligheidsdienst. https://www.aivd.nl/.

[36] http://www.fas.org/irp/world/netherlands/bvd.htm.

[37] http://www.ecp.nl.

2005, ECP.NL established the Digibewust program (Digital Awareness)[38] in order to improve awareness of information security.

## National Continuity Plan for Telecommunications (NACOTEL) and National Continuity Forum Telecommunications (NCO-T)

The National Continuity Plan for Telecommunications (NACOTEL) was established in 2001 in order to structure the contingency policy and crisis management in the telecommunications sector. The public-private partnership included BT (IT-services), Enertel, KPN Telecom, Telfort, Orange, T-Mobile, and Vodafone – as well as the Ministry of Economic Affairs. NACOTEL was based on voluntary cooperation. The participants discussed possibilities to strengthen the security of the telecommunication sector. The building of trust was a central goal of the process. However, it became apparent that effective crisis management could not be achieved solely on a voluntary basis of cooperation. During crisis situations, it is possible that individual operators need to implement actions that run contrary to their interests. This analysis led to the decision to make participation in the public-private partnership mandatory for all operators of critical telecommunication services.[39] Therefore, NACOTEL was dissolved in February 2006 and replaced by the National Continuity Consultation Platform Telecommunications (NCO-T).[40]

## Strategic Board for CIP (SOVI)

The Strategic Board for CIP (Strategisch Overleg Vitale Infrastructuur, SOVI) was established in September 2006 as a dedicated public-private partnership for critical infrastructure protection. All critical sectors are represented in the strategic board, which meets two or three times a year. In 2007, the SOVI initiated a study on the electric power dependency of the various critical sectors and their resilience

[38] http://www.digibewust.nl.

[39] http://www.minez.nl/dsc?c=getobject&s=obj&objectid=150713&!dsname=EZInternet&isapidir=/gvisapi/.

[40] http://www.ez.nl/content.jsp?objectid=150712&rid=150996.

and ability to cope with longer duration power outages. It investigated issues such as secondary dependencies (e.g., dependency of various sectors on diesel oil for back-up generators) and the way in which these are prioritized amongst the critical sectors. It also studied the question of which related arrangements already exist or have yet to be made.

## Nationaal Adviescentrum Vitale Infrastructuur (NAVI)

The Dutch Nationaal Adviescentrum Vitale Infrastructuur (National Advisory Centre Critical Infrastructures, NAVI)[41] was initiated by the Dutch government as part of the CIP action plan discussed above.[42] In 2006, the Dutch parliament agreed to its business plan for 2006–2009.[43] NAVI has knowledge and expertise about the security of critical infrastructures and aims to exchange these with the critical sectors, critical sector enterprises, and government agencies. It builds upon its links within the government and critical sectors, such as current information provided by the AIVD and the Dutch National Coordinator for Counterterrorism (NCTb).[44]

NAVI offers various services to its constituency such as support for risk analysis as well as security advice. NAVI's modus operandi is derived from the (physical security aspect) of the UK's Centre for the Protection of National Infrastructure (CPNI). It has established sector-specific information exchanges between critical sectors and government functions. NAVI offers various services such as a front office and advisory function for critical infrastructure enterprises, good practices, and an international contact desk (information and good practices exchange with other nations and the EU). NAVI offers products such as risk analyses and risk methodologies, critical sector-specific threat scenarios, security methodologies, and advice.[45]

[41] http://www.navi-online.nl.

[42] House of Parliament (Tweede Kamer) 2005–2006, 26643 No. 75, 16 September 2005, and annex "Rapport ter Bescherming Vitale Infrastructuur", 1 September 2005.

[43] House of Parliament (Tweede Kamer) 2006–2007, 26 643, No. 85.

[44] http://www.nctb.nl.

[45] Information provided by an expert.

## Nationale Infrastructuur ter bestrijding van CyberCrime (NICC)

The National Infrastructure against Cybercrime (NICC) was established in 2006 as a three year program.[46] The NICC infrastructure consists of several components: a contact point, a reporting unit, trend-watching, monitoring and detection, information distribution, education, warning, development, knowledge sharing, surveillance, prevention, termination, and mitigation. The NICC further strengthens this infrastructure by hosting the Cybercrime Information Exchange, where public and private organizations share sensitive information, and by developing and supporting practical projects and trials that both solve concrete problems and generate knowledge about cybercrime.

The Cybercrime Information Exchange information-sharing model is based on the one designed by the UK's Centre for the Protection of National Infrastructure (CPNI). The NICC Information Exchange function can be pictured as following a 'flower' model. The heart of the flower is made up of government bodies, like the police, intelligence services, GOVCERT.NL, and the NICC itself. Critical infrastructure sectors and some other major industrial communities that heavily rely upon ICT can be thought of as being the petals of the flower. The different sectors chair their own petal, decide which parts of the meeting can be attended by the government bodies, and decide which information is sharable outside their sector 'petal'. The confidentiality of their exchanged information is maintained by an agreed set of rules on dissemination that follow the Traffic Light Protocol.

Many of the recognized information infrastructure sectors take part in a 'petal': The financial sector; providers of drinking water, energy, and telecommunication; Schiphol Airport; Rotterdam harbor; large enterprises / multi-nationals; and the rail sector.

One of the 2007 activities was the analysis of the information security posture of the SCADA and other process control systems in the Dutch drinking

[46] http://www.samentegencybercrime.nl/UserFiles/File/Leaflet_NICC.pdf.

water sector. As a result, a SCADA security good practices document has been developed.[47]

It is expected that the NICC will receive new instructions in a successor program from mid-2009. The information exchanges will either continue under another public-private partnership entity or be merged with the NAVI activities that are oriented more towards physical security.[48]

## Early Warning and Public Outreach

### SURFCERT (part of SURFnet)

SURFCERT, formerly known as CERT-NL, is the Computer Emergency Response Team of SURFnet, the internet provider for institutes of higher education and for many research organizations in the Netherlands. SURFCERT handles all computer security incidents involving SURFnet customers, either as victims or as suspects. SURFCERT also disseminates security-related information to SURFnet customers on a structural basis (e.g., by distributing security advisories) as well as on an incidental basis (distributing information during disasters).[49]

### GOVCERT.NL

A computer emergency response team for government departments (CERT-RO) was established in June 2002. In February 2003, it was renamed GOVCERT.NL.[50] It is operated under the responsibility of the Ministry of the Interior and Kingdom Relations (MoI). The GOVCERT.NL team is co-located and cooperates with Waarschuwingsdienst.nl (Alert Service),[51] a website and initiative

[47] Eric Luiijf. "SCADA Security Good Practices for the Dutch Drinking Water Sector", report TNO DV 2008 C096, (March 2008).

[48] Information provided by the country expert.

[49] http://cert-nl.surfnet.nl/home-eng.html.

[50] http://www.govcert.nl/render.html?it=41.

[51] http://www.waarschuwingsdienst.nl/render.html?cid=106.

provided by the Ministry of Economic Affairs/Directorate-General for Energy and Telecom (EZ/DGET). The Waarschuwingsdienst is responsible for issuing alerts and advice memoranda to the public and SMEs about viruses, Trojan codes, and other malicious software. Warnings are disseminated to the public via e-mail, web services, and SMS. The Waarschuwingsdienst was founded in early 2003 and is funded by the Ministry of Economic Affairs.

## Law and Legislation

### Penal Code

The Penal Code prohibits attacks against (non-ICT) CI (e.g., sabotage and interference with water management systems, electricity, the railway network, etc.).

### Computer Crime Laws

The second version of the Dutch computer crime law has been under development since 1999. It was delayed because of the need to adapt it to the European Cybercrime Convention, and several anti-terror measures have been included in this new national law. The Computer Crime Law II was introduced in September 2006, with some articles taking effect from September 2007 onwards.[52]

### Telecommunications Law

This law states the requirements that must be met by public telecommunication operators regarding the capacity, quality, and other properties of the services offered (e.g., free access to the 112 emergency number), as well as regulations with respect to safety and privacy precautions regarding their network and services.

[52] Official publication: Staatsblad 2006, 300 and 301, 13 July 2006.

## Criminal Code, Articles 138a and 138b

In summary, Article 138a states that any person who intentionally and unlawfully accesses an automated system for the storage or processing of data, or part of such a system, is guilty of a breach of computer peace and shall be liable to a term of imprisonment not exceeding six months or a related fine[53] if they breach security by technical intervention with the help of false signals or a false key, or by acting in a false capacity.[54]

An unauthorized person penetrating an automated system who copies the contained, processed, or transferred information for their own use or use by a third party may be punished with a maximum of four years imprisonment. The same holds for someone using public telecommunications means for accessing an automated system with the purpose of own gain or gain of a third party or for unauthorized access to an automated system of a third party.

In summary, Article 138b states that whoever deliberately and without authorization disrupts an automated system by sending information to that system shall be punishable with no more than one year's imprisonment.

The penal aspects of disrupting various critical infrastructure services have been described in specific articles of penal law for electric power, railway systems, and water management, and are covered by a cybercrime law article that raises the penalties when the safety or even the lives of people are threatened, or when people are actually injured or die.

[53] http://www.cybercrimelaw.net/laws/countries/netherlands.html.

[54] Information provided by the country expert.

# New Zealand

## Critical Sectors

Critical information infrastructure protection (CIIP) in New Zealand is about the protection of infrastructure necessary to provide critical services. "Critical services are those whose interruption would have a serious adverse effect on New Zealand as a whole or on a large proportion of the population, and which would require immediate reinstatement."[1] New Zealand's critical sectors comprise the assets and systems required for the maintenance of:[2]

- Emergency Services,
- Energy (including Electricity Generation and Distribution, and the Distribution of Oil and Gas),

[*] The Country Survey of New Zealand 2006 was reviewed by Richard Byfield and Mike Harmon, Centre for Critical Infrastructure Protection (CCIP). For this edition, the authors have thoroughly updated the New Zealand country survey by referring to open-source material.

[1] E-Government Unit, State Services Commission. "E-Government: Protecting New Zealand's Infrastructure from Cyber Threats", (December 2000). http://www.ccip.govt.nz/about-ccip/background/niip-report-final.pdf.

[2] Ibid.

- Finance and Banking,
- Governance (including Law and Order and National and Economic Security),
- Telecommunications and the Internet,
- Transport (including Air, Land, and Sea).

The various critical sectors depend on each other. Most systems assume the continuity of power and telecommunications infrastructures and make extensive use of networked information technology in their management and control systems.

## Past and Present Initiatives and Policies

The New Zealand government's Defence Policy Framework is a crucial document illustrating that CIIP is a key objective of the country's overall security policy. The Centre for Critical Infrastructure Protection (CCIP)[3] addresses the cyber-threat aspects of that objective.

### CIIP within the Defence Policy Framework

New Zealand's government promotes a comprehensive approach to security and aims to protect and maintain the country's physical, economic, social, and cultural security. In the government's Defence Policy Framework of June 2000, critical infrastructure protection is identified as one of the key objectives: "[…] to defend New Zealand and to protect its people, land, territorial waters, Exclusive Economic Zone, natural resources and critical infrastructure."[4]

[3] http://www.ccip.govt.nz.

[4] "New Zealand Defence Policy", (June 2000). http://www.defence.govt.nz/defence-policy.html and "Protecting New Zealand's Borders – The Government's Approach", (30 August 2007). http://www.beehive.govt.nz/speech/protecting+new+zealand%E2%80%99s+borders+%E2%80%93+government%E2%80%99s+approach.

## Report on Protecting New Zealand's Infrastructure from Cyber-Threats

New Zealand's State Services Commission's e-Government Unit released the report Protecting New Zealand's Infrastructure from Cyber-Threats[5] on 8 December 2000. The report deals with the protection of New Zealand's critical infrastructure from cyber-crime and other IT-based threats. The report assessed levels of risk due to IT-based threats in finance and banking, transport, electric power, telecommunications and the internet, oil and gas, water, and critical state services that support national safety, security, and income.[6] The report made several recommendations such as:[7]

- The establishment of a New-Zealand-based security-monitoring and incident-handling organization;
- Harmonization of computer-crime legislation with that of other nations (e.g., Australia, the US, Britain, and Canada);
- Adoption of specific IT security standards;
- Establishment of an ongoing cooperation program between owners of critical infrastructure and the government.

## Report Towards a Centre for Critical Infrastructure Protection (CCIP)

The Centre for Critical Infrastructure Protection was established in February 2001. The process of the center's development is traceable within the documents addressed below.[8] On 11 June 2001, the report Towards a Centre for Critical Infrastructure Protection (CCIP) was issued by the e-Government Unit.[9]

[5] "E-Government: Protecting New Zealand's Infrastructure From Cyber Threats", op. cit.

[6] Minister of State Services. Media Release on Cyber-Crime. "Government addressing Cyber-Crime and IT-Based Threats", (11 February 2001). http://www.ccip.govt.nz/about-ccip/background/mediarelease-cybercrime.pdf.

[7] "E-Government: Protecting New Zealand's Infrastructure from Cyber Threats", op. cit.

[8] http://www.ccip.govt.nz/about-ccip/background.html.

[9] "Towards a Centre for Critical Infrastructure Protection", (11 June 2001). http://www.ccip.govt.nz/about-ccip/background/ccip-final-report.pdf.

Following the previous National Information Infrastructure Protection (NIIP) report of December 2000, it recommended that the government establish a centre for critical infrastructure protection. The argument was that the dependence of citizens and businesses on various infrastructure services, the vulnerability of IT systems, and the risks and possible damage caused in case of failure were increasing. Therefore, measures had to be taken to ensure that infrastructure operators and government agencies were kept up to date on vulnerability and threat information: "The CCIP is proposed as an insurance measure in that it mitigates, for a low cost, a risk of a large loss."[10]

## Manual on Security in the Government Sector

The Interdepartmental Committee on Security issued a comprehensive and detailed manual in 2002 called Security in the Government Sector[11], which took into account the Australian/New Zealand Standard AS/NZS ISO/IEC 17799:2001 Information Technology – Code of Practice for Information Security Management, which deals with possible sources of threats to information and ways to counter them. The manual's security guidelines are mandatory for government departments, ministerial offices, the New Zealand Police, the New Zealand Defence Force, the New Zealand Security Intelligence Service, and the Government Communications Security Bureau (GCSB). In the manual, the government requires that information important to its functions, its official resources, and its classified equipment be adequately safeguarded to protect the public and national interests and to preserve personal privacy.

Furthermore, the manual proposes that overall responsibility for security should rest with a manager, the designated Departmental Security Officer (DSO). That person's duties should include formulating and implementing the general security policy and common minimum standards within the organization, issuing instructions on security, and serving as liaison with the secretary of the

[10] Ibid., p. 5. For more information about the CCIP, see the chapter on Organizational Overview.

[11] Department of the Prime Minister and Cabinet. "Security in the Government Sector", (2002). http://www.security.govt.nz/sigs/index.html.

Interdepartmental Committee on Security (ICS), the New Zealand Security Intelligence Service (NZSIS), and the GCSB for any special advice.[12]

### Security Policy and Guidance Website

The security policy and guidance website[13] provides information on the government's activities in the area of information security. This website acts as a focal point for the publication of government information about security standards, procedures, and resources.

### Standards New Zealand (SNZ)

Standards New Zealand (SNZ)[14] promotes several standards specific to New Zealand, as well as a host of joint Australian/New Zealand and international standards. AS/NZS ISO/IEC 17799 Information Security Management provides an overview of factors to be considered and included in the protection of information and information systems.

## Organizational Overview

Among the public agencies concerned and involved with CIIP in New Zealand are the Domestic and External Security Group (DESG), the Officials Committee for Domestic and External Security Co-ordination (ODESC), the Interdepartmental Committee on Security (ICS), the Centre for Critical Infrastructure Protection (CCIP), the Government Communications Security Bureau (GCSB), and the e-Government Programme.

As public-private partnerships, the New Zealand Security Association (NZSA) tries to engage representatives of both sectors in a dialog, as does the Computer Society Special Interest Group on Security (NZCS SigSec).

[12] Ibid., chapter 2.

[13] http://www.security.govt.nz.

[14] http://www.standards.co.nz/default.htm.

## Public Agencies

### The Domestic and External Security Group (DESG)

The main actor in charge of formulating New Zealand's security policy, including CIIP, is the Domestic and External Security Group (DESG), which co-ordinates central government activities aimed at protecting New Zealand's internal and external security, including intelligence, counter-terrorism preparedness, emergency and crisis management, and defense operations. The DESG director provides timely advice to the prime minister on issues affecting the security of New Zealand, including policy, legislative, operational, and budgetary aspects. DESG is the support secretariat for the Officials Committee for Domestic and External Security Co-ordination.[15]

### Officials Committee for Domestic and External Security Co-ordination (ODESC)

The Officials Committee for Domestic and External Security Co-ordination (ODESC) is chaired by the prime minister and makes high-level policy decisions on security and intelligence matters, including policy oversight in the areas of intelligence and security, terrorism, maritime security, and emergency preparedness. ODESC comprises chief executives from the Ministry of Foreign Affairs and Trade, the Ministry of Defence and the Defence Force, the New Zealand Security Intelligence Service, the Government Communications Security Bureau, the police, the Ministry of Civil Defence and Emergency Management, the Treasury, and others when necessary.[16]

### Interdepartmental Committee on Security (ICS)

The Interdepartmental Committee on Security (ICS)[17] is a sub-committee of the Officials Committee for Domestic and External Security Co-ordination

[15] http://www.dpmc.govt.nz/dess/index.htm.
[16] Ibid.
[17] http://www.security.govt.nz.

(ODESC). It formulates and coordinates the application of all aspects of security policy and sets common minimum standards of security and protection that all government organizations must follow. In addition, the ICS provides detailed advice on information security matters to government and other organizations or bodies that receive or hold classified information.[18]

## Centre for Critical Infrastructure Protection (CCIP)

The Centre for Critical Infrastructure Protection (CCIP)[19] was established in 2001 to provide advice and support to public and private owners of CI, in order to protect New Zealand's critical infrastructure from cyber-threats.

In the early stages of CCIP planning, the location of the new center was constrained by the need to give private-sector companies the confidence that their sensitive commercial and security information would be adequately safeguarded, as well as by the need to provide a secure environment to provide adequate protection for intelligence information that the CCIP had to be able to access. It was stated that "Overseas experience shows that the center should not be part of a law-enforcement agency, since this might reasonably focus on the pursuit of offenders, to the detriment of rectifying damage and of confidentiality."[20]

The Government Communications Security Bureau was finally given the responsibility for this effort, based on cost-effectiveness as well as its significant IT security skills and its culture of security.[21] Furthermore, the e-Government Unit acknowledged that the CCIP requires timely access to classified intelligence, among other sources, in order to provide the best chance of a successful threat warning.[22]

Hence, the CCIP is located within the Government Communications Security Bureau and has three main tasks:[23]

[18] "Security in the Government Sector", op. cit.

[19] http://www.ccip.govt.nz.

[20] Centre for Critical Infrastructure Protection. "Cabinet Paper", (13 August 2001), pp. 5, 9–11. http://www.ccip.govt.nz/about-ccip/background/mediarelease-cybercrime.pdf.

[21] Ibid. See also: "Towards a Centre for Critical Infrastructure Protection", op. cit, p. 2.

[22] "Towards a Centre for Critical Infrastructure Protection", op. cit., p. 9.

[23] http://www.ccip.govt.nz/about-ccip.html.

- To provide a round-the-clock watch and warning advice to owners and operators of critical infrastructure and to the government;
- To investigate and analyze cyber-attacks against critical national infrastructure; and
- To work with national and international critical infrastructure agencies to improve awareness and understanding of cyber-security in New Zealand.

Whereas the CCIP provides coordination, support, and advice on the ways in which information security can be maintained and improved, owners of critical infrastructures in the public and private sectors remain responsible for the security of their own systems.[24]

### Government Communications Security Bureau (GCSB)

In 1977, the Combined Signals Organization was replaced by the current signals intelligence agency, the GCSB, which is a civilian organization. Its chief executive reports directly to the prime minister. The GCSB gives advice and assistance to New Zealand government departments and agencies concerning the security of information-processing systems.[25]

One of the GCSB's tasks is to ensure the integrity, availability, and confidentiality of official information through the provision of Information Assurance (IA) services to departments and agencies of the New Zealand government, and to contribute to the protection of the critical infrastructure from IT threats.[26] The New Zealand Security of Information Technology (NZSIT) publications are therefore produced as guidelines for New Zealand government organizations in support of securing and protecting IT systems and associated information and services.[27]

[24] Cabinet Paper: Centre for Critical Infrastructure Protection, (13 August 2001). http://www.ccip.govt.nz/about-ccip/background/cabinetpaper-ccip.pdf.

[25] Domestic and External Security Group. "Securing our Nation's Safety: How New Zealand manages its security and intelligence agencies", (December 2000). http://www.dpmc.govt.nz/dpmc/publications/securingoursafety/index.html.

[26] http://www.gcsb.govt.nz/functions/index.html.

[27] http://www.gcsb.govt.nz/publications/nzsit/index.html.

## e-Government Programme

The e-Government Unit[28] was established in July 2000 within the State Services Commission (a department of the New Zealand Public Service). The responsibilities of the e-Government Unit, as defined by the cabinet, included, first, the development of an overarching e-government strategy; second, to facilitate the uptake of the e-government vision by government agencies; third, to coordinate collaboration in identifying opportunities across government agencies; fourth, the unit is responsible for providing policy advice to the minister of State Services in relation to e-government; and finally, it is in charge of monitoring progress toward achieving the e-government vision.[29] In April 2001, the work of the new unit resulted in the publication by the government of New Zealand's first e-government strategy. The strategy was updated in December 2001, in June 2003, and most recently, in November 2006. The latest version, called Enabling Transformation, reflects changes in the IT environment. The strategy paper covers the following areas:[30]

- It clarifies what the goal of transformation means for service delivery and collaboration;
- It matches the measurement of success to the indicators for the development goals for state services;
- It confirms the key role of collaboration, standards, and interoperability;
- It provides an updated high-level outline of the work undertaken across the government;
- It establishes a new goal for the way in which the government uses technology by 2020.

[28] http://www.e.govt.nz.

[29] http://www.e.govt.nz/resources/research/public-sector-2004/public-sector-27-04.pdf.

[30] http://www.e.govt.nz/about-egovt/strategy.

## Public-Private Partnerships

### New Zealand Security Association (NZSA)

The New Zealand Security Association (NZSA)[31] was formed in 1972. It represents licensed and certificated persons providing services to government departments, state-owned enterprises, businesses, and private users. The NZSA has two member groups: Corporate members, who are individuals or companies engaged in the security industry, and associate members, who are individuals or companies involved or interested in security, although security is not at the core of their business operations. Members of the latter category include government departments, insurance companies, airlines, banks, food distributors, area health boards, oil companies, etc.[32] Among the NZSA's main objectives are:[33]

- To set minimum operating standards for members, and to develop and approve codes of practice;
- To co-operate with the police, government departments, and other organizations and agencies concerned with the safekeeping of people, property, and information in New Zealand;
- To provide information and advisory services, education, and training.

### Computer Society Special Interest Group on Security (NZCS SigSec)

The New Zealand Computer Society's Special Interest Group on Security (NZCS SigSec)[34] is a forum for networking with others with an interest in IT security from within and outside government. The group meets quarterly for a presentation and networking.[35]

[31] http://www.security.org.nz.

[32] http://www.security.org.nz/Accredited_Members.php.

[33] http://www.security.org.nz/education.php.

[34] http://www.nzcs.org.nz/SITE_Default/special_interest_groups/SITE_Information_Systems_SIG/default.asp.

[35] http://www.kaonsecurity.co.nz/TFCC_demo/Sigs_manual/chapter2.html.

## Early Warning and Public Outreach

### AusCERT

AusCERT[36] is the national Computer Emergency Response Team for Australia. It also provides significant support to New Zealand organizations. It is one of the leading CERTs in the Asia/Pacific region; it provides prevention, response, and mitigation strategies for members.[37]

AusCERT was founded as a commercial CERT for Australia before the New Zealand Centre for Critical Infrastructure Protection (CCIP) was formed. The CCIP has a working relationship with AusCERT, but also provides an early-warning service and a moderated mailing list through its website. Moreover, CCIP Vulnerability Alerts are posted daily on the CCIP website and contain a summary of a vulnerability or patch deemed important by its operations center for general public release.[38]

Several commercial organizations – including the New Zealand company Co-logic – also provide vulnerability alerts filtered and tailored for their customers.[39]

## Law and Legislation

### Crimes Amendment Act 2003: Crime Involving Computers

The Crimes Amendment Act came into force in October 2003. It includes four new offenses relating to the misuse of computers and computer systems. These offenses are:

- Accessing a computer system for a dishonest purpose (Section 249);

[36] See also the Country Survey on Australia in this volume.
[37] http://www.auscert.org.au.
[38] http://www.ccip.govt.nz/vulnerability-alerts.html.
[39] http://www.cologic.co.nz/aboutus.html.

- Damaging or interfering with a computer system (Section 250);
- Making, selling, or distributing or possessing software for committing a crime (Section 251);
- Accessing a computer system without authorization (Section 252).The terms "access" and "computer system" are defined in Section 248.

The first two offenses carry a range of penalties depending on the seriousness of the offense, with a maximum of seven and ten years' imprisonment respectively, while the remaining offenses carry a maximum penalty of two years' imprisonment.

The Section 249 offense involves accessing a computer system directly or indirectly, either to obtain a benefit for oneself or to cause loss to another person, or with intent to do so. The essential element of the crime in either case is dishonesty or deception (which is separately defined in Section 240(2)).

The Section 250 offense involves intentional or reckless destruction, damage, or alteration of a computer system. In the most serious case, if this is done by a person who knows or ought to know that danger to life is likely to result, the section provides a maximum penalty of ten years' imprisonment. In cases where a person damages, deletes, modifies, or otherwise interferes with or impairs any data or software without authorization, or causes a computer system to either fail or deny service to any authorized users, the maximum penalty is seven years' imprisonment.

The key element of the Section 251 "sale, supply, or distribution" offense is that the person must either know that a crime is to be committed, or must promote the software in question as being useful for the commission of a crime, knowing that or being reckless as to whether it will be used for such a purpose. In the case of the "possession" offense, the key element is intention to commit a crime.

In practice, the more significant of these two offenses is likely to be Section 252, which in effect makes computer "hacking" a criminal offense. The offense is simple unauthorized access, whether direct or indirect, to a computer system, knowing that or being reckless as to whether one is unauthorized to access that computer system.

Sections 253 and 254 contain qualified exemptions in respect of the Section 252 offense for the New Zealand Security Intelligence Service and the Government

Communications Security Bureau respectively, where those organizations are acting under the authority of (in the case of the NZSIS) an interception warrant or (in the case of the GCSB) a computer access authorization issued under Section 19 of the GCSB Act 2003.[40]

[40] http://www.cybercrimelaw.net/laws/countries/new_zealand.html.

# Norway

## Critical Sectors

In April 2006, the Commission for the Protection of Critical Infrastructures in Norway submitted a report to the Ministry of Justice and the Police that defined the critical infrastructures of Norway as follows: "Critical infrastructures are those constructions and systems that are essential in order to uphold society's critical functions, which in time safeguard society's basic needs and the feeling of safety and security in the general public."[1]

Based on this definition, the commission identified the critical sectors, distinguishing between critical infrastructures and critical societal functions. A societal function is critical when it is indispensable for covering society's basic

[*] The country survey of Norway was reviewed by Stein Henriksen, Norwegian National Security Authority; Håkon Styri, Norwegian Post and Telecommunications Authority; Einar Oftedal, Norwegian National Security Authority; and Lene Bogen Kaland, Norwegian National Security Authority and National Information Security Co-ordination Council.

[1] Commission for the Protection of Critical Infrastructures. "Protection of Critical Infrastructures and Critical Societal Functions in Norway", Report NOU, 2006:6, (April 2006), English summary, p.4.
http://www.regjeringen.no/upload/JD/Vedlegg/Norwegian_CIP_Commision_-_Report_NOU_2006_No_6_English_summary.pdf.

needs. These "critical societal functions" are themselves dependent on different infrastructures, some of which are deemed to be critical. The criticality of infrastructures is assessed according to three criteria: dependency (a high degree of dependency on other infrastructures implies criticality), alternatives (few or no alternatives imply criticality), and tight coupling (a high degree of linkages to other infrastructures implies criticality).

Using these criteria, the commission identified the following critical infrastructures:

- Electrical Power,
- Electronic Communication,
- Water Supply and Sewage,
- Transport,
- Oil and Gas,
- Satellite-based Infrastructure.[2]
- These critical infrastructures provide the basis for the following critical societal functions:
- Banking and Finance,
- Food Supply,
- Health Services, Social Services, and Social Security,
- Police Services,
- Emergency and Rescue Services,
- Crisis Management,
- Parliament and Government,
- Judiciary,
- Defense,
- Environment Surveillance,
- Waste Treatment.[3]

[2] Ibid., p. 5.

[3] Ibid.

## Past and Present Initiatives and Policies

Over the past few years, and as a result of technological developments, there has been an increased focus on CIIP. CIIP has been regarded as a security issue in Norway since the end of the 1990s. In fact, CIIP was placed on the political agenda by the government commission on "A Vulnerable Society". Moreover, US policy has been an important trigger in putting CIIP on the political agenda in Norway as a political, security, and economic issue.[4]

### Policy Statements

In 1998, the State Secretary Committee for ICT[5] formed a subcommittee with a mandate to report on the status of ICT vulnerability efforts in Norway. Furthermore, the importance of CIIP is also stressed by the Defense Review 2000 and the Defense Policy Commission 2000.[6] In the aftermath of attacks in the US on 11 September 2001, the government considered it necessary to increase national safety and security, particularly within civil defense, in the Police Security Service, and in emergency planning within the health sector.[7]

### Report A Vulnerable Society

The governmental commission on A Vulnerable Society was established by royal decree on 3 September 1999. It was active from 1999 until 2000. The findings gave important input to the national planning process.[8] The commission's task was to study vulnerabilities in society with a broad perspective. The mandate was to assess the strengths and weaknesses of current emergency planning, to assess priorities and tasks, and to facilitate increased awareness, knowledge, and debate about vulnerabilities.

[4] Information provided by an expert.
[5] "Statssekretærutvalget for IT – SSIT".
[6] Information provided by an expert.
[7] Report No. 17 to the Storting (2000–2001).
[8] Information provided by an expert.

The government commission identified several focus areas. One of these was CI.[9] In its green paper A Vulnerable Society,[10] the commission placed great emphasis on the significance of ICT for the vulnerability of society in general. The commission, in what was probably its most controversial proposal, recommended that responsibility for safety, security, and emergency planning should be concentrated in a single ministry.[11] Furthermore, a strategy based on the following pillars was proposed:[12]

- Partnership between the public and private sectors;
- Promotion of information exchange,
- Establishment of an early-warning capacity,
- Harmonization and adjustments of laws and regulations,
- Public responsibility for CIP.

## ICT Vulnerability Project

The ICT Vulnerability Project was an interdepartmental group commissioned by the Ministry of Trade and Industry in 1999. The project collaborated with the government commission on A Vulnerable Society, and the two groups coordinated their findings on ICT vulnerabilities.[13] In the ICT Vulnerability Project, each sector authority evaluated the risks linked to specific functions in that sector. A common feature of these evaluations is that each individual sector operation is dependent on its own ICT user systems as well as on the public telecommunications services. Therefore, robust access to telecommunications seems to be very important to most sectors. The telecommunications services are dependent on ICT. This project resulted in the publication of the National Strategy for Information Security in 2003.

[9] Jan Hovden. "Public policy and administration in a vulnerable society: regulatory reforms initiated by a Norwegian commission." In: Journal of Risk Research, Vol. 7, No. 6, pp. 629-641.

[10] http://www.regjeringen.no/Rpub/NOU/20002000/024/PDFA/NOU200020000024000DDDPDFA.pdf (in Norwegian).

[11] Ibid.

[12] Ibid.

[13] Dependability Development Support Initiative (DDSI). "European Dependability Policy Environments", Country Report Norway, (April 2002 version).

## Safety and Security of Society

On 5 April 2002, the Ministry of Justice and the Police presented its 17th report on the Safety and Security of Society to the Norwegian Storting (parliament). The report is a comprehensive statement of the government's proposals regarding the reduction of vulnerabilities in modern society and measures to increase safety and security in the future. It states that when assessing the vulnerability of society, it is important to "consider the consequences of lapses in CI, such as a lapse in the distribution of power or a lapse in telecommunication".[14] The recommendations laid the basis for new government measures, including most importantly the formation of the new Directorate for Civil Protection and Emergency Planning (DSB) in 2003.[15]

## National Guidelines to Strengthen Information Security, 2007-2010

The Norwegian government published a national strategy for securing ICT systems in Norway in June 2003.[16] The strategy involved all aspects of ICT security, ranging from security for individuals, businesses, and the daily activities of the government to the security of IT-dependent critical infrastructure. As a result of the recommendations of the strategy, the NorCERT, NorSIS, and KIS organizations were established (for more information on these organizations, see below in the chapters on Organizational Overview and Early Warning and Public Outreach). In 2007, this was supplanted by the National Guidelines to Strengthen Information Security, 2007–2010.

[14] Report No. 17 to the Storting (2000–2001). "Statement on Safety and Security of Society" (April 2002). http://www.regjeringen.no/en/dep/jd/Documents-and-publications/Reports/Reports/2002/Statement-on-Safety-and-Security-of-Soci.html?id=420173.

[15] http://www.dsb.no/forside.asp.

[16] The Norwegian Government. "National Strategy for Information Security: Challenges, Priorities and Measures". http://webdomino1.oecd.org/COMNET/STI/IccpSecu.nsf/viewHtml/index/$FILE/Norway_Nat%20strat%20info%20security.pdf. This strategy proposed several initiatives for improving security based on the "OECD Guidelines for the Security of Information Systems and Networks".

These guidelines state three overriding targets for the work in the field of information security:

- Resilient and secure critical infrastructures and support systems for critical societal functions;
- A good security culture guiding the development and use of information systems and sharing of electronic information;
- High competence and a focus on research about information security.

Based on these three targets and on present security challenges, 11 objectives have been identified that will form the basis of concrete measures by the National Information Security Co-ordination Council (KIS):

- Increased protection of ICT infrastructures critical to society;
- Review of legislation for information security;
- Categorization of information and information systems;
- Implementing risk and vulnerability analyses;
- Awareness-raising and sharing of knowledge;
- Rapid and co-ordinated warning and incident management;
- Promoting use of standards and certifications;
- Increasing focus on R&D, education, and development of competencies in the area of information security;
- Establishing a co-ordinated scheme for identity management;
- Co-ordinating and developing Norwegian international participation;
- Continued development of the National Information Security Co-ordination Council.[17]

[17] Ibid.

## Report on the Protection of Critical Infrastructures and Critical Societal Functions in Norway

This report was issued in April 2006 by the Commission for the Protection of Critical Infrastructure for the attention of the Ministry of Justice and Police and represents the most recent analysis of CIP and CIIP in Norway. It is a comprehensive assessment on how critical infrastructures and critical societal function are protected in Norway and analyzes the impact of recent evolvements (emergence of new threats, shifts in the ownership of infrastructures, reorganizations within the government) on CIP and CIIP.

As mentioned above, the report starts by defining critical sectors and critical societal functions and clarifies the concepts of threats, risks, vulnerabilities, prevention, etc. Furthermore, it provides an overview on the situation in all critical sectors and functions.[18]

The report also contains various recommendations to improve the protection of critical infrastructures. The commission highlights the importance of coordinating the various CIIP efforts and recommends that the Ministry of Justice and Police assume leadership with regard to this task.[19]

## An Information Society for All

The report "An Information Society for All" was issued in December 2006 by the Ministry of Government Administration and Reform. The purpose of the report is to show the state of affairs in the ICT sector, and to invite debate on challenges and the way ahead. Chapter 9, dealing with ICT security, describes a number of security measures necessary to achieve secure ICT infrastructures. The

[18] "Protection of Critical Infrastructures and Critical Societal Functions in Norway", op. cit, p. 13ff.

[19] Ibid., p. 7.

report also clarifies responsibilities among several ministries – both in relation to preventive security work and responsibilities during a crisis.[20]

## Organizational Overview

In Norway, the ministry or authority that has responsibility for an area during peacetime or non-crisis times also has responsibility during times of crisis and war. This system also applies to CIIP. The coordinating authority on the civilian side is the Ministry of Justice and Police. The overall authority for ICT security is the Ministry of Government Administration and Reform, which took over this task from the Ministry of Trade and Industry, while the Ministry of Defense is responsible on the military side. The Ministry of Transport and Communications has responsibility for the communication sector in Norway, including all related security issues. The directorates and authorities that are responsible for handling the various aspects of CIIP on behalf of the ministries are answerable to the respective ministries.[21]

In order to promote public-private partnerships, the National Information Security Co-ordination Council (KIS) cooperates with the private sector.

### Public Agencies

#### Directorate for Civil Protection and Emergency Planning (DSB)

The Directorate for Civil Protection and Emergency Planning (DSB) was established on 1 September 2003, replacing the former Directorate for Civil Defense

[20] Report No. 17 (2006–2007) to the Storting. "An Information Society for All". http://www.regjeringen.no/en/dep/fad/Documents/Government-propositions-and-reports-/Reports-to-the-Storting-white-papers/20062007/Report-No-17-2006---2007-to-the-Storting.html?id=441497/.

[21] The Office of the Auditor General. "The Office of the Auditor General's Investigation into the Authorities' Work to Secure IT Infrastructure". http://www.riksrevisjonen.no/NR/rdonlyres/2E806C9B-CB55-4F65-9BBA-09D23E3D6044/0/Eng_Doc_3_4_2005_2006.pdf.

and Emergency Planning and the Directorate for Fire and Electrical Safety. The DSB is subordinate to the Ministry of Justice and Police, and its main task is to serve as a center of resources and expertise for emergency contingency planning. The DSB is a point of contact between the central authorities and regional commissioners during disasters occurring in peacetime.

To ensure adequate preparedness measures in the community, the DSB devotes considerable efforts to ensure that all Norwegian municipalities carry out risk and vulnerability analyses. The DSB works to ensure that activities involving preparedness responsibilities lead to the implementation of internal control systems to ensure the quality of emergency planning at local government level. The DSB also supervises the planning efforts in the ministries and offices of the regional commissioners. In the context of CIIP, the DSB coordinates and carries out research on vulnerabilities and the protection of critical assets in cooperation with other actors.[22]

## Norwegian National Security Authority (NSM)

The Norwegian National Security Authority (NSM)[23] was established on 1 January 2003 and coordinates preventive IT-security measures. It controls the level of security, e.g., of central and local public administration, and monitors private suppliers of goods and services to the public when the products or services concerned are security-sensitive. The NSM also develops technical and administrative security measures and issues threat evaluations and vulnerability reports. The Ministry of Defense funds and administers the NSM. Moreover,

- The NSM hosts SERTIT,[24] the public Certification Authority for IT Security in Norway.
- The NSM operates NorCERT (see chapter on Early Warning and Public Outreach).

[22] http://www.dsb.no/forside.asp/.
[23] http://www.nsm.stat.no.
[24] http://sertit.no/article/1.

## Norwegian Post and Telecommunications Authority (NPT)

The Norwegian Post and Telecommunications Authority (NPT)[25] is an autonomous administrative agency under the Norwegian Ministry of Transport and Communications, with monitoring and regulatory responsibilities for the postal and electronic communications markets in Norway. The NPT is responsible for contingency planning regarding the public electronic communications infrastructure.

## The National Information Security Co-ordination Council (KIS)

The National Information Security Co-ordination Council (KIS) was established in May 2004.[26] It is chaired by the Ministry of Government Administration and Reform and consists of representatives from six ministries, the Prime Minister's Office, and ten different directorates. KIS has no authority to make decisions, but provides a platform for discussions and advises ministries and government agencies in topics related to ICT security, national security (interests), critical information infrastructure, common standards, working methods for ICT security, risks, and vulnerabilities.

KIS will have a central role in the implementation of the national guidelines to strengthen information security by:[27]

- Keeping track of the implementation of measures in different areas of responsibility;
- Identifying cross-sectoral challenges in information assurance that have to be followed up;
- Pushing for the implementation of measures of a cross-sectoral nature.

The KIS will be in close dialog with the private sector, local government, and others that may be impacted by the guidelines during the implementation of measures.

[25] http://www.npt.no.

[26] http://www.kis.stat.no.

[27] Ibid.

### Public-Private Partnerships

In reaction to the report A Vulnerable Society, public-private initiatives have been established to enhance early-warning capabilities, e.g., NorCERT and NorSIS. In addition, there are sectoral co-operation bodies within sectors such as electric power, finance, oil, and telecommunications. KIS co-operates with the private sector in the further development of the guidelines. Representatives of the private sector are invited to participate in working groups when required.

## Early Warning and Public Outreach

### NorCERT

The Norwegian Computer Emergency Response Team (NorCERT) was formally established in January 2006 as an operational department of the NSM and is the national CERT for Norway. NorCERT consists of two integrated sections:[28]

- The Warning System for Digital Infrastructure (VDI) was established in 2000 by the government. VDI intended to enable security professionals to chart the extent of the threat to vulnerable information infrastructure through the use of a national monitoring system to collect data on emerging threats. Since 2006, VDI has been an integrated part of NorCERT.
- The Incident Handling Section is responsible for incident handling and coordination, including vulnerability handling and artifact handling.
- Together, these two sections manage the Operation Center, where they maintain an up-to-date view of current cyber-threats and day-to-day operational matters.

[28] http://www.nsm.stat.no/Arbeidsomrader/Internettsikkerhet-NorCERT/Internettsikkerhet---NorCERT/NorCERT/English/.

Apart from early warning and incident-handling, NorCERT also serves as a point of contact for similar organizations abroad and shares information with other response teams regarding emerging threats.

## UNINETT CERT

The Computer Emergency Response Team of the UNINETT (the academic research network)[29] was already formed in 1995. Its constituency consists of the Norwegian state universities, colleges, and research and development institutions. The team was created to contribute to better internet security for UNINETT member institutions, and to serve as a focal point for security issues regarding UNINETT member institutions.[30] The basic duty of UNINETT CERT is to provide assistance on handling and investigating incidents involving one or more members of the constituency, but it also collaborates with NorCERT to improve overall information security.[31]

## Norwegian Center for Information Security (NorSIS)

The aim of the Norwegian Center for Information Security (NorSIS) is to improve the overall level of information security in Norway. Its primary target groups are SMEs and the public authorities. NorSIS engages in the following activities:

- Making the public aware of the importance of information security by means of training and information;
- Compiling guidelines and tutorials for users;
- Establishing an overall awareness towards information security.
- The NorSIS has its own web page[32] offering news, advice, and guidance. In addition, the NorSIS helps to disseminate information during serious incidents.

[29] http://forskningsnett.uninett.no/index.en.html.
[30] http://cert.uninett.no/policy.html.
[31] Ibid.
[32] http://www.norsis.no.

## Norwegian Post and Telecommunications Authority

The Norwegian Post and Telecommunications Authority (NPT) has responsibility for contingency planning related to the public telecommunications infrastructure. Its area of responsibility includes the following tasks:

- Considering investment in measures designed to increase the robustness of the telecom networks;
- Conducting inspections to see that the required measures are implemented;
- Creating awareness, improving expertise, and offering guidance to operators, users and other players (courses, seminars, company visits, establishment of forums of expertise, etc.);
- Arranging joint exercises and developing cooperation between the operators of telecom networks.

Electronic communications providers who provide essential electronic communications services to users who have socially critical functions must notify the NPT of significant operational and technical problems that could reduce or have reduced the quality of services.

The establishment of the nettvett.no portal[33] in April 2005 is one example of the NPT's instructional undertakings within the security area. This portal provides information about the secure use of the internet.

## Law and Legislation

There are a number of regulations concerning information assurance and critical infrastructures, distributing responsibility onto several bodies. The most pertinent and overriding regulations concerning CIIP in Norway are:

[33] http.//www.nettvett.no.

- The Security Act:[34] This act applies to the protection of objects and information from incidents threatening security.
- The Electronic Communications Act:[35] This act applies to activity connected to the transmission of electronic communications and the associated infrastructure, services, equipment, and installations.
- Personal Data Act:[36] This act applies to the processing of personal data wholly or partly by automatic means, and other processing of personal data that is part of or intended to form part of a personal data filing system.

In addition to these, there are sector-specific regulations. Most Norwegian public and private bodies are subject to relevant regulations issues by various authorities. The national guidelines to strengthen information security will, inter alia, focus on making regulations about information assurance more consistent and user-friendly.

[34] http://ww.nsm.stat.no/.

[35] http://www.npt.no/portal/page/portal/PG_NPT_NO_EN/PAG_NPT_EN_HOME/PAG_ PUBLICATIONS/PAG_REGULATIONS/.

[36] http://www.datatilsynet.no/templates/Page____194.aspx/.

# Poland

## Critical Sectors

According to expert opinion, Poland perceives those physical and cyber-based systems as critical infrastructures that are essential to the minimum required operations of the economy and the government. They include the following sectors:

- Telecommunications,
- Energy,
- Banking and Finance,
- Transportation,
- Chemical Industry,
- Water and Sewage Systems,
- Private and governmental emergency services. [1]

[*] The Country Survey of Poland was reviewed by Tomasz Prząda, Polish Internal Security Agency, Michał Młotek, Polish Ministry of Interior and Administration, and Mirosław Maj and Krzysztof Silicki, NASK/CERT Polska, Poland.

[1] Mieczyslaw Borysiewicz and Slawomir Potempski. "Critical Infrastructure Protection: actions to be implemented shortly". In: ECN European CIIP Newsletter, August/September 2005, Vol.1 No. 2, pp. 21ff. http://www.irriis.org/ecn/European%20CIIP%20Newsletter%20No%202.pdf.

In the same expert document, information and communications systems are more specifically defined as key assets within the overall realm of critical infrastructures. Therefore, among other things, it is recommended that the control systems be enhanced and prioritization plans be developed for ensuring cybersecurity.

## Initiatives and Policy

It was officially acknowledged in Poland in 2000 that access to information has become increasingly significant for the economy and social life, and therefore the Polish government seeks to use means of communication to support the economy and to improve the public standard of living. These government activities were in response to the Polish parliament's resolution of 14 July 2000 on building the foundation of an Information Society in Poland, which underlines that modern technologies, services and applications of telecommunication, communication, and multimedia services may be a catalyst for economic growth, increase the competitiveness of the economy, create jobs, foster the development of the democratic state and its regions, assist in education and health care, and improve access to cultural goods.[2] As a consequence of this acknowledgement, several initiatives have been launched. On the one hand, these initiatives mainly fall into two categories – the development of the Polish Information Society (ePolska) and the application of elements of the Information Society to the public administration (e-government). On the other hand, issues related to the protection and security of information and its infrastructure are addressed exclusively within a single research and development organization, the Polish data networks operator and Research and Academic Computer Network (NASK). The latter are addressed in the early warning and public outreach section of this chapter.

[2] https://www.oecd.org/dataoecd/9/38/1952799.pdf.

## ePoland

In reaction to the above-mentioned parliamentary resolution on building the foundations for a Polish Information Society, the Council of Ministers adopted two relevant documents in 2001: A strategic publications called Aims and Directions of the Information Society Development in Poland and a paper on practical aspects called Action Plan for the Information Society Development in Poland for the years 2001–2006 – ePoland.[3] The strategic document had been prepared by the State Committee for Scientific Research in cooperation with the then Ministry of Telecommunications. It set out the following priorities:[4]

- Universal access to information;
- Information technology education;
- Changes in employment structure;
- Law and offences in the information and communications field;
- Electronic documents and commerce;
- Public procurement;
- Information technology implementation in the administration;
- Information and communication technology market development;
- Science and culture.

The Action Plan ePoland, oriented more towards practical applications, followed the European action plan eEurope – an Information Society for All that was issued by the European Commission in May 2000.[5] The ePoland program[6] deals with a number of issues connected with the implementation of the Information Society, taking into consideration developments and realities in Poland. An absolute precondition for realizing the aims enshrined in the program is broad-

[3] Elbzbieta Stefanczyk. "Polish libraries in the information society". http://www.svkbb.sk/colloquium/zbornik/data/stefanczyk.pps.

[4] https://www.oecd.org/dataoecd/9/38/1952799.pdf.

[5] http://merlin.obs.coe.int/show_iris_link.php?iris_link=2000-6:5&id=392.

[6] Europäische Audiovisuelle Informationsstelle. http://merlin.obs.coe.int/iris/2001/10/article33.de.html.

band, universal, affordable, and safe access to new electronic communication networks. In practical terms, ePoland comprises the following aims: Preparing society for rapid technological changes in the social and economic sphere due to the emergence of the Information Society, education of adults in the area of information technologies, and the promotion of professions connected with the application of these technologies. It foresees the adaptation of the legislative framework to the standards of rapid technological progress and the information age. Moreover, the ePoland action plan is to be compatible with the requirements of the electronic economy. This could be achieved by introducing legal regulation on electronic signatures, electronic transactions means, legal protection of databases, providing universal access to information technology, and electronic commerce. An additional advantage for the development of the Information Society in Poland is identified in the implementation of an electronic procedure in public procurement, facilitating online access to public administration, enhancing the participation of small- and medium-sized enterprises in e-commerce, and the elaboration of models for digital media in Poland.

In 2003, the ePolska action plan was updated in preparation for its adoption on 13 January 2004 by the Council of Ministers. Called ePoland – The Strategy on the Development of the Information Society in Poland for the years 2004–2006, it identifies information technology as a key challenge for Poland and specifies three priorities in order to achieve the goal of becoming a competitive knowledge-based economy and improving the quality of life of citizens:[7]

- Common access to electronic content and services;
- The development of valuable content and services accessible via the internet;
- The ability to use them.

The official projection of the prospects of the Information Society in Poland in the middle range perspective is contained in the document entitled The Proposed Direction of the Information Society Development to the year 2020, which was issued in late 2004. The document focuses on the prioritization of various

[7] http://www.itu.int/wsis/stocktaking/scripts/documents.asp?project=1103559107&lang=en.

aspects of public life in the context of Information Society development, and on the problem of ICT infrastructure as a factor shaping the overall framework of development opportunities.[8]

## E-government

The second pillar of Polish Information Society policies concerns the government's use of ICT and accessibility of government services. One of the government's most important programs for integration of information technology is the summary plan for communications technology development and its application in government administration, drawn up by the Ministry of the Interior and Administration.[9] In July 2003, the government accepted a draft bill on the "informatization of the public administration". The bill creates a legal framework for the monitoring and coordination of the various informatization projects of the public administration and specifically aims at the following:[10]

- To ensure compatibility of public IT systems and registries;
- To establish a legal framework for the development of e-government in Poland;
- To attain budgetary savings thanks to better coordinated spending on IT projects and to shift a number of public services to electronic platforms;
- To enhance the efficiency of the public administration and increase the quality of its services.

The bill empowered what was then the Ministry of Scientific Research and Information Technology (now the Ministry of Science and Higher Education) to audit all public IT systems for their appropriateness and viability and to establish mandatory standards for the exchange of documents and information

[8] Andrzej M.J. Skulimowski. "The Information Society in Poland: recent developments and future perspectives". http://www.scholze-simmel.at/starbus/r_d_ws1/poland.pdf.

[9] https://www.oecd.org/dataoecd/9/38/1952799.pdf.

[10] Marcin Piatkowski. "Information Society in Poland. A Prospective Analysis."Transformation, Integration and Globalization Economic Research, Leon Kozminski Academy of Entrepreneurship and Management, Warsaw, Poland, (January 2004). http://www.tiger.edu.pl/onas/piatkowski/Information_Society_in_Poland_A_Prospective_Analysis.pdf.

between various public institutions. Moreover, the bill opens a way for citizens to deliver various public documents electronically.

Common access to e-government services is conditional on providing all citizens with internet access, or at least establishing a network of public internet access points. These projects have not been finished yet. In March 2005, the then Ministry of Science and Information Technology published a statement on "the comparative position of Poland in basic categories of e-government services". Among various services delivered by the public administration via internet, two basic categories can be pointed out based on the target group of the specific service: government to citizen (G2C) – with its reverse (C2G) services – and the second one, government to business (G2B) and reverse (B2G) services. Poland ranks low in the overall European comparison.[11]

## National Foresight Program

The Polish National Foresight Program was initiated in early 2003 by the then Ministry of Science and Information Technology. It is conceived as a method of building a vision for the medium- and long-term development of scientific and technical policy, its directions, and priorities, and is being implemented at the initiative of the Ministry of Science and Higher Education. An initiatory group of high-ranking experts was responsible for the definition of the foresight areas. The program's scope of realization covers three research areas: sustainable development, security, and information and telecommunications technologies. The latter area is to be coordinated by the Polish Ministry of Science and Higher Education[12] and centers on five major issues:

- Access to information;
- ICT and the society;
- ICT and education;
- e-Business;

[11] Andrzej M.J. Skulimowski. "The Information Society in Poland: recent developments and future perspectives". http://www.scholze-simmel.at/starbus/r_d_ws1/poland.pdf.

[12] Ibid.

- New media.

The foresight program is organized and managed by a coordination consortium, the conceptual work is done by different expert panels, and partnership institutions give scientific and analytical support.[13]

## Organizational Overview

Within the Polish government, two ministries have responsibilities that impinge upon the country's information infrastructures and their protection – the Ministry of Science and Higher Education and the Ministry of the Interior. As a public-private partnership, the Polish Competence Center for eGov and eEdu[14] strives to provide a platform to bring together the public sector and the IT companies.

### Public Agencies

In January 1991, the Parliament of the Republic of Poland passed an act creating the State Committee for Scientific Research (KBN). This governmental body was responsible for the science and technology policy of the state. Following the Council of Ministers' regulation of 18 March 2003, the Committee for Scientific Research was integrated into the newly founded Ministry of Science and Information Society Technologies. For the first time in the history of the Republic of Poland, a governmental body responsible for the country's information technology was created. After the parliamentary elections in 2005, the Ministry of Education and Science was established through the merger of the Ministry of National Education and Sport and the Ministry of Science and Information Technology. In mid-2006, the next reorganization resulted in the creation of the Ministry of Science and Higher Education.[15]

[13] http://www.foresight.polska2020.pl/mis/en.
[14] http://www.egov.edu.pl.
[15] http://www.eracareers-poland.gov.pl/page.html?kid=549:4620.

## Ministry of Science and Higher Education

The main player and the coordinating body for science and technology policies is the Ministry of Science and Higher Education, which is involved in all policies relating to information infrastructures and their protection. Until November 2005, it was called the Ministry of Science and Information Technology. Its responsibilities relating to critical information infrastructures include:

- IT infrastructure, networks, and systems of the public administration;
- The establishment of IT standards for the public administration;
- Supervision and support of IT projects in public, central, and local administrations;
- Education and vocational training in Information Technology standards;
- The development of an Information Society in Poland;
- International cooperation within the IT sector and participation in EU programs.[16]

The establishment of this ministry (and of its immediate predecessor) created a single coordinating institution for all state policies on informatization, it advises other ministries and institutions on informatization strategies, and it ensures the compatibility of national public IT systems and the economic viability of new informatization projects. Moreover, the national foresight program Poland 2020 is also located under the auspices of the Ministry of Science and Higher Education.

## Ministry of the Interior and Administration

The Ministry of the Interior and Administration is crucial insofar as it is responsible for the national IT infrastructure, the national teleinformation system, and the national information administrative systems. These responsibilities are handled by the Department of Information Technology Development on the one hand, and through the Department of Teleinformational Infrastructure on

[16] Skulimowski, op. cit.

the other hand. Both these departments are located at the Undersecretariat of State.[17] The latter is mainly in charge of maintenance of IT systems of the ministry, with particular attention given to security and availability of all processed data. Moreover, its responsibilities include:[18]

- Supervision of the teleinformation networks used by government entities for accessing the state registries, planning, developing, and coordination of all IT networks of the ministry;
- Acting as an administrator of the government communication systems, including radio communications and also isolated systems;
- Fulfillment of tasks regarding the Polish Local Domain of the TESTA network and communication center of all the units of the ministry, including supervision and coordination in regard to isolated TESTA SIS/VIS networks;
- Supervision and maintenance of the Public Key Infrastructure (PKI) of the ministry as well as coordination of all tasks regarding digital signatures;
- Building and implementation of a special communication infrastructure for all public security and rescue forces;
- Maintaining continuity of all infrastructure considered essential for the state teleinformation systems and government communication;
- Prevent internal and external threats through securing the above-mentioned infrastructures.

Overall, the Ministry of the Interior and Administration is responsible for digitizing the public administration, developing the Information Society, and protecting it from exploitation of its vulnerabilities.

[17] http://www.mswia.gov.pl/portal/en/3/63.

[18] Information provided by an expert.

## Public-Private Partnerships

### The Polish Competence Center for eGov and eEdu

The Polish Competence Center for eGovernment and eEducation was founded in February 2005 by four partners, including the Fraunhofer Institute for Open Communications FOKUS (Berlin), the Poznan Supercomputing and Networking Center (Poznan), the Foundation for Economic Education (Warsaw), and Witold Sartorius, the designated head and CEO of the center. It is currently run by the Foundation for Economic Education as a consortium and plans to become an incorporated not-for-profit company in Poland. The competence center aims at being an independent and trustworthy platform to bring the public sector, as a potential qualified customer, together with the IT companies to initialize successful and innovative IT projects with additional and significant cost saving and revenues for the partners. Therefore, the center supports and coaches partners and public sector clients during the whole process of preparing, organizing, and financing eGov and eEdu projects and brings them to the final implementation stage.

This includes tasks related to technology, organization and re-organization, as well as financial engineering in bigger and smaller projects. The center acquires, checks, tests, shows, and promotes modern IT and software solutions for the public sector and education. It has close links with Polish government bodies at both the ministerial and local levels. Moreover, the center also addresses projects in support of small and medium enterprises. The center's activities are driven by the belief that the strategic planning and realization of cost-effective IT solutions is the key to success for the Polish administration and public sector. Therefore, it aims at bringing the respective relationships to the next level by creating public-private institutional partnerships focused on the promotion of internet business solutions for the local governments. To this end, the competence center cooperates with a variety of programs and initiatives such as, among others, ePolska, the Cisco networking Academy Program, and the Polish education portal Interkl@sa.[19]

[19] http://egov.edu.pl/?id=2&lang=2.

## Early Warning and Public Outreach

As mentioned earlier, the concerns of information infrastructure protection in Poland are mainly addressed by one particular organization – the Polish data networks operator NASK.

### NASK Polska

NASK connected Poland to the internet in 1991. Since 1993, it has been a research and development organization and the leading Polish data networks operator. It offers telecommunications and data solutions to business, administration, and academic customers. Its service packages comprise broadband internet access, corporate networks, data transmission, collocation and hosting, videoconferencing, and network security services. NASK also carries out scientific and research activities in cooperation with the faculty of electronics and information technology at the Warsaw University of Technology – in particular, its cooperation with the Institute of Control and Computation Engineering led to the establishment of a biometric laboratory – and it is a member of many international organizations and associations including the Forum of Incident Response and Security Teams (FIRST) (see the survey on FIRST in this volume), the Council of European Top Level Domain Registries (CENTR), the Trans-European Research and Education Networking Association (TERENA), and the European IP Networks (Réseaux IP Européens, RIPE). Moreover, NASK is the Polish national registry of internet names in the .pl domain. The Polish Computer Security Response Team (CERT Polska), a part of the NASK organization, is very much engaged in information infrastructure protection and security issues.[20]

[20] http://www.nask.pl/run/n/home.

## CERT Polska

The Polish Computer Emergency and Response Team that is now called CERT Polska was formerly known as CERT NASK and was established in March 1996 by the NASK director. Its goals include:

- To provide a single trusted point of contact in Poland for the community of NASK customers and other networks in Poland to deal with network security incidents and their prevention;
- To respond to security incidents in networks connected to NASK and networks connected to other Polish providers reporting security incidents;
- To provide security information and warning of possible attacks in cooperation with other incident response teams all over the world.

The CERT Polska team registers all requests, alerts, and incoming and outgoing information and provides statistical data and reports on registered incidents. It also provides help for sites that have security problems, and supplies current information about security problems and solutions for dealing with them.[21] CERT Polska itself points out that the creation and maintenance of a computer security and incident response team benefits the government in many respects. Four of its areas of activities in particular contribute to critical infrastructure protection: Early warning and alerting, centralized security management, security response, and auditing.[22] CERT Polska signed a cooperation agreement on IT security with the Information Security Department of the Polish Internal Security Agency in July 2004.[23] It also organizes a highly respected annual conference under the auspices of NASK. The SECURE conference series, organized since 1997, brings together company and IT managers; specialists in information system, network, and database security; and telecommunications and data network users who are interested in security issues. Co-sponsored by ISSE (Information Security Solutions

[21] http://www.cert.pl/index3.html?id=24.

[22] Przemek Jaroszewksi. "All you wanted to know about CSIRTs but were afraid to ask". http://www.ceenet.org/workshops/lectures2005/Przemek_Jaroszewski/Ohrid_Day1.pdf.

[23] Mirosław Maj. "CERT Polska and CIIP in Poland", (2005). http://www.terena.org/activities/tf-csirt/meeting15/ciip-maj.pdf.

Europe), ENISA (European Network and Information Security Agency) and the Polish Ministry of the Interior and Administration, SECURE is Europe's largest conference on data communications safety.[24]

## CERT GOV PL

On 1 February 2008, the Internal Security Agency established the government's computer incident response team (CERT GOV PL). Its goals include ensuring and developing the ability of public administration units to defend themselves against cyber-threats, in particular against attacks on the infrastructure consisting of IT systems and networks, the disruption or destruction of which might to a large extent threaten the life and health of people, national heritage, and the environment, or result in considerable financial losses and disrupt the operation of the state.

The goals of the CERT GOV PL include:[25]

- Creating a policy concerning cyber-defense;
- Coordination of the information workflow among the above-mentioned entities with reference to cyber-threats;
- Detection and recognition of, and response to cyber-threats;
- International cooperation concerning cyber defense;
- Playing an oversight role in relation to all national institutions, organizations, and units within governmental departments concerning cyber-defense;

The main objectives of the CERT GOV PL are:

- Collecting information concerning the current security status and threats to the critical IT infrastructure;
- Responding to IT security incidents, in particular the ones concerning the national critical IT infrastructure;

[24] http://www.nask.pl/newsID/id/431.

[25] Information provided by an expert.

- Post-incident computer forensics;
- Establishing the policy for defense of the cyberspace of the Republic of Poland;
- Training sessions and raising awareness of the topic;
- Consulting and advising with reference to cyber-security.

## ARAKIS-Gov

In 2004, ARAKIS-gov, a distributed internet-based early-warning system developed and maintained by CERT Polska (NASK) in cooperation with the Information Security Department of the Polish Internal Security Agency, was accepted as the most important system for ensuring the protection of the Polish critical information infrastructure. The goal formulated for this project is to create a real early-warning system that can detect a new threat, analyze the exploit, and create a description of a new attack.[26] Therefore, data from various sources, such as firewalls, darknets, honeypots, and anti-virus systems are correlated in order to detect emerging threats against the Polish network (also, notably, against governmental institutions), to detect new attack patterns, to monitor differences between attacks observed in Poland and in other countries, to gather statistical data, and to aid in general incident-handling activities. ARAKIS also provides a public dashboard showing a snapshot of network activity observed by the system. In the form of a polar chart, the alerts as generated by the ARAKIS system over the last 24 hours are plotted.[27]

## PIONIER-CERT

This incident response service entity is responsible for incident-handling in an academic network environment. The main purpose of this initiative is to establish a single point of contact for all security incidents occurring in the constituency of PIONIER, which consists exclusively of Polish academic research institu-

[26] Przemek Jaroszewksi, op. cit.
[27] http://arakis.cert.pl/en/index.html.

tions.[28] In order to assist system administrators in handling the technical and organizational aspects of incidents, the overall process of incident response is divided into three main stages: incident triage, incident co-ordination, and incident resolution. The incident resolution is performed in a very limited range, and is in fact limited to special cases with a potential significant impact on PIONIER's constituency. The actual range of activities in such cases may cover removing vulnerability, restoring a system that has been compromised, or providing direct technical support while colleting evidence where criminal prosecution or other disciplinary actions are being considered.[29]

## Law and Legislation

Relevant legislation as concerns the protection of data and information in Poland consists of Articles 267 to 269 of the penal code. These three articles regulate the respective crimes of

- Unauthorized access to information (267);
- Destruction, alteration, deletion, or damaging of information (268);
- Destruction, alteration, deletion, or damaging of information with particular significance for national defense, transport safety, the operations of the government, or other state authority or local governments (269).

These crimes are defined as being of increasing gravity, and the punishments range from two, three, to eight years respectively.[30]

[28] A precise list of PIONIER's constituency can be found on the website. http://arakis.cert.pl/en.

[29] http://cert.pionier.gov.pl.

[30] http://www.cybercrimelaw.net/laws/countries/poland.html.

# Russia

## Critical Sectors

During the last few years, Russia has made significant progress in improving its information infrastructure. The national security and economic welfare of the Russian Federation depends to a substantial degree on ensuring information security, a dependence that will increase in future with technological progress.

The information security is determined by the protection of national interests in the information field. The content of those interests can be inferred from the Information Security Doctrine of the Russian Federation and include the state's guarantee of human rights in the information field, IT support of the state policy of the Russian Federation, development of a domestic information industry, and the protection of information and of information and communication systems in

[*] The Country Survey of Russia 2008 was reviewed by Anatoly Streltsov, Professor at the Institute of Information Security, Lomonosov Moscow State University. We are also grateful to Martin Wählisch, Humboldt University Berlin, for his extensive research assistance and translation of Russian documents for earlier versions of this survey.

the various areas of public life. The critical sectors subject to critical information infrastructure protection are the following:[1]

- Economy,
- Domestic and Foreign Policy,
- Science and Technology,
- State Information and Communication Systems,
- Defense,
- Justice,
- Disaster Response.

The Information Security Doctrine of the Russian Federation reflects the G8 Okinawa Charter of the Global Information Society,[2] which was prepared in the year 2000. However, in the Russian Information Security Doctrine, the specific social and economic circumstances and long-term reforms of the Russian Federation as well as its experience with terrorist attacks were taken into consideration.[3] In Russia, information assurance includes not only (technical) information security, but also the safeguarding of state secrets.

## Past and Present Initiatives and Policies

In 2008, the president of the Russian Federation approved two documents, including Strategy for the Development of Information Society in Russia and Measures for Ensuring the Information Security of the Russian Federation in the Field of Information and Communication Systems use for International Information Exchange.

Earlier, the Russian government had approved the federal program The Development of United Information Environment for Education (2001–2005)

[1] Information provided by an expert.

[2] "Okinawa Charter on Global Information Society", (Okinawa, 22 July 2000). http://www.g8.utoronto.ca/summit/2000okinawa/gis.htm.

[3] Information provided by an expert.

(2001) , the Concept for the Use of Information Technologies in the Federal State Organizations (2004), a federal program entitled Electronic Russia (2002–2010) (2005), and a federal program entitled National Technological Basics 2007–2011 (2007).[4]

## Information Security Doctrine of the Russian Federation

The Information Security Doctrine[5] of the Russian Federation, adopted on 9 September 2000, is an extension of the National Security Concept[6] (approved by the President on 10 January 2000) intended to strengthen state policy regarding information security. Its aim is to help formulate legal, methodological, technical, and organizational provisions for information security in Russia and to assist the development of specific programs for this purpose. The doctrine defines the context of the nation's interests in the information sphere and assesses information threats to citizens, society, and the state. The doctrine is very comprehensive in scope and ranges over many policy areas, from data protection, personal privacy, copyright, and computer misuse (hacking) to state secrets, access to information, and the functioning of the media.[7]

Russian information security is defined in the doctrine as "the state of protection of its national interests in the information sphere defined by the totality of balanced interests of the individual, society, and the state." Russia views both public opinion and the national information systems as integral parts of its concept of information security.[8] Moreover, the Russian government considers the uncon-

[4] Information provided by an expert.

[5] "Doctrine of the Information Security of the Russian Federation". Approved by the president of the Russian Federation, Vladimir Putin (9 September 2000), No. Pr-1895. http://www.medialaw.ru/e_pages/laws/project/d2-4.htm.

[6] http://www.kremlin.ru/eng/articles/institut04.shtml.

[7] Ian Leigh. "Information Security Doctrine of the Russian Federation", (no date). http://www.isn.ethz.ch/news/dossier/ssg/pubs/books/FluriSulakshin/05A_LEIGH.pdf.

[8] Timothy L. Thomas. "Information Security Thinking: A Comparison of U.S., Russian and Chinese Concepts", (July 2001). http://fmso.leavenworth.army.mil/documents/infosecu.htm.

trolled spread of foreign media in Russia to be a threat to Russian information security and, as a result, intends to "strengthen" the Russian media.[9]

The doctrine is legally based on Russian federal laws on security, state secrets, the protection of information, and participation in international information exchange. The document is divided into four major chapters, covering 11 sections. The four main chapters are:

- Information security: This chapter defines the Russian Federation's national interests in the information sphere, referring to constitutional rights, to IT support for state policy, to the development of the information industry, and to the security of information against unauthorized access. Moreover, internal and external sources of threats to Russia's information security are identified. The doctrine acknowledges frankly that just like private monopolies and organized crime, government policy and legislation can also pose a threat. Aggressive foreign corporations and international terrorists are mentioned as major foreign threats. In the domestic arena, the critical state of the national industry as well as the under-development of the legal framework can constitute a barrier to full exploitation of information technology, particularly where e-commerce is concerned. Finally, the chapter discusses the state of information security in the Russian Federation and objectives for amending it. The deteriorating safety of data constituting state secrets is identified as a major problem;
- Methods of ensuring information security: This chapter covers legal, organizational-technical, and economic methods for information security. Moreover, it describes a number of features of information security in

[9] This aspect of Putin's doctrine has been criticized by journalists, who fear restrictions on freedom of opinion and speech. Yevgenia Albats. "Information Security Doctrine Redux". In: The Moscow Times, (14 September 2000). http://www.themoscowtimes.com/stories/2000/09/14/007.html.
The Information Security Doctrine claims to protect the interests of the individual, society, and the state in the information sphere. In fact, however, the main focus lies on the government's and society's interests in this field, and the document stresses the possible external threats to information security coming from abroad. Among these, the document mentions the dominance of certain states in the information sphere, foreign policy issues in the economic, military, and intelligence fields, and the exclusion of Russia from the information market by other states. GeoPowers. "Sicherheitskonzept Russland: Wunschdenken?", (7 February 2000). http://www.geopowers.com/Machte/Russland/russland.html.

various spheres, such as the economy, domestic policy, foreign policy, science and technology, information and telecommunication systems, defense, law enforcement, and emergency situations. Finally, it mentions international cooperation in the field of information security such as banning information warfare, supporting information exchanges, coordinating law enforcement activities, and preventing unsanctioned access to confidential information;

- The main provisions of the state policy for ensuring information security, and priority measures for implementing it: This chapter lays out – at a high level of abstraction – the policy of the government, ranging from observing the constitution to supporting the development of new technologies. The chapter suggests provisions for information security, such as developing guidelines for federal institutions. In addition, the document mentions priority measures for implementing the rule of law, an increase in the efficiency of state leadership, programs providing access to information archives, educational measures, and a system for harmonizing standards in the field of computerization and information security are mentioned;
- Organizational basis of ensuring information security: This chapter describes the functions of the system of information security, as well as the organizational elements and actors of Russia's information security system, including the president, the Federation Council of the Federal Assembly, the State Duma of the Federal Assembly, the government of the Russian Federation, the Security Council, and other federal executive authorities, presidential commissions, judiciary institutions, public associations, and citizens.

An area of obvious emphasis is the creation of a legal base for information security. The laws on the Constitution of the Russian Federation, State Secrecy, Information, Computerization, and Information Protection, Participation in International Information Exchange, and Essentials of Legislation of the Russian Federation on the Archive Collection of the Russian Federation and Archives are specifically mentioned. Legal instruments constitute one of three approaches to information security mentioned in the doctrine – the other two being organizational-technical and economic measures. Furthermore, the document stresses the threat of attacks against Russia's information infrastructure and the threat of foreign governments using information warfare techniques against Russia. In addition, special attention is given to the development of telecommunication systems, the integrity of information resources, space-based reconnaissance, and electronic-warfare facilities.[10]

## Electronic Russia

The idea of Electronic Russia[11] appeared in early 2001, when the Ministry of Economic Development and Trade was elaborating a strategic development plan for Russia up to the year 2010. The program is based on the notion that in order to reduce the country's economic lag, it is necessary to develop the hi-tech sector, where it would be possible to reach a higher productivity level than in the raw-materials sector. None of this would be possible without computers and powerful ICT.[12]

[10] Timothy, op. cit.

[11] Federal Target Program. "Electronic Russia (years 2002–2010)", approved by the government of the Russian Federation (Decree No. 65 of 28 January 2002). http://old.developmentgateway.org/download/182707/erussia_final_en_jr28-02.doc.

[12] All cities in Russia with populations over 30,000 should soon be connected to the country's "fiber-optic backbone", although the connections to individual homes and offices can still be relatively primitive. Many thousands of villages in Russia still do not have a single telephone line, so it will be many years before some of the more sparsely populated areas can hope to have a fully operational telecommunications infrastructure. Many options are under consideration to provide this infrastructure, including satellite delivery. The Electronic Russia plan seeks to deliver an increasing number of government services online, and to alleviate some of the heavy bureaucratic burden on Russia's citizens and businesses. It will then be possible to perform tasks such as tax filing and business registration online. The country's vast geographic area and the financial difficulties of the education system have encouraged Russian planners to seek creative solutions to the provision of education throughout the country. The delivery of a wide range of distance-learning packages via the internet is seen as a potentially effective solution to this problem, which the Electronic Russia plan seeks to explore. Yuri Hohlov. Institute of the Information Society. "E-Russia Program for 2002–2010", State of the Art October 2005. http://www.tedbr.com/apresentacoes/e-Brasil/e-russia_and_e-moscow_programs_2005-10-14.pdf, and http://www.e-rus.ru.

Involving various ministries[13] and coordinated by the Ministry of Telecommunications and Informatization (which became the Ministry of Information Technologies and Communication in 2004), Electronic Russia 2002–2010 is the core IT program that will lay the groundwork for a more efficient economy and public administration through mass implementation of information and telecommunications technology.[14] It is also designed to facilitate by technological means the advancement of civil institutions by securing the right of citizens to unrestricted information access, and by expanding IT training opportunities for specialists and qualified users.[15]

Electronic Russia has a nine-year planning horizon and addresses four key areas:

- Regulatory environment and institutional framework;
- Internet infrastructure;
- e-Government;
- e-Education.

The main objective of Electronic Russia is to increase the efficiency of the economy, to improve management in the public sector, and to enhance self-government by applying information and communication technologies. In order to reach this goal, the following tasks are addressed:

- To create effective legislation governing ICT;
- To ensure open communication and interaction between the state bodies, agencies, and companies by applying state-of-the-art ICT technologies;
- To create conditions for more extensive and more effective use of ICT in the economic and social spheres;
- To provide up-to-date computer training for professionals;

[13] Ministry of Economic Development and Trade, Ministry of Education, Ministry of Industry, Science and Technologies, Aviation and Space Agency, Federal Agency of Government Communications and Information with the President, Agency on Systems Management.

[14] http://www.uni-koblenz.de/~kgt/PM/SemB/Russland.ppt.

[15] http://www.bisnis.doc.gov/bisnis/bisdoc/011001E-Russia.htm.

- To create incentives for the development of an independent press and media by employing ICT in their professional activities;
- To develop the infrastructure of telecommunication networks, as well as access to electronic libraries, archives, databases of scientific and technical information for citizens, state-owned organizations, and educational institutions;
- To support the establishment of e-commerce for state procurement and other commercial activities of the state.[16]

In 2006, the government of the Russian Federation modified some of the aims and tasks of this program. The main aim of the Electronic Russia program has initially been restricted to increasing the quality of the public administration through implementation of information and telecommunications technology in government bodies, in order to increase the skills of the state employees in their use of IT and the quality of the state's services for citizens. Now Electronic Russia has a four-year planning horizon and addresses mainly e-Government issues.

The main objective of Electronic Russia is to increase the efficiency of management in the public sector by applying information and communication technologies. In order to reach this goal, the following tasks are addressed:

- Formulating standards and proposals related to the use of information and communication technologies in state governance;
- Providing for effective interaction between different bodies through information and communication technologies and integration of the state information systems;
- Providing for effective interaction between the state authorities, citizens, and organizations through information and communication technologies;
- Application of the information systems to control the activities of state authorities;
- Creation of software and technical solutions to support the activities of state authorities;
- Monitoring the program's implementation.

[16] Federal Target Program "Electronic Russia", op. cit., p. 3f.

One of the regional branches of the Electronic Russia Program is the city program Electronic Moscow.[17] This program, announced on 24 December 2002, aims to strengthen Moscow's role as the information industry center of Russia. The program is based on the city's powerful telecommunication infrastructure – the Moscow Fiber Optic Network. The issues addressed by e-Moscow include the creation of a normative and legal basis for the information society; a more efficient city management, based on e-Government; developing the urban economy and overcoming information inequality within the city; building an interoperability framework; and integrating all existing ICT projects of the municipal authorities.[18]

## International Cooperation

International cooperation is an important component of the Russian Federation's efforts in the field of ensuring information security. Russia's international cooperation in ensuring information security has two distinctive features: International competition for technological and information resources and for dominance in the markets has increased, and the world's leading economies have achieved a growing technological lead that allows them to build up their potential for information warfare. Russia views this development with concern, as it could lead to a new arms race in the information sphere and raises the threat of foreign intelligence services penetrating Russia through technical means, such as a global information infrastructure. Therefore, the main areas of the Russian Federation's international cooperation in the field of information security are:[19]

- Banning the development, proliferation, and application of instruments of information warfare;

[17] http://mgd.iis.ru.

[18] Sergey Filippov. "Policy for ICT Adoption in Moscow", "Electronic Moscow" Programme, (no date). http://i-policy.typepad.com/informationpolicy/2004/09/policy_for_ict_.html, and . Yuri Hohlov. Institute of the Information Society. "e-Moscow Program for 2003-2007", State of the Art October 2005. http://www.tedbr.com/apresentacoes/e-Brasil/e-russia_and_e-moscow_programs_2005-10-14.pdf.

[19] http://www.medialaw.ru/e-index.html.

- Ensuring the security of international information exchange, including the security of information being transmitted via national telecommunications channels;
- Coordinating the activities of law-enforcement bodies worldwide for preventing computer crime;
- Preventing unauthorized access to confidential information in international banks, telecommunications networks, and information support systems that are indispensable for maintaining global trade; and sharing information with international law-enforcement organizations fighting transnational organized crime, international terrorism, the spread of narcotics and psychotropic substances, the illegal trade in arms and fissile materials, and human trafficking;
- Active participation of Russia in all international organizations active in the field of information security, including standardization and certification.

In accordance with UN General Assembly Resolution No. 58/32 of 8 December 2003, a group of government experts on international information security was organized, chaired by a Russian representative.[20] The group of government experts includes representatives of 15 countries.[21] Furthermore, the Russian government has special partnerships with the state members of the Shanghai Cooperation Organization (SCO)[22] and with the state members of the Collective Security Treaty Organization (CSTO)[23] in the sphere of information security.

[20] Arkadiy Kremer. "Cyber Security in Russia". Presentation held at ITU-T Cybersecurity Symposium (Florianopolis, Brazil, 4 October 2004). http://www.itu.int/ITU-T/worksem/cybersecurity/presentations/CsecS2-p2-kremer.ppt.

[21] United Kingdom, China, Russia, France, Belarus, Brazil, Germany, India, Jordan, Malaysia, Mali, Mexico, South Korea, and South Africa.

[22] In addition to Russia, these include: China, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan.

[23] In addition to Russia, these include: Armenia, Belarus, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan.

# Organizational Overview

The main organizations responsible for information security in Russia are the Security Council of the Russian Federation, the Federal Security Service of the Russian Federation (FSB), the Federal Guard Service of the Russian Federation, the Federal Technical and Export Control Service, and the Ministry of Information Technologies and Communications.

As far as public-private partnerships are concerned, the Russian Association of Networks and Services (RANS) strives to contribute to the development of norms for the implementation and use of secure IT, while PRIOR, as a national public initiative, aims at uniting public, private, and non-profit organizations directed at developing the Russian Information Society.

## Public Agencies

### Security Council of the Russian Federation

The Security Council of the Russian Federation[24] is appointed by the president in accordance with the constitution and the Federal Law on Security. It is responsible for ascertaining Russia's national interests related to information and defines information resources that must be defended. The Security Council defines conceptual approaches to national security.[25] It drafts policy proposals on defending the vital interests of individuals, society, and the state against internal or external threats. The Security Council also coordinates the elaboration of a strategy for the Russian Federation's information security, and helps the president to carry out his constitutional duties in defending human and civil rights, as well as Russia's sovereignty, independence, and territorial integrity.[26]

[24] http://www.scrf.gov.ru.

[25] http://www.kremlin.ru/eng/articles/institut04.shtml.

[26] http://www.fas.org/irp/world/russia/docs/edict_1024.htm.

## Federal Security Service of the Russian Federation (FSB)

According to its statute, the FSB[27] is a federal agency of the executive branch of government with a mandate to safeguard the security of the Russian Federation. This includes defending and protecting the state borders of the Russian Federation, as well as its internal waterways, territorial waters, exclusive economic zone, and continental shelf and their natural resources, and safeguarding the information security and the main areas of activity of agencies of the Federal Security Service, as defined in the laws of the Russian Federation.[28]

As far as technical support is concerned, the FSB has its own research institute specializing in information technologies. It carries out technical information assessments, particularly regarding criminal cases.[29] It is also responsible for tracking cases of cyber-terrorism.[30] The FSB Computer and Information Security Directorate (Directorate-R) was established in October 1998. The Directorate's main tasks are counterintelligence and the fight against cyber-crime. Since undergoing a minor reform in September 2004, the FSB has a changed structure. The Computer and Information Security Directorate is part of its counterintelligence service.[31]

Among the fundamental objectives of the FSB in the field of information security are the planning and implementation of state and scientific-technical policy in the sphere of information security; the organization of support for the cryptographic and technical engineering security of information and telecommunications systems; and protecting state secrets as well as systems of encrypted, classified, and other special types of communications in the Russian Federation and in its institutions abroad. Another function is to certify equipment for the protection of information, telecommunications systems, and networks, as well as technical devices for the detection of electronic surveillance in buildings and

[27] http://www.fsb.ru.

[28] Text of the "Statute on the Federal Security Service of the Russian Federation and Structure of the Federal Security Service Agencies". Approved by presidential edict no. 960 of 11 August 2003, signed by V. Putin, President of Russian Federation. http://www.fas.org/irp/world/russia/fsb/statute.html.

[29] Ibid.

[30] http://www.russia-gateway.ru/content/NEWS/NewsItem_2376921.jsp.

[31] http://www.agentura.ru/english/dosie/fsb/structure; http://www.agentura.ru/english/press/about/jointprojects/mn/fsbreform.

technical equipment, in accordance with federal law. Moreover, it certifies special technical equipment for the covert collection of information and technical equipment to safeguard the security and (or) protection of information, and defines the basic guidelines of the activity of the agencies of the Federal Security Service in these areas. Finally, it regulates the development, production, sale, use, export, and import of encryption (cryptographic) equipment, telecommunications systems, and networks protected by encryption systems.[32]

## Federal Guard Service of the Russian Federation

According to its statute, the Federal Guard Service of the Russian Federation is a federal body of the executive branch of government with a public mandate to shape state politics and legal regulations, as well as to conduct monitoring and surveillance to ensure the safety of the president of the Russian Federation, the chairman of the government of the Russian Federation, and other important public figures. An additional structure – the Special Communication and Information Service – was added in August 2004 as a result of the administration reform of the Federal Guard Service of the Russian Federation.[33]

Until 2004, the Federal Agency for Government Communications and Information (FAPSI)[34] was the main responsible body for information security. FAPSI was abolished in 2003 and its functions distributed between the Federal Security Service (FSB) and the Federal Guard Service of the Russian Federation. FAPSI was responsible for ensuring the security of communications;[35] the cryptographic and technical security of encrypted communications; intelligence-gathering activities; and providing information to higher bodies of authority. The agency also fought domestic criminals, foreign intelligence services, and engaged in other forms of information warfare; and it monitored informa-

[32] "Statute on the Federal Security Service of the Russian Federation", op. cit.

[33] Decree of the President of the Russian Federation No. 1013 of 7 August 2004. "Issues of the Federal Guard Service of the Russian Federation" (with Amendments and Additions of 28 December 2004, 22 March and 1/6 October 2005). http://egarant.park.ru/rubric.jsp?urn=2622189142 (registration required).

[34] http://www.agentura.ru/english/dosie/brit/fapsi.

[35] http://www.shaneland.co.uk/ewar/docs/dissertationsources/russiansource1.pdf.

tion security in the financial sector. FAPSI was a strategic asset and oversaw information security on this level for the Russian Federation. It developed the technological basis not only for the country's administrative system, but also for the command-and-control system of the armed forces.[36]

## Federal Technical and Export Control Service

The Federal Technical and Export Control Service was formed in August 2004.[37] The Federal Technical and Export Control Service's activities are guided by the president of the Russian Federation and come under the jurisdiction of the Ministry of Defense. The Federal Technical and Export Control Service is an executive body dealing with the following issues:

- Ensuring information security in ICT systems that are important for the state's and society's security;
- Countering foreign technical espionage on the territory of the Russian Federation;
- Ensuring the protection of the state's classified information and other data by restricting access and preventing technical leaks and unauthorized access;
- Export control.

## Ministry of Information Technologies and Communications

The Ministry of Information Technologies and Communications is a branch of the federal government that implements state policy and oversight in the telecommunications sector. Among many other tasks, the ministry, together with other parts of the federal government, takes measures aimed at the restoration of the information and communication networks of the Russian Federation in emergency situations. It develops and implements a scientific-technical strategy

[36] http://www.fas.org/irp/world/russia/fapsi/index.html.

[37] "Edict no. 314" of the president of the Russian Federation of 9 March 2004 on the System and Structure of Federal Executive Bodies.

for information security. The ministry also coordinates efforts to develop the national IT infrastructure.[38]

## Public-Private Partnerships

For many years, information security problems in Russia were only studied and addressed in a timely fashion for the protection of state secrets in military, governmental, or other state-related automated systems. Thus, over time, a situation developed in which very specific commercial-sector problems went unresolved because of the absence of such a sector.[39] At present, the development of commercial IT security products in the Russian market is prospering, yet it is sometimes limited by financial restrictions and the shortage of IT specialists.

Genuine public-private co-operation in the field of information security remains rather limited when compared to efforts in other countries. This is a result of the fact that for many (especially small and medium-sized) businesses in Russia, information assurance is not the most pressing problem. But both sides – private and public – are currently changing their stance, making more cooperation a much likelier prospect.[40]

### Russian Association of Networks and Services (RANS)

The Russian Association of Networks and Services (RANS)[41] is a public and governmental organization. RANS is developing norms and legal documents for the implementation and use of secure IT. The establishment of RANS was initiated by the Ministry for Information Technologies and Communications of the Russian Federation in 1994. At present, RANS has 122 members from all over Russia including universities, scientific institutions, ministries, legal and insurance companies, operators, ISPs, vendors, and users. RANS has several committees and workgroups on main topics covering the internet, security and

[38] http://english.minsvyaz.ru/site.shtml?id=17&page=1.

[39] Mikhail B. Ignatyev, op. cit.

[40] http://www.iis.ru/projects. Information provided by an expert.

[41] http://www.rans.ru/eng.

privacy, wireless communications, education and training, and IP telephony. One of its working groups monitors standards.

The main activities of RANS are:[42]

- Assisting the development of the internet in Russia;
- Establishing a predictable, informative, non-contradictory, and clear legal environment for internet activities;
- Creating and realizing projects and programs aimed at the development of networks, systems of data transmission, telematic services, and information safety;
- Integration and coordination of the interests of users, producers, and operators of information and telecommunication systems;
- Integration of Russian information and telecommunication systems into the European and global infrastructure;
- Organization of conferences and exhibitions; publishing activities, and professional development.

In the sphere of information security, the program of RANS covers:[43]

- The creation and development of the PKI and information security concept in Russia;
- The preparation of a draft law on electronic digital signatures;
- The preparation of proposals in co-operation with the Ministry for Internal Affairs for the prevention of illegal activities in the telecommunication networks;
- Creating a hierarchical PKI Infrastructure, managed by the Federal Cryptographic Body.

[42] http://www.rans.ru/eng/directions.

[43] http://www.rans.ru/eng/programs. Other major projects are in the fields of telecommunications, e-business, and education and training.

## PRIOR

PRIOR[44] is a national public initiative that unites public, private, and non-profit organizations. Through its activities, this initiative aims to supplement the existing state and non-governmental programs and projects directed at developing an Information Society and a knowledge economy in Russia. PRIOR recognizes the importance of participating in the major development programs, including those of the state. These include the Federal Program Electronic Russia for the Years 2002–2010, the municipal program Electronic Moscow, the program Electronic Saint Petersburg, and others.

PRIOR's major project is creating the Russia Development Gateway,[45] which is envisioned as an environment for partner interaction and collaboration to reach common goals as well as a means of integrating expert knowledge in the development field. It is an unprecedented coalition of equal partners instead of the traditional Russian hierarchical system.

PRIOR is a volunteer association of organizations and individuals who have pooled their efforts and resources in order to provide mutual informational, technological, consulting, financial, organizational, and other types of support to reach common goals. These goals include e-Governance, e-Business, the networked society, distance learning, digital libraries, and strengthening international, national, and local projects and initiatives through effective dissemination of best practice knowledge and experience.

Among others, PRIOR's aims are:[46]

- To assist in developing the legal base of the Information Society, the infrastructure of information processing, and communications channels;
- To serve as an effective national system for applying innovations;
- To educate and train qualified knowledge workers;
- To provide relevant local information content and services;
- To establish a unified methodological and terminological base regarding the Information Society and the knowledge economy;

[44] http://prior.russia-gateway.ru/en.

[45] Ibid.

[46] Ibid.

- To give Russian users access to best-practice solutions and know-how and to assist in the implementation of partnership-based programs and projects aimed at development through ICT.

## Early Warning and Public Outreach

The Russian Information Security Doctrine mentions the development of some early-warning mechanisms: "In these specific conditions, information security is ensured, among other things, by developing an effective system of monitoring critical objects whose malfunction may give rise to emergency situations and prediction of emergency situations".[47]

### Russian Computer Emergency Response Team (RU-CERT)

The Russian Computer Emergency Response Team (RU-CERT)[48] was founded in 1998 and is maintained by the Russian Institute for Public Networks (RIPN).[49] RU-CERT is part of the RBNet Network Operation Center (NOC).[50] RBNet was established to provide internet services for science and high school communities in Russia. RBNet is a project funded by the Russian government under the responsibility of the RIPN.

RU-CERT provides computer-incident prevention and response services for RBNET users. The initial goal of the RU-CERT project was the coordination of efforts in the Greater Moscow area in their fight against hackers, primarily "script kiddies" who used stolen dial-up passwords and caused considerable material damage. However, it quickly became clear that service providers prefer to solve all problems independently and hide the results of their anti-hacker efforts from

[47] "Doctrine of the Information Security of the Russian Federation", op. cit.
[48] http://www.cert.ru/index_eng.html.
[49] http://www.ripn.net:8080/en/index.html.
[50] http://www.rbnet.ru/en/about_en.shtml.

the public. It was subsequently decided to change the scope of its activity and to create an organization like the US CERT for Russia.

### Governmental Scientific Support

One of the important factors determining the state outreach policy in the field of the ensuring information security is scientific support. The coordination of the activities of Russian scientific organizations in this field has been entrusted on the Institute Information Security Issues (IISI)[51] of the Moscow State University and the Academy of Cryptography of the Russian Federation (which deals with technical aspects of such problems).

## Law and Legislation

The legal framework for information security in Russia includes three main parts: the legal insurance of information security, the legal insurance of the security of information infrastructure and the legal insurance of the legal status of the information security's subjects.

The legal framework for information security is based on the Law of the Russian Federation on Mass Media, the Federal Law on Advertising, the Federal Law on Countering Extremist Activity, the Federal Law on Political Parties, the Code of Administrative Offences of the Russian Federation. It is also governed by a number of other legal acts[52] such as the Law of the Russian Federation On State Secrets,[53] the Basic Principles of the Legislation of the Russian Federation on the Archive Fund of the Russian Federation and Archives,[54] and the Federal Laws On Information, Informatization and Information Protection,[55] which focus mainly on the use of information resources, information access rights, and information protection in the sense of preventing unauthorized access to docu-

[51] http://www.iisi.msu.ru/GeneralEng.html.

[52] Information provided by tan expert.

[53] http://www.medialaw.ru/laws/russian_laws/txt/8.htm.

[54] http://www.rusarchives.ru/lows/zakon.shtml.

[55] http://medialaw.ru/e_pages/laws/project/d2-4.htm.

mented information that may cause damage to government bodies or any other holder of information resources. Moreover, the Law of the Russian Federation on Legal Protection of Computer Programs and Databases[56] protects the content of computer programs and databases.

The legal framework for the security of information infrastructure is based on the Federal Law on Communications,[57] which also covers communication network management in emergencies.[58] A number of other laws[59] have been adopted, and work has begun on implementing them and preparing draft laws regulating social relations in the information sphere.[60] The government hopes that the new federal Electronic Digital Signature (EDS) Law[61] will serve as a tool for regulating the field of information security. The law provides for recognizing the EDS as being legally equivalent to a physical personal signature. Specifically, the EDS Law protects the rights of persons who use EDS in their electronic data exchange. As part of enforcing this law, the government has been working to put into place a network of EDS authentication centers that will help enforce the law and derive regulations. The new Russian Law on Technical Regulation[62] also offers a new definition of the concept of security.[63] It states that "security is a condition in which intolerable risk of harm is absent". Furthermore, Article 7 of this law states that "technical regulations taking into account the degree of risk of harm establish minimum necessary requirements for ensuring, among others, electrical security."[64]

The legal provision on the status of the subjects of information security is based on the Constitution of the Russian Federation, the Criminal Code of the

[56] http://www.russoft.org/docs/?doc=131.

[57] http://www.medialaw.ru/e_pages/laws/russian/comm_eng/comm_1.html.

[58] Federal Law on Communications, Chapter 10, Articles 65–67.

[59] Further information: http://www.fas.org/irp/world/russia/docs/arf_p2.htm.

[60] http://www.medialaw.ru/e-index.html.

[61] http://www.bakernet.com/NR/rdonlyres/996F168D-3FED-4EDB-B725-4E5E42B03E2F/28188/RussianElectronicDigitalSignatureLaw.pdf; and: http://www.akdi.ru/gd/proekt/086086GD.SHTM.

[62] http://www.cababstractsplus.org/google/abstract.asp?AcNo=20043101434, and: http://www.aprok.ru/tecreg/chronicle.php.

[63] http://books.nap.edu/openbook.php?record_id=10968&page=107.

[64] Interestingly, before 2003, documents issued by Russian state organizations on information security did not include the word "risk".

Russian Federation, the Law of the Russian Federation on Mass Media, and other legal acts that consolidate norms ensuring the rights of citizens, organizations, and state bodies in their information-related activities.

## Russian Criminal Code 1996/2004

The number of cyber-attacks against enterprises, organizations, and citizens is growing at a stable pace. According to information from the Main Administration for Special Technical Measures of the Russian Ministry of Internal Affairs, the number of computer-related crimes committed in Russia has increased by almost 150 per cent over the previous years.[65]

The Russian Criminal Code of 1996 (revised in 2004) provides for the punishment of the following crimes related to breaches of computer security:[66] Unlawful access to lawfully protected computer information; development of computer programs or introduction of changes into existing computer programs that are known to lead to unsanctioned destruction, blocking, modification, or copying of information; disruption of the operation of the computer, the computer system, or its networks, and likewise the use or dissemination of such programs or discs containing such programs; and violation of the rules of use of a computer, computer system, or network by a person having access to this computer, computer system, or network.

The Criminal Code of the Russian Federation now includes articles establishing penalties for types of crimes that had not been defined previously. Chapter 28 of the code, Crimes in the Computer Information Sphere, consists of three articles outlining the penalties for unlawful access to computer information (Article 272); for the creation, use, and dissemination of malicious computer programs (Article 273); and for violations of rules for the operation of computers, computer systems, and networks (Article 274).[67]

[65] http://www.mvdinform.ru/; Source: http://www.nap.edu/catalog.php?record_id=10968.

[66] Further information: http://www.crime-research.org/analytics/Liability_for_computer_crime_in_Russia.

[67] http://books.nap.edu/openbook.php?isbn=0309089719&page=102.

# Singapore

## Critical Sectors

New security threats that have emerged in the post-11 September 2001 era emphasized the need for closer cooperation between the military and homefront agencies in Singapore. Immediately after the attacks in the US in 2001, the homefront agencies undertook a review of the vulnerabilities and strengths of Singapore's national critical infrastructures from the following sectors:

- Banking and Finance,
- Information- and Telecommunications,
- Energy,
- Water,
- Transportation,
- Health.[1]

[*] The Country Survey of Singapore 2006 was reviewed by the relevant officers from the Ministry of Home Affairs. For this edition, the authors have thoroughly updated the Singapore country survey by referring to open-source material.

[1] Speech by Senior Minister Of State For Law and Home Affairs Ho Peng Kee at the Monoc Seminar, Ministry of Home Affairs, 22 March 2002. http://app3.mha.gov.sg/news_details.aspx?nid=876.

Since 2002, the critical infrastructures of these six sectors have been reviewed and assessed, and remedial plans were implemented. However, infrastructure protection policies in Singapore are not limited to these sectors, but have been expanded to the following sectors:

- Food supply,
- Aviation Security,
- Maritime Security.[2]

Even though these sectors have been at the focus of the most recent efforts to prevent terrorism, they do not represent the totality of Singapore's critical infrastructure. Other sectors may well be included in future protection efforts.

## Initiatives and Policy

Singapore adopted the internet comparatively early. According to the Network Readiness Index by the World Economic Forum, Singapore was the most network-ready country in 2004–2005.[3] In spring 2005, the Singaporean government presented a comprehensive "Infocomm Security Masterplan" for the years 2005–2007 that is part of the country's national security strategy to address cyber-security and cyber-terrorism.[4]

[2] Cf. National Security Coordination Centre. "The Fight Against Terror – Singapore's National Security Strategy", pp. 47–51. http://app-stg.nscc.gov.sg/data/25fight-terror.pdf.

[3] Valerie D. Costa "Singapore's Internet Policy. Workshop on Internet Governance at the National Level", 19 July 2005. http://www.wgig.org/docs/Singapore%20Internet%20Policy%2019%20Jul%2005.ppt.

[4] Ministry of Information, Communication, and the Arts. "Keynote address by Minister for Information, Communications, and the Arts Lee Boon Yang at the 17th Annual FIRST Conference". http://www.mica.gov.sg/pressroom/press_050629.html.

## National Emergency System (NEST)

Since the mid-1980s, Singapore has planned and developed its homefront preparedness efforts along the lines of a total defense concept. The Ministry of Home Affairs (MHA) has brought various ministries and emergency authorities together to integrate homeland preparedness plans. Since 2001, the MHA has boosted its efforts and developed a robust National Emergency System (NEST) for national security, while the Singapore Armed Forces are in charge of external defense. NEST is a comprehensive system encompassing civil security, civil defense, the provision of essential services, and the smooth operation of the economy during an emergency. It also ensures the provision of essential services and commodities such as water, power, health services, telecommunications, food, and fuel to the public.[5]

## National Critical Infrastructures Assurance (NCIA) Program

As announced in 2002,[6] the Singapore government has set up a National Critical Infrastructure Assurance (NCIA) project to carry out an in-depth assessment of the vulnerabilities of the nation's critical national infrastructures and of necessary measures to reduce these vulnerabilities. The project involves consultation and partnership between the government agencies and the private sector. The National Infocomm Security Committee (NISC) supports the NCIA program.

[5] Speech by Minister Ho Peng Kee, op. cit.

[6] Asia-Pacific Conference on Cybercrime and Information Security (Seoul, 11–13 November 2002). "Country Report on Singapore", p. 15. http://www.unescap.org/icstd/cybercrime%20meeting/Presentations/Session%203%20-%20country%20and%20org.%20reports/Singapore/Singapore%20written%20report.doc.

## The Fight Against Terror – Singapore's National Security Strategy

In August 2004, the government's National Security Coordination Centre released a document entitled The Fight Against Terror – Singapore's National Security Strategy,[7] according to which security standards in crucial areas such as aviation security, maritime security, land transport security, border control, and critical infrastructure protection have been raised in Singapore.[8] In response to terrorist attacks in the US and based on the recommendations of the National Critical Infrastructure Assurance Committee, Singapore has initiated several measures to protect its physical critical infrastructure and key installations, including prominent public places, power stations, and transportation and water supply networks.[9]

## Infocomm Security Masterplan

In response to cyber-threats such as hacking, virus attacks, and cyber-terrorism, the deputy prime minister announced the three-year Infocomm Security Masterplan (2005–2008) in February 2005. He said that as Singapore's economy would continue to rely heavily on ICT, securing the information and communication environment would be critical. The government would thus set aside S$38 million (about US$23 million) over the next three years to build capabilities in managing cyber-threats and enhancing the security of cyberspace.

The master plan was developed through a multi-agency effort led by the Infocomm Development Authority of Singapore (IDA) under the guidance of the National Infocomm Security Committee (NISC), and is the result of extensive private and public collaboration. Companies and government agencies

[7] The Fight Against Terror, op. cit.

[8] Ibid., p. 12.

[9] Arabinda Acharya. "Defending Singapore's Vital Infrastructure Against Terrorism, IDSS Commentaries". http://se1.isn.ch/serviceengine/FileContent?serviceID=PublishingHouse&fileid=1A3BA5E1-F1AA-226F-7CEC-C0096894A6ED&lng=en.

provided feedback and input through surveys and focus group discussions.[10] It was discovered that businesses have difficulty formulating and complying with IT security policies and best practices, as they lack the necessary professionals and experience.

The Infocomm Security Masterplan has two main aims:

- To maintain a secure IT environment for the government, businesses, and individuals. This involves raising awareness of risks, cyber-threats, and appropriate security measures among internet users and businesses. Two planned key projects to secure these three sectors are the National Authentication Infrastructure, which will develop reliable and robust authentication means to curb identity theft and promote more secure e-services, and the Business Continuity Readiness Assessment Framework. They will measure the effectiveness of government agencies' business continuity plans;
- To defend Singapore's critical infrastructure from cyber-attacks. The master plan also outlines strategies to develop national capabilities, to enhance security technology research and development, and to improve the resilience of critical information infrastructure.

Finally, a Common Criteria Certification Scheme and a set of international standards on security are planned.[11]

The Infocomm Security Masterplan 2005–2008 will be replaced by a new five-year master plan in 2008. The new plan will build on existing efforts and will perpetuate the collaborative approach to ensure information security in Singapore.[12]

[10] Peter Ho. "Singapore's Strategy in Securing Cyberspace", Keynote Address at the Infocomm Security Seminar 2005. http://www.ida.gov.sg/News%20and%20Events/20050717164621.aspx?getPagetype=21.

[11] IDA press release. "Singapore Gears Up for Cyber Security. Three-year Infocomm Security Masterplan Unveiled", 22 February 2005. http://www.ida.gov.sg/News%20and%20Events/20050712110643.aspx?getPagetype=20.

[12] http://www.ida.gov.sg/News%20and%20Events/20050717164621.aspx.

# Organizational Overview

The Infocomm Development Authority of Singapore (IDA) is the chief technology office of the Singapore government covering planning, policy formulation, regulation, and cooperation with the private sector in the field of ICT. The National Infocomm Security Committee (NISC) and the Technology Crime Division (TCD) within the Singapore Police Forces also play important roles in the field of CIIP.

In addition, the government of Singapore has recognized the importance of public-private partnerships to secure critical information infrastructures. In his speech on the occasion on the launch of the Infocomm Security Masterplan, Peter Ho, the then chairman of the National Infocomm Security Committee, emphasized the need for collaboration: "The cyber-threat landscape is constantly changing. No single organization can deal with these changes alone. Instead, collaboration among infrastructure owners, operators and government must take place. This is because separately, each of us sees only a small part of the picture and may not comprehend the full scale of malicious activities involved."[13]

Accordingly, Singapore has implemented different initiatives to foster public-private collaboration in the field of information security. The second part of this section lists the most important among them with regard to the protection of critical information infrastructure.

## Public Agencies

### Infocomm Development Authority of Singapore (IDA)

IDA is a statutory board of the Singapore government that was formed in 1999 as the result of a merger between the National Computer Board (NCB) and the Telecommunications Authority of Singapore (TAS). The aim was to have a single agency for integrated planning, policy formulation, regulation, and in-

[13] Peter Ho. "Singapore's Strategy in Securing Cyberspace", op. cit.

dustry development of the ICT sector.[14] IDA operates under the Ministry of Information, Communications, and the Arts (MICA).

Among IDA's main responsibilities are fostering a competitive IT industry in Singapore, preparing residents for living and working in the "New Economy", supporting the delivery of citizen-centric e-Government services, and building and operating the government's IT infrastructure.[15] IDA sets ICT standards and regulations and supports the private sector in implementing security measures.

IDA's Infocomm Security Division (iSec) plays a central role in establishing and implementing a solid IT security infrastructure for Singapore's national ICT infrastructures. iSec monitors the implementation of ICT security measures and practices for the whole public sector. Moreover, iSec conducts awareness-raising programs for the public and the private sector as well as individuals. For instance, in 2001, IDA initiated a yearlong public-awareness campaign that aimed to educate users from the public and private sectors as well as the general public about safe computing practices.[16]

## National Infocomm Security Committee (NISC)

The National Infocomm Security Committee (NISC) was set up to formulate policies and strategic direction for cybersecurity at the national level. With members from various government agencies, it is a platform for the government to institutionalize considered policies and mandate strategic initiatives in IT security. It comprises representatives from the Ministry of Home Affairs, the Ministry of Defence; the Ministry of Information, Communication and the Arts; the Ministry of Finance; the DSO National Labs; and the Defence Science and Technology Agency (DSTA). IDA serves as the secretariat for this committee.[17]

[14] Among other entities, IDA supports the Information Technology Standards Committee (ITSC), the National Trusts Council (NTC) – an industry-led council to build confidence in e-Commerce –, and the Public Key Infrastructure (PKI) Forum Singapore.

[15] http://www.ida.gov.sg/About%20us/20060406102431.aspx.

[16] Asia-Pacific Conference on Cybercrime and Information Security, op. cit.

[17] Cf.: IDA. "Singapore Gears Up for Cyber Security", op. cit.

### Technology Crime Division (TCD) within the Singapore Police Force

Within the Singapore Police Force (SPF), the Criminal Investigation Department (CID) is the primary investigation agency in Singapore for all criminal matters.[18] The Technology Crime Division (TCD) is part of the CID. TCD provides specialized investigative and forensic services in addition to training the entire police force in investigating high-tech crime. Its scope of operation goes beyond computer crime and includes traditional crimes committed with the use of technology, such as encrypted mobile devices, the internet, and even wireless platforms. In order to prepare the nation for crimes of the future, the approach adopted by TCD is also to build capabilities through research, alliance-building, and education.[19]

## Public Private Partnership

### Critical Infocomm Infrastructure Surety Assessment (CII-SA)

The Critical Infocomm Infrastructure Surety Assessment project was established in 2006 to assess the security readiness of Singapore's critical information and communications infrastructure. The project is led by the IDA, and provides a platform for owners and operators of CII to work together and ascertain the adequacy of their protection measures.[20]

### Information Technology Standards Committee (ITSC)

Volunteer members from the industry, supported by the Productivity and Standards Board (PSB) and IDA, established the industry-led Information Technology

[18] http://www.spf.gov.sg.

[19] Clement Leong. "Security Initiatives in the Computerisation of the Singapore Government". http://www.gsa.gov/gsa/cm_attachments/GSA_DOCUMENT/13-Homeland-Security-Singapore_R2GVIV_0Z5RDZ-i34K-pR.htm.

[20] iGov.Sg. "2006 Report on Singapore e-Government", p.22. http://www.igov.gov.sg/NR/rdonlyres/0D5EE595-4D44-4B02-948C-07FB18239313/0/2006ReportonSporeeGov.pdf.

Standards Committee (ITSC)[21] in 1990. It is a neutral platform for interested industry and government parties to convene to agree on technical standards. To this end, the ITSC organizes workshops and seminars on various topics.

### Governmentware Seminar

The annual Governmentware IT Security seminar series began in 1991. The seminars are organized by the IT Command of the Internal Security Department (ISD) of the Ministry of Home Affairs (MHA). Since 2002, the Institute of Public Administration and Management (IPAM) of the Civil Service College has been the MHA's organizing partner. The lectures are also open to an audience from outside the public sector. The first seminar, organized by ISD for civil service participants, was held in the wake of urgent concerns about virus attacks against the PCs of government users. The Governmentware seminars alert participants to the latest security threats posed by emerging technology and advanced hacking techniques. Private-sector IT security industry experts are invited to participate and share their knowledge.[22]

## Early-Warning Approaches

### Singapore Computer Emergency Response Team (SingCERT)

The Singapore Computer Emergency Response Team (SingCERT)[23] is responsible for the detection, resolution, and prevention of security-related incidents on the internet. SingCERT also issues advisories and alerts about incidents. It maintains a website and a hotline for reporting and dissemination of advisories. SingCERT was initially established in October 1997 as a program of IDA, in

[21] http://www.itsc.org.sg.

[22] http://www.governmentware07.com/home.htm.

[23] http://www.singcert.org.sg.

collaboration with the Centre for Internet Research at the National University of Singapore (NUS).

SingCERT provides the following services:

- Broadcasting alerts, advisories, and security patches;
- Promoting security awareness through security courses, seminars, and workshops;
- Collaborate with vendors or other CERTs to find solutions to security incidents.

SingCERT is also a founding member of the Asia Pacific Security Incident Response Coordination Working Group (APSIRC-WG). The APSIRC-WG is staffed by volunteers from the national Incident Response Teams (IRTs) of Japan, Korea, and Singapore and aims to promote collaboration with other international IRTs and security groupings, such as the Forum of Incident Response and Security Teams (FIRST). Furthermore, APSIRC-WG provides assistance to countries in the region that would like to establish their own IRTs.[24]

## National Cyberthreat Monitoring Centre (NCMC)

Under the Infocomm Security Masterplan, the National Cyberthreat Monitoring Centre (NCMC)  as a national resource to safeguard Singapore's cybersecurity and to provide focused tracking of cyber-threats. Besides the round-the-clock monitoring of critical networks, the centre will provide regular in-depth analysis of cyber-threats by incorporating information from all available sources. The NCMC will provide latest trends in cyber-threats, allowing the authorities to better respond to, and even pre-empt future attacks.[25]

[24] Ibid.

[25] Ministry of Information, Communication, and the Arts. "Keynote address by Minister for Information, Communications, and the Arts Lee Boon Yang", op. cit.

# Law and Legislative Action

## Computer Misuse Act 1993/1998

The Computer Misuse Act (CMA) was first enacted in 1993 and first amended in 1998. It is aimed at protecting computers, computer programs, and information stored in computers from unauthorized access, modification, use, or interception. The CMA also applies to any person, irrespective of physical location, who hacks into computers located in Singapore, and to any person in Singapore who hacks into computers outside Singapore.

The 1998 amendments also address newer forms of cyber-crime (such as Trojan horses, password trafficking, or denial-of-service attacks). The amended CMA also provides enhanced penalties for computer crimes proportionate to the potential and actual harm caused. The amendment gives the police the legal authority to gain access to computer material, including encrypted material.[26]

## Computer Misuse (Amendment) Act 2003

The amendment to the Computer Misuse Act in 2003 allows the minister to authorize  any person or organization to take necessary measures to prevent or counter any threat to a computer system that can affect the national security, essential services, defense, or foreign relations of Singapore. This is part of the government's efforts to establish a robust defense against cyber-attacks.

As in many other countries, Singapore's essential and critical services such as water, electricity, gas, telecommunications, and transportation are increasingly dependent on computer networks and information systems. Terrorists and criminals can exploit this dependence. Any attack on the critical infrastructure and essential services will severely disrupt the economy and threaten the national security.

Furthermore, with an increasingly computer-literate population and widespread availability of user-friendly hacker tools, more people around the world

[26] http://www2.mha.gov.sg/mha/ibrowse.jsp?type=3&root=0&parent=0&cat=8.

now have the necessary skills to carry out cyber-attacks. Hackers and computer viruses can flood network connections, steal or tamper with information, and disrupt essential services.

Section 15A of the Computer Misuse Act allows the minister to authorize any person or organization to take necessary measures to prevent or counter any threat that may endanger the national security, essential services, defense, or foreign relations of Singapore. The new Section 15A would be invoked to deal with situations of an outright cyber-attack, or in cases where specific intelligence has been received of an imminent cyber-attack against Singapore's critical infrastructure.

The powers given to the minister under Section 15A may not be used indiscriminately. The measures are aimed at preventing or countering any threat to a computer or computer service, or to any class of computers or computer services. The powers would be invoked only to avert threats that may endanger national security and essential services, such as any service directly related to the communications infrastructure, the banking and finance sectors, and the defense and foreign relations of Singapore. The powers under the new Section 15A would not be invoked to prevent or investigate a criminal offence that does not threaten the national security or essential services. Singapore's security agencies will also be required to satisfy the minister that the cyber-threats are imminent before the powers provided by Section 15A can be invoked.[27]

## Electronic Transactions Act 1998

The Electronic Transactions Act (ETA) was enacted in 1998 to provide a legal infrastructure for electronic signatures and electronic records, and to ensure predictability and certainty for electronic contracts. The ETA establishes the supporting legal infrastructure for the Public Key Infrastructure (PKI). The ETA addresses the following issues:

- Commercial code for electronic commerce transactions;

[27] http://www.mha.gov.sg/basic_content.aspx?pageid=52.

- Use of electronic applications and licenses for the public sector;
- Liability of service providers;
- Provision for a PKI.

# Spain

## Critical Sectors

For a long time, Spain's critical sectors had not been exhaustively defined by the Spanish government. On 7 May 2007, the State Security Secretariat approved the so-called National Plan for the Protection of the Critical Infrastructures (Plan Nacional de Protección de las Infraestructuras Críticas). This plan defines the critical infrastructures as "those installations, networks, services, physical equipment, and information technologies whose interruption or destruction would have a grave impact on the health, security, or economic wellbeing of the citizens or on the efficient functioning of the state institutions and of the public administration".[1] Moreover, the plan includes a list of 12 strategically critical sectors. These are:[2]

- Chemical Industry,
- Nuclear Industry,
- Investigative installations,
- Centers of Power,

[*] The Country Survey of Spain was reviewed by the Directorate of the Centre for the Protection of National Infrastructure (CNPIC).

[1] Information provided by an expert. Translation by the author.

[2] Information provided by an expert.

- Space,
- Energy sector,
- Telecommunications,
- Transportation,
- Water supply,
- Alimentation,
- Financial Sector,
- Public Health.

On 12 June 2007, Congress in a plenary session unanimously urged the government to put together a catalog with an exhaustive list of the national critical infrastructures within six months.[3] This classified catalog was elaborated and now contains 3,500 critical installations all over Spain.[4] Moreover, the catalogue is designated to become the basis of information for the European Program for Critical Infrastructure Protection (EPCIP) and will be constantly updated.

The Department of the Interior's General Directorate for Infrastructures and Security Equipment (Dirección General de Infraestructuras y Material de la Seguridad) is tasked, among other responsibilities, with securing the information and communications systems and data systems.[5]

## Past and Present Initiatives and Policy

The main Spanish initiatives and policies in the area of information infrastructure and security occur along a two-pronged strand and focus on the opportunities

[3] Invertia.com. "El Congreso insta al Gobierno a concluir en seis meses el catálogo de infraestructuras críticas", (12 July 2007). http://www.invertia.com/noticias/noticia.asp?subclasid=&clasid=&idNoticia=1764166.

[4] http://www.publico.es/012947/gobierno/crea/centro/protegera/infraestructuras/criticas/24/horas/dia.

[5] http://www.mir.es/MIR/estrorganica/estructura/subsec/dgas1.html.

and positive challenges created by the current developments in information and communications technologies.

## Information Society Action Plan

In 1999, the Spanish government launched a strategic initiative for the development of the Information Society corresponding to the insight that Spanish society and the country's economy as a whole would benefit from the capacity to adopt the Information Society's technological innovations and to exploit the opportunities thus created.

The very first step of this initiative was the adoption of INFO XXI: La Sociedad de la Inform@ción para todos[6] in January 2000, a project that aims at building the Information Society of Spain. It consists of several structured programs and action steps to help stimulate the development of the Information Society in Spain. The first Action Plan INFO XXI (2000–2003) intends to establish the coordination of public administration initiatives by achieving three major objectives:[7]

- To stimulate the telecommunications and information technologies sector and complete the liberalization process within this sector by fostering competition;
- To enhance e-Government;
- To foster inclusive access to the Information Society.

In July 2003, the successor plan for the further development of the Information Society, called España.es, was adopted by the Spanish government to replace the INFO XXI plan. Covering the two-year period of 2004–2005, it is partly based on the recommendations of an expert commission on the Information Society and pursues two main objectives: to stimulate Information Society services in

[6] This document is accessible in its entirety. http://www.fulp.ulpgc.es/documentacion/temp/texto_infoxxi.pdf.

[7] http://www.fulp.ulpgc.es/index.php?pagina=investigadores&ver=infoxxi.

the population and to improve the infrastructure, contents, and services. The three strategic axes of the new action plan are as follows[8]:

- To foster the availability of contents and services that are most likely to stimulate demand;
- To improve the accessibility of Information Society services in the broadest sense, by offering public access points and developing training and communication;
- To connect small and medium-sized enterprises to enable them to fully take advantage of the benefits of e-Business.

To deliver on these objectives, the plan comprises six areas of action divided into two categories: vertical actions targeting specific segments of society such as the public sector (administración.es), education (educación.es), or small and medium-sized enterprises (pyme.es), and horizontal actions covering the whole population, accessibility and inclusion (navega.es), contents (contenidos.es), and communication and marketing (comunicación.es).[9]

In November 2005, the Spanish cabinet adopted the latest successor plan, the so-called Plan Avanza, which forms part of a broader program, Ingenido2010. The latter is aimed at giving new impetus to research and development investment in Spain. Plan Avanza focuses in particular on the investments needed for the ongoing development of the Information Society.[10] Plan Avanza has three major domains of activity including digital citizenship, small and medium-sized enterprises, and local entities. The element of information and communications security within all three domains is the jointly maintained anti-virus early-warning center (Centro de Alerta Temprana sobre Virus y Seguridad Informática).[11]

[8] http://ec.europa.eu/idabc/jsps/documents/dsp_showPrinterDocument.jsp?docID=1483&lg=en.

[9] http://www.gemeinsamlernen.de/euconet/Projects/Spanien/espana?language=en.

[10] http://ec.europa.eu/idabc/en/document/5578/343.

[11] http://www.planavanza.es/Canales/CiudadaniaDigital/Todos/CATA.htm?rGuid={B838B40E-72D5-4AED-A8E2-768EE989A730}, and: http://alerta-antivirus.red.es/portada.

## E-Government Action Plan

Jointly launched in 2003 by the Ministries of Science and Technology and of Public Administration, the Spanish e-Government action plan initially had the objective to enhance the drive towards electronic public services with a "short sharp shock". Therefore, a bunch of measures was implemented organized around the following four strategic areas: [12]

- Facilitating access to electronic services for all citizens (with the introduction of the electronic ID card, and the development of public access points to the internet);
- Developing interactive and transactional services that meet users' needs in terms of need, accessibility, and sophistication (starting with the improvement of the central e-government portal administracion.es);
- Enabling data and information interchange between administrations, both at the central level and with regional and local administrations;
- Supporting the internal change and re-engineering efforts of public administrations (coordination of developments, technical assistance, and reorganization of supporting structures).

In October 2004, this plan was updated to become the Public Administration Technological Modernization Plan 2004–2007 aiming to "connect administrations and connect people" while reducing bureaucracy, simplifying procedures, and eliminating unjustified delays.[13] Therefore, an electronic system for the secure interchange of data between administrations was to be put in place. In January 2006, the national e-Government initiatives were once again updated to boost the transition of the country's national public administration into cyberspace by offering a full range of on-line services to Spanish citizens. A new new key element of the latest plan, called MODERNIZA, is a wide-ranging law on e-Government (see the chapter on Law and Legislation). MODERNIZA covers the period from 2006 to 2008 and consists of 16 measures to be implemented

[12] http://ec.europa.eu/idabc/en/document/1065/343.

[13] http://ec.europa.eu/idabc/en/document/3316/343.

with the aim of achieving a huge step towards e-Government in Spain. The new law, for example, establishes citizens' electronic access to all public administration services and their right to submit electronic documents and signatures for official purposes. Other measures in the action plan repeated earlier calls for the distribution of electronic ID cards, the online availability of 800 new administrative forms, the conversion of 100 services to cyberspace, and a progressive introduction of electronic payment of public fees and royalties. The government is also creating an integrated network of information points and a single one-stop-shop web portal service for citizens to replace more than 500 different websites.

## Organizational Overview

The various aspects of Spanish critical information infrastructure policies mainly come under the auspices of the Ministry of Industry, Tourism, and Trade; the Ministry for Public Administration; and the Ministry of the Interior.

There are two State Secretariats under the administration of the Spanish Ministry of Industry, Tourism, and Trade: the State Secretariat of Tourism and Trade and the State Secretariat of Telecommunications and for the Information Society. The State Secretariat of Telecommunications and for the Information Society, in turn, is in charge of two General Directorates – the General Directorate of Telecommunications and Information Technologies (Dirección General de Telecomunicaciones y Tecnología de la Información – DGTTI) and the General Directorate for the Development of the Information Society (Dirección General para el Desarrollo de la Sociedad de la Información – DGDSI).[14]

Three initiatives under the auspices of the Ministry for Public Administration are particularly important as regards Spain's information and communication infrastructure and its security. These are the e-Government Council, its Technical Committee, and the so-called technimap project.

[14] http://www.mityc.es/es-ES/Ministerio/Estructura.

The Police Services and the National Center for the Protection of the Critical Infrastructure operate under the auspices of the Ministry of the Interior.

The two main public-private partnership initiatives include the Information Society and Telecommunications Analysis Center, called Enter, and the Spanish Electronics, Information Technology, and Telecommunications Industries Association, AETIC.

## Public Agencies

### General Directorate for the Development of the Information Society

The General Directorate for the Development of the Information Society was created by Royal Decree 1554 of 25 June 2004. Article 9 of this decree defines a set of 20 functions and jurisdictions for the general directorate, distributed among the following Sub-Directorates: [15]

- Sub-Directorate for access to the information society;
- Sub-Directorate for companies of the Information Society;
- Sub-Directorate for the services of the Information Society;
- Sub-Directorate for audiovisual tools.

The DGDSI maintains multiple services[16] ranging from Plan Avanza over the provision of ICT technologies to small and medium-sized companies, universities, and the public, to the extension of broadband access and a program for the promotion of technical research. Other departments address a variety of international cooperation programs, e-Government, a range of Information Society services, and information security. The latter comes under the jurisdiction of the Antivirus Early Warning Center (Centro de Alerta Temprana sobre Virus y Seguridad Informática – CATA).[17]

[15] http://www.mityc.es/DGDSI/Organizacion/FuncionesyCompetencias.
[16] http://www.mityc.es/DGDSI/Secciones/PorServicio.
[17] http://www.mityc.es/DGDSI/Secciones/PorUnidadTematica.

## General Directorate of Telecommunications and Information Technologies

The General Directorate for Telecommunications and Information Technologies is in charge of six Sub-Directorates and is organized into 11 sections.[18] It offers manifold services,[19] electronic forms,[20] and access to legislation relating to telecommunications.[21] Most importantly, several so-called advisory councils and commissions are organized and convened by the DGTTI, including the following three bodies in particular. First, the Advisory Council of Telecommunications and of the Information Society is composed by delegated members of the different administrative units including the national government the autonomous administrations, and the local administrative authorities. Furthermore, representatives of the industrial and commercial sectors, of the telecommunications services providers, of the sectoral trade organizations, and delegates of the educational sector make up this advisory body. The main function of the Advisory Council is to study, deliberate, and advise the government on an informed basis concerning matters of IT policy.[22]

Second, the Special Study Commission for the Development of the Information Society has the task of analyzing the consequences of implementing the Information Society for both small and medium-sized companies and for Spanish society in general. It is tasked with issuing written recommendations. It is composed of eminent members who are acknowledged experts in their respective professional fields, both technological and academic.

The third and most wide-ranging council is the Interministerial Commission of the Information Society and of the New Technologies in Spain, which was created with the objective of elaborating, developing, and evaluating the government's strategic initiatives relating to the Information Society and information technology. More precisely, the commission's tasks include:

[18] http://www.mityc.es/telecomunicaciones.

[19] http://www.mityc.es/es-ES/Servicios/OficinaVirtual/Procedimientos/SETSI.

[20] http://www.mityc.es/Telecomunicaciones/Servicios/AdmFormularios.

[21] http://www.mityc.es/Telecomunicaciones/Servicios/Legislacion.

[22] http://www.mityc.es/Telecomunicaciones/Organizacion/Consejos/ConsejoTeleco.htm.

- To collate a catalog of all activities undertaken by the various ministerial departments and other public entities regarding the Information Society;
- To elaborate and propose to the government a strategic initiative for the development of the Information Society, including objectives, priorities, and an agenda for implementation;
- To evaluate the tools considered for use in the strategic initiative, and to submit an annual report to the Council of Ministers;
- To propose guidelines to the government on the position to be adopted by Spain in the most relevant international forums and bodies in this field;
- To promote the diffusion of the strategic initiative and its tools within Spanish society.

The commission is to carry out its functions through specialized working groups. It is chaired by the minister of science and technology, and its secretary is the general director for the development of the Information Society. The list of the participating members is composed by representatives of 15 different ministerial secretariats.[23]

## Red.es

Besides the two General Directorates described above, the State Secretariat of Telecommunications and for the Information Society manages two public entities – the red.es office and the Telecommunications Market Commission – as well as an autonomous organism, the State Agency for Radiocommunications.[24] On the same organizational level as the two General Directorates, the red.es office aims to promote the development of the Information Society through the execution of the programs defined in Plan Avanza; to analyze efforts pertaining to the Information Society by means of the Spanish Telecommunications and Information Society Observatory; to offer advice and specific support to the

[23] http://www.mityc.es/Telecomunicaciones/Organizacion/Consejos/ComisionInterministerial.htm.

[24] http://www.mityc.es/es-ES/Ministerio/Estructura/SecretariaEstadoTelecomunicaciones/Organigrama.

national government; and it is responsible for handling registrations of domain names under the country-code top level domain .es for Spain.[25]

The various programs of red.es aim to promote digital inclusion and ameliorate the quality of services, to enhance the digitalization of the educational sector through the allocation of ICT infrastructures, to support the provision of digitalized public services both for citizens and for companies, to enhance broadband infrastructures, and to raise awareness of security mechanisms that generate confidence in ICT and digital content. The Observatory of red.es analyses the activities of the ICT sector and pursues the development of Plan Avanza for convergence among the autonomous regions and of Spain with Europe. The red.es office advises the Spanish government by submitting studies and reports to the various administrative bodies and by assisting the implementation of e-Government.[26]

## The e-Government Council

Among the bodies of the Ministry for Public Administration is the e-Government Council (Consejo Superiór de Administración Electrónica). In 2005, it replaced the Council for Informatics and for the Promotion of e-Government, which had replaced the first incarnation of this body – the Council for Informatics – two years before. The task of this council is to prepare, elaborate, develop, and apply the government's IT policies and strategies.[27] It has seven main areas of activities, including statistical services, the promotion of telecommunications in the administration, the enhancement of the quality and productivity of the services, international activities, IT cooperation between the different levels of the administration, organization, and human resources.

Moreover, the council is assigned with the task of elaborating a security policy in collaboration with the National Cryptology Center of the National Intelligence Center for the development of information and communication security measures and systems security.[28] Under this header, it has developed

[25] http://www.red.es/sobre_red/index.html.

[26] http://www.red.es/actividades/index.html.

[27] http://www.csi.map.es/csi/nuevo/csae_1.htm.

[28] http://www.csi.map.es/csi/nuevo/pg4000_4.htm.

tools for ICT security; issued publications on security criteria, standardization, and conservation of information and communications;[29] and published documentation on methodology for risk analysis and management[30] in information systems – the latest version of which dates from June 2006. The council operates as a plenum, has a permanent commission that is responsible for coordinating the technical support supplied by various bodies under the jurisdiction of different ministries, and its activities are sub-divided into ministerial commissions (Comisiones Ministeriales de Administración Electrónica).

## Technical Committee for the Security of Information Systems and Personal Data Processing

The Technical Committee for the Security of Information Systems and Personal Data Processing (Comité Técnico de Seguridad de los Sistemas de Información y Tratamiento Automatizado de Datos Personales – SSITAD)[31] is responsible for cyber-security and for supporting the e-Government Council's task of elaborating a Spanish information security policy. The main task of this committee is to unify activities related to information systems security among all government departments. In order to achieve this objective, the SSITAD defines common information security policies and procedures, provides advice and training, and fosters general awareness. It also works on the adoption of international and European regulations in information systems security.[32] The committee exercises its functions in plenary sessions and also in four ad-hoc working groups. These are responsible, respectively, for personal data protection, the elaboration of directives for information systems security, the evaluation and certification of information systems security, and the use of electronic, information, and telematics technology in the government.[33]

[29] http://www.csi.map.es/csi/pg5c10.htm.

[30] http://www.csi.map.es/csi/pg5m20.htm (also in English).

[31] http://www.csi.map.es/csi/nuevo/csae_7.htm.

[32] IST-2000-29202 Information Society Technologies. "National Dependability Policy Environments SPAIN", (1 November 2002).

[33] http://www.csi.map.es/csi/nuevo/csae_7.htm.

## TECNIMAP

Tecnimap[34] is a conference that brings together ICT experts from various areas of the public administration, the main companies in the field, and other experts. It aims at creating a space to exchange experiences, ideas, and projects in the field of information technologies and public services. The first conference was held in 1989 (Madrid). The 2007 conference, the tenth one, was organized in association with the Ministry of Public Services, the Government of the Principality of Asturias, and the Gijón City Council, and was held from 27 to 30 November. Over 5,000 participants, 250 enterprises, and representatives of 100 media outlets attended the event. Round tables and workshops were held for four days, during which interesting subjects relating to new technologies and e-administration were discussed.

The 2007 conference also included an opportunity to observe the latest projects developed by the public administration, and a forum was held at which citizens presented their opinions and suggestions. This conference discussed legal issues related to public access to the public administration using IT and other emerging issues.

## The Police Services

Under the auspices of the Ministry of the Interior, both the Policía Nacional and the Guardia Civil deal with cyber-crime. The national police operates through the Information Technology Crime Unit (Unidad de Investigación de la Delincuencia en Tecnología de la Información), and the Guardia Civil hosts a High Technology Crime Department (Departamento de Delitos en Alta Tecnología). The National Police Department and the General Judicial Police Department have an emergency service for cyber-crime. This citizen/police contact service allows the police to act rapidly and efficiently to prevent cyber-crime. The 24-hour alert system is active in the areas of cyber-crime, child pornography and telecommunications fraud.[35]

[34] http://www.tecnimap.es/Tecnimap.

[35] IST-2000-29202 Information Society Technologies. "National Dependability Policy Environments SPAIN", (1 November 2002).

## National Center for the Protection of the Critical Infrastructures

An organization that is more generally concerned with the protection of critical infrastructures is the National Center for the Protection of the Critical Infrastructures (Centro Nacional de Protección de Infraestructuras Críticas – CNPIC), which was established on 2 November 2007 under the responsibility of the State Security Secretariat of the Ministry of the Interior.[36] This agency is responsible for leading, coordinating, and supervising the protection of the national critical infrastructures. The Ministry of the Interior had previously elaborated the antiterrorism prevention and protection plan as well as the national plan for the protection of the critical infrastructures, and had forged the agreement by the Ministerial Council of 2 November 2007 that established the CNPIC. Moreover, the State Security Secretariat is also responsible for the application of the National Plan for the Protection of the Critical Infrastructures, for the coordination of Spain's policies with the requirements of the EU, and for the elaboration of consistent best practice procedures. More specifically, the tasks of CNPIC include:[37]

- The maintenance and updating of the national security plan for the critical infrastructures and of the catalog;
- The collection, analysis, integration, and evaluation of the information furnished by the public institutions, police services, and strategic sectors;
- Threat assessment and risks analysis concerning strategic installations;
- The design and establishment of information, communication, and alert mechanisms;
- Coordination with the respective programs of the EU.

[36] http://www.la-moncloa.es/ActualidadHome/021107-enlacecriticas.htm?FRAMELESS=true.

[37] Information provided by an expert.

## Public-Private Partnerships

### The Information Society and Telecommunications Analysis Center/ENTER

The Information Society and Telecommunications Analysis Center (Centro de Análisis de la Sociedad de la Información y las Telecomunicaciones) called ENTER is a public-private partnership designated as a center for providing information and analysis on the Information Society from the perspective of digital conversion. It brings together private companies and public institutions.[38] ENTER is structured into four functional units of analysis, including a technology section, an economic section, a societal section, and a regulations section. These four units supply data to a shared knowledge management system. Moreover, ENTER disseminates knowledge on the Information Society, which it holds in a database[39] and in an extensive collection of documents.[40]

### AETIC

The Spanish Electronics, Information Technology and Telecommunications Industries Association (Asociación de Empresas de Electrónica, Tecnologías de la Información y Telecomunicaciones de España, AETIC) is a non-profit organization representing Spanish companies from the electronic, IT, and telecommunications sectors. AETIC collaborates with various arms of the public administration, including with the Presidential Office, the Ministry of Industry, Tourism, and Commerce, and with the Ministry of Public Administrations.[41] This collaboration between AETIC and the public administrations is mainly guided by the desire to protect the general interests of the industries that AETIC represents to the government at all levels.[42]

[38] For a list of its members see: http://www.enter.es/que_es_enter/quienes_somos/enter_3_1.html.

[39] http://www.enter.es/buscador/enterdata_bbdd.html.

[40] http://www.enter.es/buscador/enterknowledge.html.

[41] For a full list of the ministries that AETIC collaborates with, see: http://www.aetic.es/VerLibre.aspx?id=118&idcontenidos=143&Idioma=es.

[42] http://www.aetic.es/CLI_AETIC/INFO%20Introduction%20AETIC.ppt.

# Early Warning and Public Outreach

## Antivirus Early-Warning Center

The Antivirus Early-Warning Center (Centro de Alerta Temprana Antivirus, CATA) became operational in 2001 and is located under auspices of the Ministry of Industry, Tourism, and Trade's Secretariat of Telecommunications and for the Information Society.

It supplies users with current first-hand information about computer viruses, information system vulnerabilities, and identified security loopholes. The center collaborates with numerous public bodies at all levels as well as with ministries, universities, and private entities such as the large internet service providers and the producers of anti-virus programs.[43] The center aims to assure the security of data transmitted by means of electronic devices. Therefore, it provides an information platform for IT experts and users.[44] The services offered by the center are structured into four groups. First, the virus-warning group provides effective virus warnings and background information. Second, CATA issues reports about the emergence of new viruses, and collates statistical reports on electronic traffic between particular Spanish investigation centers and universities searching for virus incidents. Third, users can use a search engine to find information about known viruses within the center's databases, including advice on how to deal with virus incidents. And fourth, CATA provides preventive recommendations, FAQs, a virus encyclopedia, a list of the criteria applied, and a documentation center with all relevant information.[45]

## CERT of the National Cryptology Center

The CERT-CNN (Equipo de Respuesta ante Incidentes de Seguridad Informática de Centro Criptológico Nacional de España) is dedicated to enhancing the level

[43] http://www.mityc.es/DGDSI/Secciones/PorUnidadTematica/SeguridadInformatica/CATA.htm.

[44] http://www.alerta-antivirus.es/acercade/ver_pag.html?tema=A&articulo=1&pagina=0.

[45] http://www.alerta-antivirus.es/acercade/ver_pag.html?tema=A&articulo=2&pagina=0.

of security of the information systems of the public administrations of Spain. Its mission is to warn about and respond to security incidents, and to help the public administrations rapidly and efficiently in the case of emerging security threats that affect their information systems. The CERT-CNN, which resides within the National Intelligence Center, furnishes information services such as warnings about new threats and vulnerabilities, provides investigation reports and conducts awareness-raising campaigns, and offers support and coordination services for incident resolution.[46] CERT-CNN is member of the global Forum for Incident Response and Security Teams (FIRST) (see the survey on FIRST in this volume).

## RedIRIS

In 1988, the National Plan for Research and Development initiated a special program called IRIS for the interconnection of computer resources (Interconexión de los Recursos InformáticoS) of universities and research centers.[47] In 1991, when the first stage was finished, IRIS became what RedIRIS is today: the national academic and research network, which is still funded by the National Plan for Research and Development and was managed from 1994 to 2003 by the Scientific Research Council.[48] Since January 2004, RedIRIS has become a department within Red.es, but has preserved its autonomy. About 250 institutions are connected to RedIRIS today.[49]

## IRIS-CERT

IRIS-CERT is the security service of RedIRIS', and is dedicated to the early detection of security incidents affecting RedIRIS centers, as well as the coordination of incident handling in cooperation with these centers. Proactive measures are constantly being developed, including timely warning about potential emerging problems, technical advice, and training. IRIS-CERT also provides

[46] https://www.ccn-cert.cni.es/index.php?option=com_content&task=view&id=12&Itemid=32.
[47] http://wwwn.mec.es/ciencia/jsp/plantilla.jsp?area=plan_idi&id=2.
[48] http://www.csic.es/index.do.
[49] http://www.rediris.es/rediris/index.en.html#inicio.

incident handling coordination for the rest of the .es domains. IRIS-CERT has been a member of FIRST since 1997 and contributes to CSIRT Coordination in Europe.[50]

## Law and Legislation

### Spanish Penal Code

Three sections of the Spanish penal code in particular apply to cyber-crime. These in include Article 197 On the Discovery and Revealing of Secrets, Articles 248, 264, 256, and 270 On Fraud, and Article 273 On Crimes Involving Corporate Property.[51] No specific cyber-crime laws have been passed yet, but the Ministry of the Interior is preparing a proposal for cyber-crime laws in order to amend several articles of the penal code.

### Law on Citizens' Electronic Access to Public Services

On 20 June 2007, the Spanish Congress adopted[52] a new law on electronic access of citizens to public services (Ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos). This law recognizes the right of citizens to communicate with the public administrations by electronic means and states the obligation of the administrations to guarantee this right. The most notably innovations introduced by the new law are:

- New rights for citizens vis-à-vis the public administrations;
- The creation of the position of a "users' advocate " (Defensor del usario de la administración electrónica)

[50] http://www.rediris.es/cert/servicios/iris-cert/rfc-2350.en.html.

[51] http://www.cybercrimelaw.net/laws/countries/spain.html.

[52] For the full text, see: http://www.map.es/iniciativas/mejora_de_la_administracion_general_del_estado/moderniza/Administracion_Electronica/parrafo/04/document_es/a7%20(121-116)%202007-06-14%20Texto_definitivo_aprobado_Congreso.pdf.

- The obligation of public administrations to implement these regulations by 2009;
- Access to e-Government services is to be ensured from everywhere and at all times.

# Sweden

## Critical Sectors

Sweden does not yet have an official definition of CII or CIIP. However, CIIP can be understood as the protection of essential electronic information services, such as IT systems, electronic communications, and radio and television services. CIIP has not only a technical, but also a human aspect. The following are regarded as critical information infrastructure sectors:[1]

- Air Control Systems,
- Supervisory Control And Data Acquisition (SCADA) systems in use within water, transport, and industry,
- Financial Systems,
- National Command Systems,
- Telecommunication Systems,
- The Internet.

[*] The Country Survey of Sweden 2008 was reviewed by Linda Englund and Jan Lundberg, Swedish Emergency Management Agency (SEMA).

[1] Information provided by the country experts.

- Disruption of any of these systems would have immediate serious consequences for society.

## Past and Present Initiatives and Policies

CIIP issues have been on the political agenda in Sweden for many decades. Measures to increase the robustness and security of critical national infrastructures have been implemented since World War II. The vulnerability problems associated with society's increasing dependence on IT and information infrastructures were identified early on as a matter of national security. In addition, management of IT-related vulnerabilities has been discussed since the early 1970s. The present Swedish CIIP policy is derived from these historical developments and from some more recent initiatives described below. The CIIP area in Sweden is currently in a transformative phase. The functions and responsibilities of governmental agencies are under review.

### Commission on Vulnerability and Security

Following a decision on 23 June 1999, the Swedish government authorized the minister for defense to appoint a special investigator to head a commission of inquiry, with a mandate to analyze and submit proposals for a more integrated approach to civil defense and emergency preparedness planning.[2] The findings and proposals of the Commission on Vulnerability and Security, as presented in May 2001, have been a most important step in the implementation of a new structure for defense and emergency preparedness planning in Sweden.

[2] Ministry of Defence. "Vulnerability and Security in a New Era – A Summary", (A summary of Swedish Government Official Report SOU 2001:41). http://www.sweden.gov.se/sb/d/574/a/25658.

The commission suggested several strategic measures for improving the general stability of critical technical infrastructure.[3] In its final report, the commission also proposed measures specifically designed to enhance information assurance and improve protection against information operations. The commission's view was that the central government must assume responsibility in these areas. At the same time, the commission emphasized that all managers and system owners are responsible for securing their own systems against computer intrusions and other types of IT-related threats. The role of the government should be to support these activities and to provide functions and facilities that exceed the financial capabilities of other sectors in society. In 2005, it submitted its final report to the Swedish government.[4]

## Bill on Swedish Security and Preparedness Policy

In March 2002, the government presented its first bill on Swedish security and preparedness policy. The bill was, to a large extent, based on the findings and proposals of the Commission on Vulnerability and Security.

The bill presented the government's framework for a new planning system to prepare for major societal crises and for activities related to a potential threat of war. Furthermore, the bill gave an account of how the crisis management structure would be strengthened. All of this has implications for the security of critical infrastructures in general, and of critical information infrastructures in particular.[5]

[3] Such as cross-sector activity, security standards, Computer Emergency Response Teams, a coordinating body for IT security, an information security technical support team, an intelligence and analysis unit, research and development, international cooperation, a system for the certification of IT products, and more. Ibid., pp. 41–60.

[4] "SOU 2005:71 Informationssäkerhetspolitik – Organisatoriska konsekvenser". http://www.regeringen.se/sb/d/108/a/49614 and http://www.regeringen.se/sb/d/5101/a/49614 (Swedish).

[5] Information provided by expert of SEMA.

## Information Security Policy proposals by the Committee on Information Assurance

The Swedish government on 11 July 2002 instituted the Committee on Information Assurance in Swedish Society. The committee's brief was to present an assessment of information protection requirements in critical sectors of society, and to make a proposal on organizational matters of the Swedish signals protection service.

After monitoring the implementation of the information assurance measures, the Committee on Information Assurance in Swedish Society has presented its proposal for a national strategy on information assurance[6] and also an organization plan.[7] The committee's proposal was processed by the government by March 2006.

## SEMA action plan for information security

In January 2007, the Swedish Emergency Management Agency (SEMA) was commissioned by the government to prepare a proposal for a plan of action for implementing and administering the nation's strategy for information security. The plan was submitted to the government in April 2008 and consists of 47 proposed measures. The following four areas have been designated as priorities.[8]

- Improved sector-wide and cross-sectoral work is needed for civil information security. All-embracing directives for the field of information security applying to all government agencies should be prepared. At the same time, sector-specific responsibility must be clarified. Furthermore, there must be opportunities to provide practical recommendations to other civil sectors;
- A fundamental security level must be established for information security. Such a basic level is a prerequisite for being able to secure the information assets that have become increasingly fundamental for both trade and industry and the public sector;

[6] "Secure information – proposals on information security policy", (SOU 2005:42).

[7] Organizational consequences (SOU 2005:71).

[8] Information provided by the country experts.

- Society must be able to deal with extensive IT-related disturbances and emergencies. An operative national coordinating function should therefore be established;
- There are competence deficiencies in the field of information security at all levels of society. The rapid development also implies that competence deficiencies on the part of individual users have increasingly greater consequences. For this reason, several proposals are submitted that jointly constitute a broad program to raise competence in the field.

The plan of action proposes measures that address the problems reported in SEMA's annual situational assessment. The proposed measures also take into consideration, among other things, the Commission on Information Security's report Secure Information; the government bill for improved emergency preparedness; and the committee directive for a new agency with responsibility for emergency preparedness and security matters.[9]

## Organizational Overview

Swedish government agencies report to their respective ministries, but are formally subordinated only to collective cabinet decisions. The various agencies and organizations in charge of CIIP are presented below under the heading of the ministry they are affiliated with, including the Ministry of Defense; the Ministry of Industry, Employment and Communication; and the Department of Justice.

The bill on Swedish security and preparedness policy contains a few changes of tasks and responsibilities for the actors within the area of information assurance. The bill relates to other issues beyond CIIP. The Committee on Information Assurance in Swedish Society has evaluated the CIIP work and suggested the changes to be introduced in the bill. The suggested changes are presented in the following chapter in connection with each actor. Importantly, in 2009, SEMA

[9] Information provided by the country experts.

and other agencies will be replaced by a new agency called the Swedish Civil Contingencies Agency (SCCA) that will report to the Ministry of Defense; hence, there will be major changes in the overall CIIP system.

The public-private partnership initiatives in Sweden currently include SEMA's efforts to promote interaction between the public and the private sector, the Industry Security Delegation (NSD), and the Swedish Information Processing Society (DFS).

## Public Agencies

### The Swedish Civil Contingencies Agency (SCCA)

As of 1 January 2009, a new national government agency will be established with an all-encompassing task with regard to civil contingencies, that is to say, its work will cover the whole spectrum of contingencies from everyday road traffic accidents, fires, chemical emergencies, power cuts, and other technical failures to even more serious emergencies such as bomb threats and other hostile attacks, epidemics, natural disasters, and war. The responsibilities of this new agency will include information security. SEMA's current work on CIIP will be expanded, and the new agency will be given the authority to issue binding regulations.

The English designation of this new authority will be the Swedish Civil Contingencies Agency (SCCA), and it is being formed from three existing national government authorities, all of which will be closed down at the end of 2008, namely SEMA, the Swedish Rescue Services Agency (SRSA), and the National Board of Psychological Defence (SPF).

Within the Cabinet Offices, cross-departmental work is being performed on ways to implement the findings of the SEMA action plan and to reform CIIP in Sweden further.[10]

[10] Information provided by the country experts.

## The Swedish Emergency Management Agency (SEMA)

The Swedish Emergency Management Agency (SEMA)[11] is responsible for the co-ordination of national information assurance at the policy level. This includes analyses of the development of society and the interdependency of critical societal functions. The agency further promotes interaction between the public and private sectors and coordinates and initiates research and development in the area of emergency management. It also has overall governmental responsibility for information assurance in Sweden. The Information Assurance and Analysis Department at SEMA manages these tasks. Its main activities include:

- Maintaining an updated overall picture of society's information security in terms of threats, vulnerabilities, protective measures, and risks; once a year, it presents an annual assessment of information assurance in Sweden to the government;
- Hosting various forums in order to develop a common national culture of information assurance. Certain forums are solely intended for the private sector or the public sector, respectively, while there are also combined forums for the public and private sectors;
- Developing public-private partnerships;
- Gathering, analyzing, and disseminating open-source information related to information assurance;
- The development of preventive IT security recommendations (consistent with ISO/IEC 17799) to support the IT security activities of other organizations;
- Initiating research and development in the area of different important societal systems and summarizing the respective risk and vulnerability assessments;
- Managing the Board of Information Assurance;
- Participating as a member in several international forums.

[11] http://www.krisberedskapsmyndigheten.se/defaultEN____224.aspx.

In its guidelines for emergency planning for 2006 and 2007 and in its annual report on information security in Sweden for 2008, SEMA points out that there is much work to be done to raise standards of information security in Sweden to an acceptable level. SEMA also reiterates the importance of protecting the nation's critical infrastructures. Dealing with the risks of technical collapses in electricity, telecom, and IT systems that are vital for society must be given priority, according to SEMA.[12] As far as the critical infrastructure (especially the technical infrastructure) is concerned, actions designed to mitigate the consequences of serious emergencies are given priority over preventive measures with the purpose of increasing robustness.[13]

SEMA recently conducted a case study on the topic of large-scale internet attacks. The study was prompted by the attacks that Estonia was subjected to in 2007. The study aims to analyze how Sweden would handle a similar attack.[14]

## SEMA / Information Assurance Council

The Information Assurance Council was established to support SEMA's activities in the area of information assurance. This council will create a network of skilled experts from a variety of important organizations in the area. The council replaced the earlier Cabinet Office Working Group on Information Operations.[15] The council's primary assignment is to assist the senior management of SEMA by supplying:

- Information about trends in research and development in the area of information assurance;
- Suggestions and viewpoints concerning the direction, prioritizing, and realization of SEMA's activities in the area of information assurance.

[12] Information provided by expert.

[13] Information provided by expert.

[14] SEMA's Educational Series 2008:2. "Large scale Internet attacks. The Internet attack on Estonia. Sweden's emergency preparedness for Internet attacks." http://www.krisberedskapsmyndigheten.se/upload/3040/Large%20scale%20Internet%20attacks_utb-ser_2008-2.pdf.

[15] SEMA document 0160/2003. "Account of Measures Taken in Assuming Responsibilities from the Working Group on Information Operations", (Redovisning av åtgärder för att överta arbetsuppgifter från Ag IO 0160/2003).

### SEMA / Agency Cooperation Forum

The SEMA/Agency Cooperation Forum consists of seven agencies, and the main task of this forum is to secure the information assets of Swedish society in order to obtain a certain level of confidentiality, integrity, and availability. This is done through information exchange and cooperation. The focus areas of this group are:

- Strategy and regulatory framework;
- Technical and standardization issues;
- Information assurance issues at the national and international levels.

## The Swedish Defense Materiel Administration (FMV) and the Certification Body for IT Security (CSEC)

The Swedish Defense Materiel Administration (FMV)[16] is the procurement agency for the armed forces. The FMV has been involved in the area of IT security evaluations since 1989, performing in-house evaluations of equipment intended for use by the armed forces.

In the summer of 2002, the FMV was tasked by the government with establishing a national scheme for the evaluation and certification of IT security products to be used within Swedish governmental organizations. The certification body is now established as an independent entity within the FMV and is known as the Swedish Certification Body for IT Security (CSEC). Its work includes the production of quality manuals, descriptions of responsibility, descriptions of processes for licensing of evaluation laboratories, rules for implementation of certificates, and training of certification staff and evaluation companies.[17]

[16] http://www.fmv.se/default.aspx?id=121.

[17] Ibid.

## FRA/Information Security Technical Support Team

The Information Security Technical Support Team is associated with the Swedish National Defense Radio Establishment (FRA),[18] which is the Swedish signals intelligence organization. It is a civilian agency directly subordinated to the Ministry of Defense. The Information Security Technical Support Team consists of 20 experts in the field of IT security. The team is specifically intended to support:

- National crisis management where IT-security qualifications are required;
- Identification of individuals and organizations involved in IT-related threats against critical systems.

On request, the team supports the Swedish authorities, agencies, and state-owned corporations that are responsible for critical functions in Swedish society with IT-security expertise and services. The customized services consist of penetration tests, forensic computer investigations, source code analysis, audits, risk analyses, etc. The team co-operates on a regular basis with the national and international IT security community.

The changes suggested by the Committee on Information Assurance in Swedish Society concerning FRA are:

- Technical responsibility for coordination in the field of information security;
- Responsibility for signals protection;
- Creation of a group that can support initiatives in national crises with an IT component and in the case of related threats to important public systems.

[18] http://www.fra.se/english.shtml.

## The Swedish Armed Forces

The Swedish Armed Forces[19] must be able to quickly respond to different types of threats and risks. The Swedish parliament has therefore decided to develop the armed forces according to the concept of network-based defense. This places a great demand on the information infrastructure in terms of availability and security. The armed forces are therefore heavily involved in research and development in areas such as IT security and information infrastructures.

The Swedish Military Intelligence and Security Service handles operational IT security in the armed forces during peacetime. In addition, the National Communications Security Group (TSA) offers advice and inspections of cryptographic systems to Swedish defense organizations and industries.[20]

## Center for Asymmetric Threat Studies (CATS)

The National Center for IO / CIP Studies (CIOS) is now broadening its perspective from Information Operations (IO) to include terrorism, e.g., cyber-terrorism. In order to do so, the center's name has been changed to "Center for Asymmetric Threat Studies (CATS)"[21]. CATS is located at the Swedish National Defense College.[22] It conducts research and policy development in the fields of CIIP, IO (Information Operations), PSYOPS (psychological warfare), and CIP. Research at CATS is funded by the Ministry of Defense and the Swedish Emergency Management Agency (SEMA).

## The Swedish Defense Research Agency (FOI)

The Swedish Defense Research Agency (FOI)[23] focuses on research and development in the fields of applied natural sciences and political sciences, such as security policy analysis. At the Division of Defense Analysis, the Critical Infrastructure

[19] http://www2.mil.se/en/.

[20] Information provided by country experts.

[21] http://www.fhs.se/en/Research/Centers-and-Research-Programmes/CATS/.

[22] http://www.fhs.se/en/.

[23] http://www.foi.se/FOI/templates/startpage____96.aspx/.

Studies Unit (CISU) research group is carrying out a long-term research program on CIP sponsored by SEMA, in cooperation with Systems Analysis and IT Security – another FOI department. This department has acquired a deep knowledge of commercial and military IT systems and applications.

## The Swedish National Post and Telecom Agency (PTS)

The Swedish National Post and Telecom Agency (PTS) is a government authority that monitors all issues relating to ICT and postal services. One of its key tasks is to ensure the development of functioning postal and telecom markets. Within the PTS, the Department of Network Security is responsible for security issues concerning ICT.

The Department of Network Security is tasked with monitoring developments related to security issues and with implementing measures to reduce the threats to ICT from sabotage and terrorism. Emergency measures are planned in consultation with the ICT operators, the Swedish armed forces, and other agencies. As an example, critical nodes in the ICT structures are hardened, and all nodes that are crucial for running the ".se" domain autonomously have been installed within Sweden's borders. The Swedish IT Incident Center (see chapter on Early Warning and Public Outreach) is associated with this department.

## The Swedish National Police Board (NPB)

The Swedish National Police Board (NPB)[24] is the central administrative and supervising authority of the police service. The NPB administers the National Criminal Police and the Swedish Security Service. Within the NPB, the IT Crime Squad has expert knowledge in investigating IT crime. This group supports the local Swedish police departments in IT crime investigations, participates in the education of parts of the judicial system, and assembles and communicates information about IT crime. The Internet Reconnaissance Unit is linked to this squad.

[24] http://www.polisen.se/inter/nodeid=10230&pageversion=1.html.

Additionally, the Swedish Security Service (SÄPO) has the fundamental duty of preventing and detecting crimes against the security of the realm. SÄPO is engaged in four main fields: protective security (including personal protection), counter-espionage, counter-terrorism, and protection of the constitution. Whenever IT-related criminal activity touches upon these fields, the Swedish Security Service is involved.

## Public-Private Partnerships

### SEMA's Private Sector Partnership Advisory Council and Board of Information Assurance

SEMA promotes interaction between the public sector and the private sector, and works to ensure that the expertise of non-governmental organizations (NGOs) is taken into account in emergency management.

There are two advisory councils connected to SEMA: the Private Sector Partnership Advisory Council and the Board of Information Assurance.

SEMA has two forums for sharing information between private and public actors in the area of information assurance. The two established forums in the area of Supervisory Control And Data Acquisition (SCADA) and the financial sector. In these forums, the actors share information about threats and vulnerabilities in order to learn from each other. This concept is largely based on the British model for Information Exchange (IE).[25]

### The Industry Security Delegation (NSD)

The Industry Security Delegation (NSD)[26] is part of the Confederation of Swedish Enterprise,[27] whose objective is to increase cooperation between enterprises, organizations, and authorities, and to promote comprehensive views on vulnerability and security issues. The overall goal of this network structure is to enhance security and risk awareness among the general public and in the business sector.

[25] Information provided by an expert.

[26] http://www.svensktnaringsliv.se/nsd/article17105.ece.

[27] Svenskt Näringsliv. http://www.svensktnaringsliv.se/english/?csref=_umk_english.

The NSD arranges courses in information assurance as well as crisis and risk management to help its members improve security.

### The Swedish Information Processing Society (DFS)

The Swedish Information Processing Society (DFS)[28] is an independent organization for IT professionals with 32,000 members. The DFS owns the SBA brand of security products (the abbreviation stands for SårBarhetsAnalys, or "vulnerability assessment" in Swedish), which are focused on risk analysis and information security. SBA is regarded as the de-facto Swedish standard.

## Early Warning and Public Outreach

### PTS/The Swedish IT Incident Centre (SITIC)

In May 2002, the Swedish government tasked the Swedish National Post and Telecom Agency (PTS) with establishing the Swedish IT Incident Centre (SITIC).[29] The center was officially opened on 1 January 2003 and can be considered to be the Swedish government CERT. SITIC supports national activities for protection against IT incidents by:

- Operating a system for information exchange on IT incidents between both public and private organizations and SITIC;
- Rapidly communicating to the public information on new problems that can disrupt IT systems;
- Providing information and advice on preventive measures;
- Compiling and publishing incident statistics as input to the continuing improvements of preventive measures.

[28] http://www.dfs.se (in Swedish).

[29] http://www.sitic.se/in-english.

# Law and Legislation

## The Swedish Penal Code (SFS 1962:700)

The Swedish Penal code, in Chapter 4, Section 9 c, states that any person who, in cases other than those defined in Section 8 and 9, unlawfully obtains access to a recording for automatic data processing or unlawfully alters or erases or inserts such a recording in a register, shall be sentenced for breach of data secrecy to a fine or imprisonment for no more than two years, unless the deed is punishable under the Criminal Code or the 1990 Protection of Trade Secrets Act. A recording in this context includes even information that is being processed by electronic or similar means for use through automatic data processing (Law 1998:206). Attempts and preparations to do so shall be punished as stated in Chapter 23 of the Criminal Code, unless the completed act would have been regarded as a petty crime. A proposal for amendments of the Act of the Penal Code has been presented. According to the draft, denial of service attacks (DoS) will be made a criminal offence.

Other important legal texts in Sweden in this context are the Personal Data Act (SFS 1998:204) and the Electronic Communications Act (SFS 2003:389).

## The Electronic Communications Act (SFS 2003:389)

In its report, the Commission on Vulnerability and Security[30] concluded that there was a need for legislative amendments in order to support the proposals with respect to IT security and protection against information operations. A particular need for legislative amendments is seen in the following areas:

- Statutory and administrative provisions relating to the activities of local authorities and national administrative boards during major crises;
- The possibility of reallocating resources in the health services during major crises;

[30] "Vulnerability and Security in a New Era", op. cit.

- Stricter safety regulations and more effective supervision of the power supply sector.

The government has decided to review the legislation relevant to CIIP and emergency management.

# Switzerland

## Critical Sectors

Since the end of the Cold War, risks and vulnerabilities involving information and communications technologies have become a growing issue in the Swiss debate on security policy. The high density of information and communication technology (ICT) in Switzerland's public and private sectors offers a high potential for vulnerabilities. Critical Infrastructure Protection (CIP) in general and the protection of information infrastructures in particular are therefore of high relevance for Swiss security policy.

In July 2007, the Federal Council approved the First Report to the Federal Council on the Protection of Critical Infrastructures, submitted by an interdepartmental working group under the lead of the Federal Office for Civil Protection (FOCP).[1] This report defines critical infrastructures as "those infrastructures whose disruption, failure, or destruction would have a serious impact on the public health, the environment, the political affairs, the security, and the eco-

[*] The Country Survey of Switzerland 2008 was reviewed by experts from the Federal Office for Civil Protection (FOCP); the Reporting and Analysis Center for Information Assurance (MELANI); and the Federal Office for National Economic Supply (NES).

[1] http://www.news.admin.ch/message/index.html?lang=en&msg-id=13516&print_style=yes.

nomic and social well-being of a population."[2] The report defines the following ten sectors:

- Public Administration,
- Chemical Industry,
- Energy,
- Waste Disposal,
- Financial Services,
- Public Health,
- Information and Communication Technology,
- Water and Food,
- Public Safety, Rescue and Emergency Services,
- Transport.[3]

These ten sectors are further divided into 31 sub-sectors. In May 2008, the working group launched a project to define criteria to identify critical elements and parts of the Swiss infrastructure.

## Past and Present Initiatives and Policies

Since the end of the 1990s, several important steps have been taken in Switzerland to improve the management of CIIP. Strategic exercises and new threats such as the Millennium Bug have highlighted the importance of information assurance. From the beginning, the private sector was involved in the development of policies for information assurance and CIIP.

[2] Federal Office for Civil Protection. "Erster Bericht an den Bundesrat zum Schutz Kritischer Infrastrukturen" (First Report to the Federal Council on Critical Infrastructure Protection), (Berne 2007), p. 7.

[3] Ibid. p. 8.

## Strategic Leadership Exercise

Two strategic exercises were crucial for the development of Swiss protection policies in the field of information security:

- A key experience, and in fact the impetus for many later steps in Switzerland, was the Strategic Leadership Exercise in 1997 (SFU 97).[4] The exercise dealt with the revolution in information technologies and related challenges to modern society, politics, economics, and finance, as well as to other critical sectors.[5] The exercise revealed that Switzerland's CI was facing new threats. For the first time, the idea of developing an early-warning system for threats to information security was raised.
- After a two-year planning process, the Strategic Leadership Training in 2001 conducted the three-day exercise INFORMO 2001. The goals were to review the information assurance process established after 1997 and to train a newly-established Special Task Force on Information Assurance.

## Information Assurance Policy

The first Concept of Information Assurance was elaborated by the Information Society Coordination Group (ISCG) in 2000. It recommended the establishment of a crisis management system of a special task force on "Information Assurance".[6] This strategy of the Swiss Federal Council was accompanied by a large number of parliamentary initiatives and was further developed.

In December 2001, the Swiss Federal Strategy Unit for Information Technology (FSUIT) presented a four-pillar model for information assurance

[4] This exercise was organized by a unit of the Swiss Federal Chancellery called "Strategische Führungsausbildung" (SFU), which is now called "Federal Crisis Management Training" (CMT). The unit is responsible for the periodical training of federal decisionmakers. http://www.bk.admin.ch/org/bk/00351/00423.

[5] Swiss Federal Chancellery. "Strategische Führungsübung 1997 – Kurzdokumentation über die SFU 97", (Berne, 1997), p. 2.

[6] Swiss Federal Strategy Unit for Information Technology. "Vulnerable Information Society – Challenge Information Assurance", (Berne 2002), p. 19.

in Switzerland.[7] Since then, the Swiss CIIP policy has been based on the following four pillars:

- Prevention: Suitable preventive measures must be implemented to limit the number of incidents;
- Early recognition: Dangers and threatening situations have to be recognized as early as possible to provide the necessary defensive measures or to avoid particularly vulnerable technology. The Reporting and Analysis Center for Information Assurance (MELANI) is the main actor in this field.
- Crisis management: The effects of disruptions on society and the state must be kept to a minimum. The major actors in charge for this are the Special Task Force on Information Assurance (SONIA), together with MELANI and the Federal Office for National Economic Supply (NES), which includes the ICT Infrastructure Unit.
- Technical problem solution: The technical causes of the disruption must be identified and corrected. This area is covered by MELANI together with the experts in charge in the private sector.

It is a tenet of Swiss information assurance policy that all four of the above pillars, or principles, must be taken into account to achieve a complete and strong system of CIP/CIIP.

## Risk Analysis: InfoSurance and the Federal Office for National Economic Supply (NES)

The InfoSurance Foundation (see the chapter on Organizational Overview) started its work in 2002 with the initiation of a nation-wide risk analysis covering various sectors and branches such as telecommunications, finance, energy (electricity), emergency and rescue services, transportation and logistics, and health care. The risk analysis focuses on interdependencies of information infrastructures both within and between the various sectors and on potential preventive

[7] Ibid., pp. 23ff.

measures that can be derived from the analysis. Since 2004, the NES has been responsible for working out and reworking the risk analysis in cooperation with the private-sector experts.

## Report on Critical Infrastructure Protection

Based on a first analysis – which was requested by the Control Delegation of the Federal Assembly – on the protection and safety of critical infrastructures in Switzerland, the Federal Council decided in 2005 to launch an interdepartmental CIP project. The FOCP was mandated to establish a working group that includes all relevant federal agencies.[8] It is the goal of the working group to improve the collaboration between all offices involved with CIP and ultimately to establish a national CIP strategy together with the private sector.

In 2007, the FOCP submitted a first report on CIP in Switzerland to the Federal Council.[9] The report was developed in close cooperation with all relevant federal agencies. It represents a first major step towards the elaboration of a national strategy. It establishes a common understanding of the problem in that it clarifies key concepts and identifies the critical infrastructure sectors relevant for Switzerland. It highlights threat scenarios from natural and technical hazards to violent and armed conflicts. It further defines the need for future action in the area of CIP. The appendix lists previous CIP activities and compares policies on international level, and highlights former and ongoing CIP developments of the relevant federal agencies.

The FOCP will submit a follow-up report to the Federal Council in spring 2009 and will elaborate a national CIP strategy by 2011.[10]

[8] Currently the working group comprises 23 offices from all seven federal departments, including the Federal Chancellery. The working group usually meets four times a year. Its work is supported by sub-working groups where the actual CIP projects are conducted (information provided by an expert).

[9] "Erster Bericht an den Bundesrat zum Schutz Kritischer Infrastrukturen", op. cit.

[10] Information provided an expert.

# Organizational Overview

The issue of CIP/CIIP involves agencies from different departments as well as the cantonal and local governments. The first part of this section provides an overview of the most important federal agencies. In the second part, the most important public-private partnerships are listed. Switzerland has a long-standing tradition of public-private collaboration. Historically, this is due to the tradition of part-time service in a strong militia system, both in the military and in politics. Accordingly, there are several important public-private partnerships in the field of CIP and CIIP (those partnerships with an early-warning function are listed in the section on Early Warning and Public Outreach).

## Public Agencies

### Federal Office for Civil Protection (FOCP)

The Federal Office for Civil Protection (FOCP)[11] is part of the Federal Department of Defence, Civil Protection, and Sports (DDPS). It supports the cantons and municipalities – which bear the principal responsibility for civil protection services in the intervention phase – in their efforts in that regard. As the responsible federal agency in the areas of both manmade and natural disasters, the FOCP ensures cooperation between the federation, the cantons, and the municipalities. The legal underpinnings of civil protection, especially the explicit aim of "protecting the population and its vital resources", are of particular relevance to critical infrastructure protection.[12]

In the field of CIP, the FOCP was therefore mandated in 2005 to coordinate the CIP interagency activities. As mentioned above, the FOCP established a working group and issued a first report for the attention of the Federal Council, summarizing the current state of work of the working group. A national CIP strategy will be elaborated by 2011.

[11] http://www.bevoelkerungsschutz.admin.ch/internet/bs/en/home/das_babs.html.

[12] Art. 2, Federal Law of Civil Protection.

## Federal Strategy Unit for Information Technology (FSUIT)

One of the main bodies on CIIP in Switzerland is the Federal Strategy Unit for Information Technology (FSUIT).[13] It is part of the Swiss Federal Department of Finance (FDF). The FSUIT reports to the FDF and is charged with producing instructions, methods, and procedures for the federal administration's information security. It collects data on incidents within the Swiss federal government and is responsible for the Special Task Force on Information Assurance (SONIA) and for the Reporting and Analysis Center (MELANI). The FSUIT itself runs the Swiss Government Computer Emergency Response Team GovCERT.ch (see the chapter on Early Warning and Public Outreach).

## Federal Office of Communications (OFCOM)

The Federal Office of Communications (OFCOM)[14] is the main regulatory body in the field of telecommunications and ICT in Switzerland. The OFCOM studies various aspects of the information revolution. It includes consumer protection and management of the frequency spectrum as well as conformity assessment rules in the telecommunications equipment area. The OFCOM deals with risks affecting the information society, such as the formation of a new two-tier society, information overload, and the resulting inability to analyze problems and make decisions, and new opportunities for the manipulation of information of a technical, political, or economic nature.

## Federal Office for National Economic Supply (NES)

The Federal Office for National Economic Supply (NES),[15] which includes the ICT Infrastructure Unit (see below, in the section on Public-Private Partnerships), reports to the Swiss Federal Department of Economic Affairs. Its main task is to ensure that the Swiss population is able to obtain vital goods and services at

[13] http://www.isb.admin.ch/index.html?lang=en.

[14] http://www.bakom.ch/index.html?lang=en.

[15] http://www.bwl.admin.ch/index.html?lang=en.

all times. The NES provides governmental support when the private sector is unable to resolve supply problems of vital goods and services on its own. However, measures to ensure a steady flow of supplies to the national economy would only be undertaken if the free-market system were seriously disrupted. In the four pillars of the Swiss information assurance policy, the NES plays an important strategic role in the fields of prevention and crisis management.

## Federal Office of Information Technology and Telecommunication (FOITT)

The Swiss Federal Office of Information Technology, Systems, and Telecommunication (FOITT)[16] is part of the Swiss Federal Department of Finance. Its responsibilities include security and emergency preparedness for the federal administration's information systems on an operational level.

## Coordination Unit for Cybercrime Control (CYCO)

Citizens can report suspected internet crimes, including unlawful access to IT systems, spreading of computer viruses, destruction of data, and similar offenses to the Swiss Coordination Unit for Cybercrime Control (CYCO),[17] which is part of the Federal Office of Police (fedpol). The offenses reported are then forwarded to the respective national or foreign prosecution authorities. CYCO also scans the internet for criminal content and is responsible for in-depth analysis of cyber-crime. In addition, CYCO collaborates closely with MELANI.

[16] http://www.efd.admin.ch/org/org/00582/00806/index.html?lang=en.

[17] http://www.cybercrime.ch/index.php?language=en.

## Public-Private Partnerships

### InfoSurance Association

InfoSurance was established as a foundation in 1999 by a number of companies with the support of the Swiss government. Today, it is an association that aims to increase awareness of the information assurance issue and to establish networks of cooperation among various players from both the public and the private sectors. The association aims at creating a closely-linked network that promotes the organizational and structural conditions for recognizing and analyzing Switzerland's growing dependency on information technologies and the associated risks. The target group of InfoSurance consists of SMEs, and the focus lies on prevention.[18]

### Federal Office for National Economic Supply (NES): ICT Infrastructure Unit (ICT-I)

Another important public-private partnership is the NES. It works in close cooperation with the private sector as well as with cantonal and municipal authorities. The federal government has requested that the NES deal with all prolonged disruptions of the information and communications infrastructure affecting the whole of Switzerland (ICT Infrastructure Unit, ICT-I).[19] The NES also conducts sector-specific risk analysis in cooperation with the private-sector experts involved. These analyses were formerly conducted by the InfoSurance association.

### CLUSIS

The non-profit association CLUSIS (Club de la sécurité des systèmes d'information –Suisse)[20] has existed in Switzerland since 1989 and represents about 230 members, including Swiss public administrations, IT suppliers, providers, banks,

[18] http://www.infosurance.ch.

[19] http://www.bwl.admin.ch/themen/00507/00520/index.html?lang=en.

[20] http://www.clusis.ch.

industries, consultants, etc. CLUSIS organizes seminars related to information security practices and technologies, issues whitepapers and publications, and is involved in education. The aim is to provide networking opportunities for their members and to share experiences. CLUSIS mainly covers the French- and Italian-speaking parts of Switzerland.

## Early-Warning Approaches and Public Outreach

In addition to the public-private partnerships listed above, collaboration between government agencies and private companies is also essential for early warning and public outreach.

### The Reporting and Analysis Center for Information Assurance (MELANI)

On 29 October 2003, the government decided to create a center for CIIP that would collect information on the security of the IT infrastructure, especially of the internet. This new center, called the Reporting and Analysis Center for Information Assurance (MELANI),[21] has been operational since October 2004 and is now the core of the Swiss CIIP early-warning system. It plays a role in all four pillars of the Swiss information assurance policy (prevention, early warning, crisis management, and technical problem solution) and is the central office for CIIP in Switzerland. In addition to its own investigations, it depends on close cooperation with the public and private sectors.

It is designed as a cooperative undertaking between the Federal Strategy Unit for Information Technology (FSUIT) and the Federal Office of Police (fedpol). These two partners of MELANI have the following main tasks:[22]

[21] http://www.melani.admin.ch.

[22] Ruedi Rytz and Jürg Römer. "MELANI – An Analysis Centre for the Protection of Critical Infrastructures in the Information Age", Paper for the Workshop on Critical Infrastructure Protection, (September 2003), p. 49.

- The FSUIT is responsible for strategic issues and the management of MELANI. Since 1 April 2008, it has also run the Swiss government's Computer Emergency Response Team (GovCERT.ch). GovCERT.ch is MELANI's technical competence center, and is responsible for dealing with technical incidents, in particular concerning the internet and computer operating systems;
- The fedpol operates the MELANI analysis center and is responsible for collecting, condensing, and presenting operational information from different sources in the public and private sectors.

MELANI offers warnings and advice for the broader public via a website, but also runs a special program for the owners and operators of critical infrastructures. For members of the so-called "closed constituency" MELANI organizes workshops, disseminates detailed warnings, and operates a 24/7 help-desk. The "closed constituency" of MELANI can be described as a dedicated public-private partnership for CIIP.

The cooperation between the involved partners as well as the conceptualization of MELANI as a public-private partnership has proven to be successful. By pooling existing resources, new threats to information security can be confronted effectively and effectively. On 24 January 2007, the Federal Council decided definitely to establish MELANI as a federal office for information assurance.[23]

## Special Task Force on Information Assurance (SONIA)

The Special Task Force on Information Assurance (SONIA)[24] is also directed by the FSUIT. SONIA is a crisis-management organization and constitutes the core element of the third pillar of the Swiss information assurance policy, namely damage limitation. Its main task is to advise the Swiss Federal Council and senior management representatives from the private sector in crisis situations and to act as a link between the public and private sectors. SONIA would be activated

[23] http://www.news.admin.ch/dokumentation/00002/00015/index.html?lang=de&msg-id=10361.

[24] http://www.isb.admin.ch/themen/sicherheit/00152/00176/index.html?lang=en.

after a breakdown in the information and communication infrastructure that resulted in (massive) disruptions in CI. Unlike MELANI, it is not a permanent body, but would only be convened for damage limitation in genuine crises. SONIA is mainly supported by the following organizations:

- The ICT Infrastructure Unit of NES, to raise awareness and to give guidance in threat and risk analysis, and to establish contacts among the experts in charge in the private sector;
- MELANI, as a provider of reliable information about a possible imminent threat and its consequences, and as an information base in case of a crisis.[25]

## Law and Legislation

### Swiss Penal Code

A number of articles in the Swiss Penal Code are of relevance in the context of CIIP:

- Article 143 (unauthorized procurement of data);
- Article 143 bis (unauthorized access to a computing system): This article states that any person who, by means of a data transmission device, gains unauthorized access to a computing system belonging to others that is specially protected against access by the intruder shall be punished by imprisonment or a fine if a complaint is made;[26]
- Article 144 (damage to property): The article states that any person who damages, destroys, or renders unusable any property belonging to others shall be punished by imprisonment or a fine if a complaint is made;[27]

[25] Haefelfinger, Rolph L. "The Swiss Perspective on Critical Infrastructure", Presentation at the PfP Seminar on Critical Infrastructure Protection and Civil Emergency Planning – New Concepts for the 21st Century, (Stockholm, 17–18 November 2003).

[26] Based on the official English translation of the Swiss Penal Code.

[27] Based on the official English translation of the Swiss Penal Code.

- Article 144 bis (damage to data): The article states that any person who alters, deletes, erases, or renders unusable data stored or transferred by electronic or similar means without authorization shall be punished by imprisonment or a fine if a complaint is made;[28]
- Article 147 (fraudulent use of a computer): The article states that any person who, with the intention of unlawfully obtaining financial rewards for himself or another, interferes with an electronic procedure through the unauthorized use of data shall be punished by community service of up to five years or imprisonment.[29]

Switzerland's laws against virus creation and the use of malicious software in general are widely applicable. However, the structure of the Swiss legal system makes prosecution difficult, due to the complexities of different laws (comprising laws on both the federal and cantonal level) and law enforcement procedures.

[28] Based on the official English translation of the Swiss Penal Code.

[29] Based on the official English translation of the Swiss Penal Code.

# United Kingdom

## Critical Sectors

In the United Kingdom, the critical national infrastructure (CNI) comprises those key elements of the national infrastructure that are crucial to the continued delivery of essential services to the UK. Without these key elements, essential services could not be delivered and the UK could suffer serious consequences, including severe economic damage, grave social disruption, or even large-scale loss of life.[1] Many of the critical services that are essential to the well-being of the UK depend on IT and are provided by both the public and private sectors. Nine sectors are considered to deliver "essential services". These are outlined below:

- Communications (Data Communications, Fixed Voice Communications, Mail, Public Information, Wireless Communications),
- Emergency Services (Ambulance, Fire and Rescue, Coastguard, Police),
- Energy (Electricity, Natural Gas, Petroleum),

[*] The Country Survey of the United Kingdom 2008 was reviewed by the Centre for the Protection of National Infrastructures (CPNI).

[1] http://www.cpni.gov.uk/glossary.aspx.

- Finance (Asset Management, Financial Facilities, Investment Banking, Markets, Retail Banking),
- Food (Produce, Import, Process, Distribute, Retail),
- Government and Public Services (Central, Regional, and Local Government; Parliaments and Legislatures; Justice; National Security),
- Public Safety (Chemical, Biological, Radiological, and Nuclear (CBRN) Terrorism; Crowds and Mass Events),
- Health (Health Care, Public Health),
- Transport (Air, Marine, Rail, Road),
- Water (Mains Water, Sewerage).

## Past and Present Initiatives and Policies

The UK government aims to protect the CNI from both two kinds of threats: physical attacks against physical installations and electronic attacks against computers or communications systems.[2] It has therefore developed a National Information Assurance Strategy. Another important field of action is data security. In reaction to a data security incident in 2007, the government has elaborated data security guidelines

### National Information Assurance Strategy

The UK Cabinet Office produces and maintains the National Information Assurance Strategy.[3] This was first produced in 2003 by the Central Sponsor for Information Assurance (CSIA), a unit within the Cabinet Office, and aims to provide ongoing assurance to the government that the risks to information systems and the information they hold are appropriately managed. The CSIA,

[2] http://www.mi5.gov.uk.

[3] Central Sponsor for Information Assurance (CSIA). "A National Information Assurance Strategy", 2007.
http://www.cabinetoffice.gov.uk/csia/national_ia_strategy.aspx.

with partner organizations, coordinates and sponsors work programs to deliver the strategy's recommendations.

Information assurance (IA) is defined as the confidence that information systems will protect the information they carry and will function as they need to, when they need to, and under the control of legitimate users. The CSIA has a lead role in helping governments to improve IA. That involves the following tasks:

- Enabling the government to deliver public services through the appropriate use of information and communications technology (ICT);
- Strengthening the UK's national security by protecting information and information systems at risk of compromise;
- Enhance the UK's economic and social well-being as the government, businesses, and citizens realize the full benefits of ICT.

Most importantly, the strategy recognizes that within an increasingly interdependent and interconnected information infrastructure, the government must concern itself with the confidentiality, availability, and integrity of all information systems.[4]

## Government Data Security

Following a data security incident in November 2007, the prime minister asked the Cabinet Office to review data handling procedures in all government departments. An interim report was presented to parliament on 20 December 2007, and the final report is expected in 2008. The government has already accepted a number of recommendations in the interim report to bring about greater transparency, increased monitoring, improved guidance, and better mandatory training.[5]

A number of other reviews are being conducted across the UK government that will have an effect on data security measures. The Poynter Review[6] is looking into the specific incident of the loss of child benefit data at HM Revenue

[4] Ibid.

[5] Information provided by an expert.

[6] http://www.hm-treasury.gov.uk/independent_reviews/poynter_review/poynter_review_index.cfm.

& Customs (HMRC)[7] and is expected to report in 2008.[8] In October 2007, before the HMRC-incident, the government had already identified the need to do more to protect the data it controls, and the prime minister commissioned the independent Walport/Thomas review on the use of information in both the public and private sectors. The review is expected to report in the first half of 2008. The Burton report, looking at data losses in the Ministry of Defence, is also due to be published in 2008.[9]

## Organizational Overview

In the UK, the main responsibility for CIIP lies with the home secretary.[10] However, a number of other departments play a role in the protection of the various CNI sectors and contribute resources and expertise to the UK CIIP effort. These contributions are coordinated by the Centre for the Protection of the National Infrastructure (CPNI).[11] CPNI was formed on 1 February 2007 from the merger of the National Infrastructure Security Co-ordination Centre (NISCC) and the National Security Advice Centre (NSAC).

CIIP policy is developed and delivered by several government departments and bodies including CPNI, the Central Sponsor for Information Assurance (CSIA), the Civil Contingencies Secretariat (CCS), the Cabinet Office Security Policy Division, the Home Office, and the Government Communications Headquarters (GCHQ).

Responsibility for the provision of advice on physical protection to the CNI is shared between CPNI, the Security Service, and the police. CSIA is in charge of the UK's broader information assurance strategy, which deals with all aspects

[7] Her Majesty's Revenue & Customs (HMRC) is responsible for collecting the bulk of tax revenue and paying tax credits and child benefits. See: http://www.hmrc.gov.uk/. For more information on the incident, see: http://www.infosecurity-magazine.com/news/071121_hmrc_bamford.html.

[8] http://www.hm-treasury.gov.uk/media/E/E/poynter_review171207.pdf.

[9] Information provided by an expert.

[10] http://www.homeoffice.gov.uk.

[11] http://www.cpni.gov.uk.

of the Information Society. The coordination of the government's contingency and emergency response effort (regardless of the cause of the disruption) is the responsibility of the CCS (part of the Cabinet Office).

Furthermore, there are several public-private partnerships in the field of CIIP. The government collaborates closely with the private sector. The CPNI shares information with the owners and operators of CNI in so-called Information Exchanges.

## Public Agencies

### Centre for the Protection of National Infrastructure (CPNI)

Since 1 February 2007, the Centre for the Protection of National Infrastructure (CPNI) has worked to protect the UK's CNI from both physical and electronic attack. CPNI provides integrated (combining information, personnel and physical) security advice to the businesses and organizations that make up the national infrastructure. Through the delivery of this advice, it protects national security by helping to reduce the vulnerability of the national infrastructure to terrorism and other threats.

CPNI advice is targeted primarily at the critical national infrastructure (CNI) – the key elements of the national infrastructure that are crucial to the continued delivery of essential services to the UK. Recommendations are drawn from the expertise, knowledge, and information of the organizations that contribute to its work. CPNI sponsors research and works in partnership with academia, other government agencies, research institutions, and the private sector to develop applications that can reduce vulnerability to terrorist and other attacks and reduce the impact when attacks take place. CPNI also has special access to intelligence and information about terrorism and other threats, and this informs its advice and priorities.

CPNI shares information, such as warnings of specific threats and vulnerabilities, with its CNI partners so that operators can install suitable defenses, and offers periodic assessments of the nature of the threat from electronic attack. This information on vulnerabilities and alerts is disseminated by the Combined

Security Incident Response Team (CSIRTUK)[12] together with GovCertUK (part of GCHQ).[13]

CPNI works with vendors and researchers to co-ordinate the release of vulnerabilities in a controlled way, so that fixes are in place before the software weaknesses are publicly disclosed. This work enhances the understanding of the potential impact of vulnerabilities.

CPNI's advice is provided to national infrastructure organizations in a variety of ways, including:

- Face-to-face advice through teams of sector-based and specialized, highly experienced advisers;
- Training;
- Online information;
- Written advisory products.

CPNI advice is integrated across the physical, personnel, and information security disciplines both in response to user requirements and derived from expert knowledge about how to make the national infrastructure less vulnerable. Its closest relationship, which has been built up over many years, is with those organizations that operate the key elements on which essential services depend.

CPNI discharges its responsibilities through government departments that have overall responsibility for ensuring that appropriate steps are taken to improve protective security within their sectors. They are also in charge of the identification of critical infrastructure within their sectors in consultation with CPNI and sector organizations. The following departments and agencies have responsibility for sectors or sub-sectors of the CNI:

- Cabinet Office (government and public services),
- Communities and local government (emergency services),
- Department for Business, Enterprise and Regulatory Reform (communications, energy),

[12] http://www.cpni.gov.uk/Products/advisories.aspx.

[13] http://www.govcertuk.gov.uk.

- Department for Environment, Food and Rural Affairs (food supply, water),
- Department for Transport (emergency services, transport),
- Department of Health (emergency services, health),
- Food Standards Agency (food safety),
- HM Treasury (finance),
- Home Office (emergency services),
- Maritime and Coastguard Agency (emergency services).

CPNI also works closely with the police. It has a particularly strong partnership with the police National Counter Terrorism Security Office (NaCTSO),[14] which is co-located with CPNI, and the nationwide network of specialist police Counter Terrorism Security Advisers (CTSAs) that they co-ordinate. NaCTSO and the CTSAs support CPNI in the delivery of advice to critical sites within the national infrastructure.

## Civil Contingencies Secretariat (CCS)

The Cabinet Office Civil Contingencies Secretariat (CCS)[15] was established in July 2001 and reports to the prime minister through the prime minister's security adviser. The CCS works in partnership with government departments, the devolved administrations of Scotland and Wales, and key stakeholders to enhance the UK's ability to prepare for, respond to, and recover from emergencies.

The aim of the CCS is to improve the UK's resilience to disruptive challenges by working with others inside and outside government on the anticipation, preparation, prevention, and resolution of threats. Its current objectives are:

- To make sure that the government can continue to function and deliver public services during a crisis. To work with departments and the wider

[14] http://www.nactso.gov.uk.

[15] http://www.ukresilience.info/ccs.aspx, and http://www.cabinetoffice.gov.uk/secretariats/civil_contingencies.aspx.

Cabinet Office to make sure that plans and systems are in place and cover the full range of potential disruption;

- To ensure improved resilience of the government and the public sector, and to support ministers in developing policy;
- To lead horizon-scanning activity to identify and assess potential and imminent disruptions. To build partnerships with other organizations and countries to develop and share best practice in horizon-scanning and knowledge of the UK's critical networks and infrastructure;
- To improve the capability of all levels of government, the wider public sector, and the private and voluntary sectors to prepare for, respond to, and manage potential challenges.

Like all Cabinet Office Secretariats, the CCS supports ministers collectively. In times of national crisis, it supports the Civil Contingencies Committee, which manages and exercises arrangements to handle national crises in the Cabinet Office Briefing Room (COBR) to deliver an integrated government response.

The Emergency Planning College is an integral part of the CCS. It has a key role to play in the development and promulgation of the UK's resilience doctrine, and in the development of cross-organizational communities to deliver it.[16]

## Public-Private Partnerships

### CPNI's Public-Private Partnerships

In addition to the assurance advice that it provides to specific CNI companies, the Centre for the Protection of the National Infrastructure (CPNI) actively promotes information-sharing. Based on the assumption that the sharing of information about the risks facing networks is beneficial to both government and industry, CPNI works with its CNI partners in Information Exchanges. These aim to create a mechanism through which one company can learn from the experiences, mistakes, and successes of another, without fear of exposing company sensitivities to competitors and the media.

[16] Information provided by an expert.

The success of Information Exchanges is based on the personal trust of representatives sharing information in a confidential meeting. In face-to-face meetings, CPNI helps to build a trusted community with a common interest. Each member organization can have a maximum of two representatives. Substitutes are not permitted, as a stranger turning up at a meeting would inhibit the sharing of sensitive information.

Warning Advice and Reporting Points (WARPs) are another way for an organization to share information from which lessons can be abstracted and shared with the CPNI. A WARP is a community-based service where members can receive and share up-to-date advice on information security threats, incidents, and solutions. Currently, there are WARPs for local governments, public services, businesses, and voluntary and international organizations.[17]

## Other Private-Public Partnerships

There is a wide range of private-sector organizations that work with the public sector to promote information assurance. These include:

- The Information Assurance Advisory Council;[18]
- The British Computer Society,
- The Internet Security Forum,
- The National Computing Centre,
- The Internet Watch Foundation,
- The Confederation of British Industry,
- The Institute of Information Security Professionals,
- European Information Society Group,
- Royal United Services Institute,
- Chatham House.[19]

[17] http://www.warp.gov.uk.

[18] http://www.iaac.org.uk.

[19] http://www.chathamhouse.org.uk.

## Early Warning and Public Outreach

### Combined Security Incident Response Team (CSIRTUK)

CPNI runs a Computer Emergency Response Team (CERT) for its partners in the private sector who operate elements of the national infrastructure. This service, which advises on how to manage the response to incidents and produces advisories on security matters, is called the Combined Security Incident Response Team (CSIRTUK). CSIRTUK receives, reviews, and responds to computer security incident reports, providing advisories and related activity for its CNI partners.[20]

An important part of risk management is to learn from the experiences of others, and national infrastructure organizations can contact CSIRTUK about potential security vulnerabilities, incidents, or events, whether they be electronic, physical, or personnel-related. Information received is treated confidentially and, if necessary, particular details that would identify individuals or organizations are removed so the information can be incorporated into generic security advice. In this way, valuable experience can be shared to help others.

By enhancing the traditional CERT role to cover holistic advice – including physical, personnel, and electronic issues – CSIRTUK provides a central point for reporting security incidents and for receiving advice and guidance.

### GovCertUK

The Communications-Electronics Security Group (CESG), the national technical authority for Information Assurance within GCHQ,[21] has the lead responsibility within the government for providing IA advice to public-sector organizations. This role includes providing an emergency response capability to public-sector organizations that may require technical support and advice during periods of electronic attack or other network security incidents. CESG therefore runs the

[20] http://www.cpni.gov.uk/Products/advisories.aspx.

[21] http://www.cesg.gov.uk.

GovCertUK, which assists public-sector organizations in the response to computer security incidents and provides advice to reduce exposure to threat.[22]

Together, CSIRTUK and GovCertUK have replaced the Unified Incident Reporting and Alert Scheme (UNIRAS), which has been the UK government CERT in the past.

## Ministry of Defence Computer Emergency Response Team

The UK Ministry of Defence Computer Emergency Response Team (MODCERT) is responsible for information security within the Ministry of Defence. It is a member organization of both the international Forum of Incident Response Security Teams (FIRST, see the chapter on FIRST in this volume) and the Trusted Introducer (TI)[23] scheme, both of which provide a mechanism for sharing information on computer security incidents among the communities concerned. MODCERT[24] consists of a central co-ordination center and a number of monitoring and reporting centers, Warning, Advice, and Reporting Points (WARPs), and incident response teams. It also works closely with GovCertUK and CSIRTUK.

## GetSafeOnline

GetSafeOnline, designed to educate the public about IT security, is the result of collaboration between the government and private-sector companies. The website has been available since October 2005 and offers comprehensive advice on safe internet use for home users and for micro-businesses about how to protect computers, mobile phones, and other devices against electronic attack. The aim of this free service is to reduce occurrences of ID theft, viruses, and

[22] http://www.govcertuk.gov.uk/index.shtml.

[23] http://www.ti.terena.nl.

[24] http://www.mod.uk/DefenceInternet/AboutDefence/WhatWeDo/SecurityandIntelligence/CERT.

spam by educating internet users and helping them to protect themselves and their computers from online threats.[25]

## Law and Legislation

The UK has created a legal framework to protect information systems. This includes a number of pieces of legislation. These are outlined below.

- Telecommunications (Fraud) Act 1997: This act amends the Telecommunications Act 1984 to make further provision for the prevention of fraud in connection with the use of a telecommunication system;
- Data Protection Act 1998: This act regulates the processing of information relating to individuals, including the obtaining, holding, use, or disclosure of such information;
- Electronic Communications Bill 2000: This Bill makes provision to facilitate the use of electronic communications and electronic data storage. It also makes provision for the modification of licenses granted under Section 7 of the Telecommunications Act 1984; and for connected purposes;
- Terrorism Act 2000: This act relates to terrorism. It makes temporary provision for Northern Ireland about the prosecution and punishment of certain offences, the preservation of peace, and the maintenance of order. It also makes the deliberate interference with or disruption of electronic systems a criminal act;
- Police and Justice Act 2006: This act makes provision for a range of items relating to policing, crime, and disorder. It also amends the Computer Misuse Act 1990.

[25] http://www.getsafeonline.org.

# United States

## Critical Sectors

In the US, critical infrastructures are defined according to the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, section 1016(e): "[…] the term 'critical infrastructure' means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[1]

Based on this definition, Homeland Security Presidential Directive 7 (HSPD-7), issued on December 2003, identified 17 critical infrastructures and key resources (CI / KR) and delineated the roles and responsibilities for the protection of these sectors. The most recent policy plan (the National Infrastructure Protection Plan,

[*] The Country Survey of the United States 2008 was reviewed by Scott C. Algeier, Executive Director IT-ISAC.

[1] http://www.epic.org/privacy/terrorism/hr3162.html.

issued in 2006)[2] and the current strategy for Homeland Security (issued in 2007)[3] both reconfirm the HSPD-7 list of 17 critical sectors and the corresponding assignment of responsibilities. However, the list of critical infrastructures and key resources is not meant to be final and conclusive – HSPD-7 states that the Department of Homeland Security (DHS) "shall [...] evaluate the need for and coordinate the coverage of additional critical infrastructure and key resources categories over time, as appropriate".[4] In March 2008, the DHS announced the establishment of the critical manufacturing sector as the 18th CI/KR sector. While further changes and additions are still possible, the following sectors are currently defined as critical infrastructures and key resources:

- Information Technology,
- Telecommunications,
- Chemicals,
- Commercial Facilities,
- Dams,
- Commercial Nuclear Reactors, Materials, and Waste,
- Government Facilities,
- Transportation Systems (including Mass Transit, Aviation, Maritime, Ground/Surface, and Rail and Pipeline Systems),
- Emergency Services,
- Postal and Shipping Services,
- Agriculture and Food,
- Public Health and Healthcare,
- Drinking Water and Waste Water Treatment Systems,

[2] Department of Homeland Security. "National Infrastructure Protection Plan", Washington, 2006, p. 3.
http://cipp.gmu.edu/archive/NIPP_Plan6-06.pdf.

[3] The White House. "National Strategy for Homeland Security", Washington, 2007, p. 27.
http://www.whitehouse.gov/infocus/homeland/nshs/NSHS.pdf.

[4] The White House. "Homeland Security Presidential Directive/HSPD-7", Washington, 17 December 2003, Section 15. http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html.

- Energy, including the Production Refining, Storage, and Distribution of Oil and Gas, and Electric Power (except for commercial nuclear power facilities),
- Banking and Finance,
- National Monuments and Icons,
- Defense Industrial Base,
- Critical Manufacturing.

## Past and Present Initiatives and Policies

There have been several efforts since the 1990s to manage Critical Infrastructure Protection (CIP) and Critical Information Infrastructure Protection (CIIP) better in the US, and CIIP still plays an important role in the overall US security strategy. The 2007 Strategy for Homeland Security highlights the importance of CIIP for the nation's safety and security: "Many of the Nation's essential and emergency services, as well as our critical infrastructure, rely on the uninterrupted use of the Internet and the communications systems, data, monitoring, and control systems that comprise our cyber infrastructure. A cyber attack could be debilitating to our highly interdependent CI/KR and ultimately to our economy and national security."[5]

Whereas traditionally, national security has been recognized as the responsibility of the federal government and is underpinned by the collective efforts of the military, the foreign policy establishment, and the intelligence community with respect to defense, homeland security in general – and CIIP in particular – is viewed as a shared responsibility that requires coordinated action across many sectors.[6] In consequence, a multitude of actors is involved with CIIP. In order to ensure coordination among all relevant stakeholders, the US government has developed various initiatives and policies.

[5] "National Strategy for Homeland Security", op. cit. p.28.

[6] Ibid. p. 4f.

## Presidential Commission on Critical Infrastructure Protection (PCCIP)

Based on the recommendations of the Critical Infrastructure Working Group (CIWG), President Bill Clinton set up the Presidential Commission on Critical Infrastructure Protection (PCCIP) in 1996, the first national effort to address the vulnerabilities of the information age.

The PCCIP included representatives from all relevant government departments as well as from the private sector. The PCCIP presented its report to the president in October 1997.[7] The commission's most important decision was to foster cooperation and communication between the private sector and the government. The commission no longer exists, as its functions have been reallocated per HSPD-7.

## Presidential Decision Directives (PDD) 62 and 63

Clinton followed the recommendations of the PCCIP and issued Presidential Decision Directives (PDD) 62 and 63 in May 1998.[8] Those directives established policy-making and oversight bodies making use of existing government agency authorities and expertise. PDD-63 set up groups within the federal government to develop and implement plans to protect government-operated infrastructure, and called for a dialog between the government and the private sector to develop a National Infrastructure Assurance Plan.[9]

[7] The President's Commission on Critical Infrastructure Protection (PCCIP). "Critical Foundations: Protecting America's Infrastructures", Washington, October 1997.

[8] William J. Clinton. "Protecting America's Critical Infrastructures: Presidential Decision Directive 63", (Washington, 22 May 1998). http://www.usdoj.gov/criminal/cybercrime/white_pr.htm.

[9] Ibid.

## National Plan for Information Systems Protection

On 7 January 2000, Clinton presented the first comprehensive national plan for CIIP – focusing on securing the cyber-components of critical infrastructures, but not the physical components – called Defending America's Cyberspace. National Plan for Information Systems Protection Version 1.0 – An Invitation to a Dialogue.[10] This plan reinforced the perception of cyber-security as a responsibility shared between the government and the private sector.

## Homeland Security Executive Orders

In the aftermath of attacks in the US on 11 September 2001, President George Bush signed two executive orders (EO) affecting CIP. With EO 13228, entitled Establishing the Office of Homeland Security and the Homeland Security Council and issued on 8 October 2001, the Office of Homeland Security was established, headed by the assistant to the president for homeland security.[11] One of the functions of the assistant to the president is to coordinate efforts to protect the country and its CI from terrorist attacks. The EO further established the Homeland Security Council, which advises and assists the president in all aspects of homeland security.

The second executive order, EO 13231 Critical Infrastructure Protection in the Information Age, established the President's Critical Infrastructure Protection Board. The board's responsibility is to "recommend policies and coordinate programs for protecting information systems for critical infrastructure."[12] Finally, the EO also established the National Infrastructure Advisory Council (NIAC), a presidential advisory committee of owners and operators of the nation's critical infrastructures.[13]

[10] William J. Clinton. "Defending America's Cyberspace: National Plan for Information Systems Protection Version 1.0", An Invitation to a Dialogue, (Washington, 2000).

[11] George W. Bush. "Executive Order 13228", Establishing the Office of Homeland Security and the Homeland Security Council (Washington, 8 October 2001). http://www.fas.org/irp/offdocs/eo/eo-13228.htm.

[12] George W. Bush. "Executive Order 13231", Critical Infrastructure Protection in the Information Age", Washington, 16 October 2001. http://www.fas.org/irp/offdocs/eo/eo-13231.htm.

[13] Ibid.

## Homeland Security Presidential Directive / HSPD-7

On 17 December 2003, Bush released Homeland Security Presidential Directive/ HSPD-7, which supersedes PDD 63 of May 1998, and any presidential directives issued prior to this HSPD-7.

This new directive established a national policy for federal departments and agencies to identify and prioritize US critical infrastructure and key resources and protect them from terrorist attack. It identified the government agencies responsible for coordinating the protection of specific critical infrastructure sectors. A key element of this directive is the designation of federal sector-specific agencies that are charged with collaborating with specific elements of the private sector.

Also, HSPD-7 required that that by July 2004, the heads of all federal departments and agencies develop plans for protecting the physical and cyber critical infrastructure and key resources that they own or operate, including identification, prioritization, protection, and contingency planning.[14]

Finally, HSPD-7 designated the secretary of homeland security as "the principal Federal official to lead, integrate, and coordinate implementation of efforts among Federal departments and agencies, State and local governments, and the private sector to protect critical infrastructure and key resources."[15]

## National Strategies

The National Strategy for Homeland Security was released in July 2002 and established the base for CIP and CIIP in the US. On February 2003, the White House released two presidential national strategies that are follow-on documents to the National Strategy for Homeland Security, namely the National Strategy to Secure Cyberspace and the National Strategy for Physical Protection of Critical Infrastructure and Key Assets.

[14] http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html.

[15] Ibid.

## National Strategy for Homeland Security

In July 2002, the Office of Homeland Security issued the National Strategy for Homeland Security[16] to secure the US from terrorist attacks. It provides direction to the federal government departments and agencies that have a role in homeland security. One of the six "critical mission areas" identified in the strategy is protecting critical infrastructure and key assets.

In October 2007, President Bush issued an updated version of the Strategy for Homeland Security.[17] The protection of critical infrastructures and key resources is maintained as a central element of the strategy. In reference to the National Infrastructure Protection Plan (see below), the strategy defines 17 critical sectors and key resources, each with cross-cutting physical, cyber, and human elements.

## National Strategy to Secure Cyberspace

The National Strategy to Secure Cyberspace (NSSC)[18] recognizes that securing cyberspace is an extraordinary challenge that requires a coordinated effort from all parts of society and government. It defines cyberspace as an "interdependent network of information technology infrastructures" and depicts cyberspace as the nervous system or control system of society. Its main aim is to set national policies to engage US citizens in securing the portions of cyberspace they own, operate, control, or with which they interact. The NSSC therefore outlines an initial framework both for organizing and prioritizing national efforts in combating cyber-attacks committed by terrorists, criminals, or nation-states, while highlighting the role of public-private engagement.

Consistent with the National Strategy for Homeland Security, the strategic objectives of the NSSC are:

- To prevent cyber-attacks against the national CI;

[16] Office of Homeland Security. "National Strategy for Homeland Security", (Washington, July 2002). http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf.

[17] National Strategy for Homeland Security 2007, op. cit.

[18] The White House. "National Strategy to Secure Cyberspace", (Washington, 2003). http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf.

- To reduce the national vulnerability to cyber-attacks;
- To minimize damage and recovery time from cyber-attacks.

The strategy recognizes that, as owners and operators of much of the internet infrastructure, the private sector is best equipped and structured to respond to cyber-threats. Therefore, public-private engagement will take a variety of forms and will address awareness, training, technological improvements, vulnerability remediation, and recovery operations.

### The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets

The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets[19] states that the CI sectors of the US provide the foundation for national security, governance, economic vitality, and "the American way of life". Its main aim is to reduce the nation's vulnerability to acts of terrorism by reducing the vulnerability of national critical infrastructure and key assets to physical attack. An attack on the nation's critical infrastructures and key assets could not only result in large-scale human casualties and property destruction, but also damage the national prestige, morale, and confidence, as experienced in the 11 September 2001 attacks. As a result, the following strategic objectives are considered:

- To identify and assure the protection of those infrastructures and assets that are deemed most critical in terms of national-level consequences for public health and safety, governance, economic and national security, and public confidence;
- To provide timely warning;
- To assure the protection of other infrastructures and assets that may become terrorist targets over time.

[19] The White House. "National Strategy for the Physical Protection of Critical Infrastructures and Key Assets", (Washington, 2003).

By pursuing these objectives, coordinated action is required on the part of federal, state, and local governments, as well as the private sector and concerned citizens. The Department of Homeland Security (DHS) provides overall cross-sector coordination in this new organizational scheme, acting as the primary liaison and facilitator for cooperation among federal agencies, state and local government, and the private sector. Cross-sector initiatives should be fostered in the areas of planning and resource allocation, in information-sharing, in personnel security (including background checks where appropriate) and awareness, in research and development, and in modeling, simulation, and analysis.

## National Infrastructure Protection Plan (NIPP) and Sector-Specific Plans (SSP)

The National Infrastructure Protection Plan (NIPP)[20] was issued by the DHS in June 2006. It provides an overall framework for existing and future programs and activities for the protection of critical infrastructures and key resources. The NIPP defines three different protection policies: deterrence of the terrorist threat, mitigation of vulnerabilities, and mitigation of potential consequences. In addition, it specifies key initiatives; lists the public and private actors involved in CIP; sets milestones and targets that are to be achieved; and provides a risk management framework for critical infrastructures.

One of the key elements of the NIPP is that it formalizes the institution of public-private partnerships in the field of CIP and CIIP. Each sector is supposed to create a sector coordinating council for policy coordination and designate an operational entity (such as Information Sharing and Analysis Centers, ISACs) for information sharing. Likewise, the government is to form a Government Coordinating Council and sector-specific agencies for coordinating efforts on specific sectors. This collaboration takes place through the Critical Infrastructure Advisory Council framework, which provides legal protections for this collaboration.

[20] "National Infrastructure Protection Plan", op. cit.

The NIPP gives special consideration to the cyber dimension of critical infrastructure protection. Cybersecurity is addressed in two ways: first, as a cross-sector element that needs to be considered in all sectors; and second, as a major component of the IT sector's responsibility in partnership with the telecommunications sector.

The responsibility of the IT sector is further outlined in the Sector-Specific Plan for Information Technology,[21] which was published in May 2007. Sector-Specific Plans (SSPs) complement the NIPP and provide the means by which the NIPP is implemented across all critical infrastructure and key resource sectors. The SSP for the IT sector was developed collaboratively by all relevant public and private actors in the field. The plan outlines the implementation of the NIPP risk management framework; establishes sector-specific goals and objectives; aligns initiatives to meet the goals and objectives; and describes roles and responsibilities.

## National Strategy for Information-Sharing

The Strategy for Homeland Security, the National Infrastructure Protection Plan (NIPP), and the Information Technology Sector-Specific Plan all emphasize the importance of information-sharing between different sectors as well as between the government and the private sector. Various organizations and initiatives have been established to enable information-sharing within and among sectors. The National Strategy for Information Sharing,[22] which was published in October 2007, builds upon the existing efforts and provides guidelines for sharing information to protect critical infrastructures. The strategy clearly highlights the need to share information with those who need it, rather than to conceal information. It states that "the exchange of information should be the rule, not the exception."[23]

[21] Department of Homeland Security. "Information Technology: Critical Infrastructure and Key Resources Sector-Specific Plan as Input to the National Infrastructure Protection Plan", Washington, 2007.

[22] The White House. "National Strategy for Information Sharing", Washington, 2007. http://www.whitehouse.gov/nsc/infosharing/NSIS_book.pdf.

[23] Ibid. p. 1.

## Organizational Overview

In the early days, two agencies had primary responsibility for coordinating US CIP policy: The Critical Infrastructure Assurance Office (CIAO), which used to be part of the Department of Commerce, and the National Infrastructure Protection Center (NIPC), formerly a division within the Federal Bureau of Investigation (FBI). However, in accordance with the various presidential directives discussed above and the creation of the DHS, the functions of the CIAO and the NIPC have been absorbed by the DHS.

Today, DHS coordinates the governmental CIP efforts. However, within the different sectors, various agencies are deeply involved in CIP, for instance as sector-specific agencies (the National Infrastructure Protection Plan assigns the responsibility for CI/KR protection activities to different federal departments).[24] Thus, while this section focuses on agencies and offices with a coordinative task (and as a result, mainly on DHS offices), this does not mean that other government agencies are no longer involved in CIP.

### Public Agencies

#### Department of Homeland Security (DHS)

The attacks of 11 September 2001 provided the impetus to restructure the overall organizational framework for the protection of homeland security, including CIP and CIIP. In March 2003, 23 federal agencies, programs, and offices were merged to become the Department of Homeland Security (DHS).[25] The DHS coordinates the efforts of several federal, state, and local governments and encompasses a variety of agencies for all different tasks related to homeland security.[26] Within the DHS, the agencies dealing with CIP and CIIP are affiliated with the National Protection and Programs Directorate, which focuses on the reduction

[24] "National Infrastructure Protection Plan", op. cit., p. 92.

[25] http://www.dhs.gov/xabout/history/editorial_0133.shtm.

[26] http://www.dhs.gov/xabout/structure/index.shtm.

of physical and virtual risks to homeland security.[27] The following two offices are dedicated to deal with CIP and CIIP:

### Office of Infrastructure Protection (OIP)

The Office of Infrastructure Protection (OIP)[28] coordinates the different sectoral efforts to protect critical infrastructures and key resources (CI/KR). Its functions include:

- Leading a robust organizational framework to facilitate the identification, prioritization, coordination, and protection of critical infrastructures/key resources (CI/KR);
- Developing and maintaining the National Infrastructure Protection Plan (NIPP);
- Coordinating and assisting the vulnerability assessments of all 18 CI/KR sectors in the US and communicating standards to the infrastructure owners/operators and key stakeholders;
- Ensuring the maintenance of a CI/KR sector governance and information-sharing framework;
- Collecting data, analyzing risks to CI/KR, and providing government and private-sector stakeholders with a means of prioritizing resource allocation and assistance;
- Establishing and maintaining international programs and relationships that promote a global culture for the protection of CI/KR.

### Office for Cybersecurity and Communications (CS&C)

The Office of Cybersecurity and Communications (CS&C)[29] coordinates with the private sector on identifying threats, managing risks and improve situation awareness. In order to be prepared for catastrophic incidents that could damage or even destroy the ICT-network, CS&C has implemented three programs:

[27] http://www.dhs.gov/xabout/structure/editorial_0794.shtm.

[28] http://www.dhs.gov/xabout/structure/gc_1185203138955.shtm.

[29] http://www.dhs.gov/xabout/structure/gc_1185202475883.shtm.

- The National Communications System (NCS)[30] has the mission to ensure national security and emergency communication for the federal government under all circumstances.
- The National Cyber Security Division (NCSD)[31] works collaboratively with private, public, and international partners to protect the information infrastructure. It does so by building and maintaining response systems (e.g., US-CERT, see the chapter on Early Warning and Public Outreach) and by working with security partners to develop and implement risk management programs for cyber-risks in critical infrastructures.
- The Office of Emergency Communications (OEC)[32] develops, implements, and coordinates interoperable and operable communications for emergency response at all levels of government.

## US Department of State

With respect to the formulation of an international CIP program in the US, the Department of State has overall statutory authority to conduct foreign affairs, and therefore takes the lead in the interagency process of coordinating international CIP matters. The Department of State collaborates closely with the Department of Defense (DoD) to develop and implement international initiatives designed to encourage allied nations to enhance the security of those critical infrastructure and key resources on which the US military depends for its operations.[33]

## Congressional Focus

Both Houses of Congress have created bodies to focus on CIIP issues. Within the Committee on Homeland Security in the House of Representatives,[34] the following subcommittees deal with questions related to CIP and CIIP:

[30] http://www.ncs.gov/about.html.

[31] http://www.dhs.gov/xabout/structure/editorial_0839.shtm.

[32] http://www.dhs.gov/xabout/structure/gc_1189774174005.shtm.

[33] http://www.state.gov/t/pm/ppa/icipt.

[34] http://homeland.house.gov/about/index.asp.

- Subcommittee on Transportation Security and Critical Infrastructure Protection;
- Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology;
- Subcommittee on Emergency Communications, Preparedness, and Response;
- Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment.

Within the Senate Committee on the Judiciary,[35] the Subcommittee on Terrorism, Technology, and Homeland Security has oversight of laws related to government information policy, electronic privacy, security of computer information, and the Freedom of Information Act.[36] The House Government Reform Committee[37] has similar, but not identical, jurisdiction.

The Senate Homeland Security and Government Affairs Committee[38] has overall jurisdiction, for the Senate, on most homeland security issues, including critical infrastructure protection. Its Subcommittee on Federal Financial Management, Government Information, and International Security has jurisdiction on matters related to cyber-security.

## Government Accountability Office (GAO)

The Government Accountability Office (GAO)[39] is the investigative arm of Congress. It is an independent and nonpartisan body that studies federal government spending and helps to improve the performance and ensure the accountability of the federal government. Congress often asks the GAO to study the programs and expenditures of the federal government. The GAO has released several reports and testimonies addressing critical infrastructure protection and information security. For example:

[35] http://judiciary.senate.gov.
[36] http://judiciary.senate.gov/subcommittees/110/technology110.cfm.
[37] http://oversight.house.gov.
[38] http://hsgac.senate.gov/public.
[39] http://www.gao.gov/about/index.html.

- In July 2004, the GAO reported on Critical Infrastructure Protection and Improving Information Sharing with Infrastructure Sectors. In this report, the GAO recommends that the DHS proceed with the development of an information-sharing plan that defines roles and responsibilities and establishes appropriate policies for interacting with ISACs and the various stakeholders involved.[40]
- In May 2005, the GAO reported on Information Security: Emerging Cybersecurity Issues Threaten Federal Information Systems, addressing the problems of spam, phishing, and spyware and the resulting security risks to federal information systems.[41]
- In May 2005, the GAO reported on Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities. The following issues were identified as key challenges facing the DHS: achieving organizational stability; gaining organizational authority; overcoming hiring and contracting issues; increasing awareness about cyber-security roles and capabilities; establishing effective partnerships with stakeholders and sharing information with these stakeholders.[42]
- In May 2005, the GAO report Information Security: Federal Agencies Need to Improve Controls over Wireless Networks advised federal agencies to implement various controls, including policies, practices, and tools, to secure their wireless networks.[43]

[40] United States Government Accountability Office (GAO). "Critical Infrastructure Protection and Improving Information Sharing with Infrastructure Sectors", (GAO-04-780, July 2004). http://www.gao.gov/new.items/d04780.pdf.

[41] United States Government Accountability Office (GAO). "Report to the Congressional Requesters, Information Security. Emerging Cybersecurity Issues Threaten Federal Information Systems", (GAO-05-231, May 2005). http://www.gao.gov/new.items/d05231.pdf.

[42] United States Government Accountability Office (GAO). "Critical Infrastructure Protection. Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities", (GAO-05-434, May 2005). http://www.gao.gov/new.items/d05434.pdf.

[43] United States Government Accountability Office (GAO). "Information Security: Federal Agencies Need to Improve Controls over Wireless Networks", (GAO-05-383, May 2005). http://www.gao.gov/new.items/d05383.pdf.

## Defense Community

In May 2007, the DoD published the Sector-Specific Plan for the Defense Industrial Base as input to the National Infrastructure Protection Plan of 2006.[44] The Defense Industrial Base (DIB) includes the DoD, the US government, and the private sector companies that design, produce, deliver, or maintain military weapon systems, subsystems, components, or parts to meet military requirements. The DIB does not include commercial communication and information infrastructure, which are addressed by the respective Sector-Specific Plans.

Nevertheless, the information infrastructure is of course crucial for the DoD. The latter has therefore established information assurance programs in the Office of the Assistant Secretary of Defense for Networks and Information Integration (OASD/NII)[45] that are headed by a Chief Information Officer of the DoD.

## Computer Crime and Intellectual Property Section (CCIPS)

The Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division of the Department of Justice is responsible for implementing the department's national strategies in combating computer and intellectual property crimes worldwide. The Computer Crime Initiative is a comprehensive program designed to combat electronic penetration, data theft, and cyber-attacks on critical information systems. CCIPS prevents, investigates, and prosecutes computer crimes by working with other government agencies, the private sector, academic institutions, and foreign counterparts.[46]

## Public-Private Partnerships

The cornerstone of US CIP policy is active cooperation between the public and private sectors. The President's Commission on Critical Infrastructure Protection (PCCIP) concluded that "the need for infrastructure protection creates a zone of

[44] http://www.dhs.gov/xlibrary/assets/nipp-ssp-defense-industrial-base.pdf.

[45] http://www.defenselink.mil/cio-nii/index.shtml.

[46] http://www.usdoj.gov/criminal/cybercrime/index.html.

shared responsibility and potential cooperation for industry and government".[47] Since then, public-private partnerships and information-sharing between public and private sectors have been central for CIP efforts in the US. This section provides an overview on the most important organizations and programs for public-private partnerships in the field of critical infrastructure protection and cybersecurity.

## DHS Interagency Committees

As the leading department for CIP, it is one of the DHS's main tasks to facilitate partnership efforts between the government and the private sector. The two following interagency committees within the DHS are responsible for coordination and supervision of partnership efforts:

- The National Infrastructure Advisory Council (NIAC)[48] advises the president on the security of the critical infrastructure sectors and their information systems. The council is composed of a maximum of 30 members appointed by the president from private industry, academia, and state and local government;
- Critical Infrastructure Partnership Advisory Council (CIPAC)[49] was established in 2006 to facilitate effective coordination between federal infrastructure protection programs with the infrastructure protection activities of the private sector and of state, local, territorial, and tribal governments. CIPAC's membership encompasses representatives from the individual sector coordinating councils as well as from federal, state, local, and tribal governmental entities;
- The president's National Security Telecommunications Advisory Committee (NSTAC) is a CEO-level advisory committee on telecommunications issues.

[47] The President's Commission on Critical Infrastructure Protection (PCCIP), op. cit, p. 35.

[48] http://www.dhs.gov/xlibrary/assets/niac/NIAC_Brochure.pdf.

[49] http://www.dhs.gov/xprevprot/committees/editorial_0843.shtm.

## Protected Critical Infrastructure Information Program (PCIIP)

The Protected Critical Infrastructure Information Program (PCIIP) aims to protect certain information shared by the private sector from being disclosed under the federal Freedom of Information Act. Under this program, only people who are trained and certified as PCII-compliant can receive protected critical infrastructure information. The program's goal is to encourage private-sector companies to voluntarily share information so that the DHS and other federal, state, and local analysts can:

- Analyze and secure critical infrastructure and protected systems;
- Identify vulnerabilities and develop risk assessments;
- Enhance recovery preparedness measures.[50]

## Information Sharing and Analysis Centers (ISACs)

Today, most critical infrastructure industry sectors have established their own Information Sharing and Analysis Center (ISAC). Private-sector ISACs are membership organizations managed by the private sector. Each ISAC has a board of directors that determines its institutional and working procedures. The function of an ISAC is to collect, analyze, and share security, incident, and response information among ISAC members and with other ISACs, and to facilitate information exchange between the government and the private sector. The following list gives an overview of the most mature ISACs with regard to CIIP:

- The IT-ISAC started operations in March 2001. Members include 20 major hardware, software, and e-commerce firms, including Microsoft, Intel, CA, Symantec, CSC, IBM, Oracle, Ebay, EWA-IIT, Harris, Hewlett Packard, BAE Systems, IT, and VeriSign, Inc. The ISAC is overseen by a board made up of members, and its operations center is managed by Internet Security Systems;[51]

[50] http://www.dhs.gov/xinfoshare/programs/editorial_0404.shtm.

[51] https://www.it-isac.org.

- The telecommunications industry has established an ISAC through the National Coordinating Center (NCC). Each member firm of the NCC monitors and analyzes its own networks. Incidents are discussed within the NCC, and members decide whether the suspect behavior is serious enough to report to the appropriate federal authorities;[52]
- The electric power sector has created a decentralized ISAC through its North American Electricity Reliability Council (NERC). Much like the NCC, the NERC monitors and coordinates responses to disruptions in the nation's supply of electricity.[53] The government and industry work together in the NERC to ensure the resilience of the electricity infrastructure in case of potential physical and cyberspace attacks;[54]
- A number of the nation's largest banks, securities firms, insurance companies, and investment companies have joined in a limited liability corporation to form a Financial Services Information Sharing and Analysis Center (FS/ISAC);[55]
- In addition to the individual sector ISACs, several ISAC leaders have convened as an ISAC Council.[56] This council strives to strengthen the relationship between the ISAC community and government, and to solve problems common to all ISACs.

## InfraGard

InfraGard is a partnership between industry and the US government as represented by the FBI. The InfraGard initiative was developed to encourage the exchange of information by members of the government and the private sector. With help from the FBI, private-sector members and FBI field representatives form local chapter areas. These chapters set up their own boards to share informa-

[52] http://www.ncs.gov/ncc.

[53] http://www.nerc.com; Energy Information Sharing and Analysis Center, http://www.esisac.com/.

[54] http://www.nerc.com/cip.html.

[55] http://www.fsisac.com.

[56] http://www.isaccouncil.org/about.

tion among their membership. This information is then disseminated through the InfraGard network and analyzed by the FBI.[57]

## National Cyber Security Alliance (NCSA)

The National Cyber Security Alliance (NCSA) is a cooperative effort between industry and government organizations to foster awareness of cyber-security through educational outreach and public awareness. Its goal is to raise citizens' awareness of the critical role that computer security plays in protecting the nation's internet infrastructure, and to encourage computer users to protect their home and small-business systems.[58] It offers computer security advice and tools for private users as well as small businesses on its website. The NCSA is sponsored by a variety of organizations.

## Partnership for Critical Infrastructure Security (PCIS)

The Partnership for Critical Infrastructure Security (PCIS)[59] grew out of initiatives outlined in Presidential Decision Directive 63 (PDD 63) as a means to coordinate CIP efforts across critical infrastructure sectors. In October 2005, the National Infrastructure Advisory Council (NIAC) recommended that the PCIS serve as the cross-sector coordinating mechanism, as part of the DHS partnership model. Today, the PCIS serves that role, and its membership consists of the leaders of the various sector coordinating councils. The PCIS works to develop joint policies to secure CI and examines cross-sector issues.

## The Cross Sector Cyber Security Working Group (CSCSWG)

The Cross Sector Cyber Security Working Group (CSCSWG)[60] serves as a forum to bring together representatives of the government and the private sec-

[57] http://www.infragard.net.

[58] http://www.staysafeonline.info.

[59] http://www.pcis.org/index.htm.

[60] The information on CSCSWG was provided by the US expert involved.

tor to address risk collaboratively across the CI/KR sectors. In this function, it replaces the National Cyber Security Partnership,[61] which was the forum for cross-sector coordination until 2005.

The CSCSWG is co-chaired by the industry and the government. It focuses on strategic cross-sector cybersecurity issues such as:

- Identifying opportunities to improve sector coordination around cyber security issues and topics (e.g., the internet, control systems);
- Considering the policy implications of cross-sector cyber dependencies and interdependencies; and
- Providing a conduit for sharing the group's products and findings with the sectors through their Sector Coordinating Council (SCC), Information Sharing and Analysis Center (ISAC), and Sector-Specific Agency (SSA) representatives.

## Institute for Information Infrastructure Protection (I3P)

The Institute for Information Infrastructure Protection (I3P), managed by Dartmouth College, is a consortium of leading national cyber-security institutions, including academic research centers, government laboratories, and non-profit organizations. Founded in September 2001, the institute's main role is to coordinate a national cyber-security research and development program and to help build bridges between academia, industry, and the government. The I3P identifies and addresses critical research problems in CIIP and opens information channels between researchers, policy-makers, and infrastructure operators.[62]

[61] http://www.cyberpartnership.org.

[62] http://www.thei3p.org.

## Early Warning and Public Outreach

Information-sharing is one of the driving factors behind effective early-warning networks. Many entities focused on information-sharing are also engaged in early-warning activities.

### CERT Coordination Center, Carnegie Mellon University

The Computer Emergency Response Team Coordination Center (CERT/CC) is the oldest and still one of the most important early-warning programs in the field of information security. It is a federally funded research and development center operated by Carnegie Mellon University. It was established in 1988 after the Morris worm crashed 10 per cent of the world's internet systems. CERT/CC acts as a coordination hub for experts during security incidents, and works to prevent future incidents.

The CERT/CC acts through several mechanisms. First, its experts research and assess network vulnerabilities and develop risk assessments. Second, they disseminate information to the public through regular security alerts and presentations to the public. Finally, members of the CERT/CC participate in various security groups to improve internet security and network survivability. The CERT/CC is a primary contributor to the US-CERT. [63]

### US-CERT

On 15 September 2003, the Department of Homeland Security, in conjunction with the CERT Coordination Center (CERT/CC) at Carnegie Mellon University, announced the creation of the US-CERT. The US-CERT works with the National Cyber Security Division (NCSD) of the IAIP to prevent and mitigate cyber-attacks and to reduce vulnerabilities to cybernetic attacks. Together, they have set up the National Cyber Alert System, a trusted warning

[63] http://www.cert.org.

system offered by the government to help home users and technology experts. It sends e-mails about major virus outbreaks and other internet attacks as they occur, along with detailed instructions to help computer users protect themselves.

The US-CERT initiative is designed to help accelerate the nation's response to cyber-attacks and vulnerabilities. The initiative also enables the DHS to provide expanded analysis, warning, and response coordination.[64]

## Federal Bureau of Investigation (FBI)

The 1997 PCCIP Report stated that efforts were required to establish a system of surveillance, assessment, early warning, and response mechanisms.[65] The FBI was chosen to serve as the preliminary national warning center for infrastructure attacks and to provide information on law enforcement and intelligence. Under PDD 63, the National Infrastructure Protection Center (NIPC) as part of the FBI was given responsibility for developing analytical capabilities to provide information on changes in threat conditions and newly identified system vulnerabilities, as well as timely warnings of potential and actual attacks.[66] The NIPC, as discussed above, was incorporated into the DHS, but the FBI still retains its responsibilities for addressing cyber-crime.

## Information-Sharing and Analysis Centers (ISACs)

The Information Sharing and Analysis Centers (ISACs) serve as an early warning and situational awareness capability by providing a forum for members to report information on threats, vulnerabilities, and incidents. ISACs then collate the information, as well as information they receive from other sources, analyze it, and issue warnings and alerts to members. Many ISACs, such as the IT-ISAC, for example, now distribute information more broadly throughout the sector, beyond its own individual membership (see the chapter on Organizational Overview).

[64] http://www.uscert.gov.

[65] President's Commission on Critical Infrastructure Protection (PCCIP), Critical Foundations, op. cit.

[66] "Presidential Decision Directive 63", op. cit.

### OnGuardOnline.gov

OnGuardOnline.gov provides practical recommendations from the federal government and the technology industry to help users be on guard against internet fraud, to secure their computers, and to protect their personal information. The comprehensive website has tips, articles, videos, and interactive activities. The Federal Trade Commission (FTC) maintains OnGuardOnline.gov with contributions from various government departments, including the DHS.[67]

## Law and Legislation

### Federal Advisory Committee Act (FACA) 1972

One obstacle to fully implementing a robust public-private partnership is the 1972 Federal Advisory Committee Act (FACA). The FACA (Public Law 92-463, 5 U.S.C., App) was enacted by Congress in 1972. Basically, this act is designed to prevent any person or company (or groups of them) from having undue influence in government decision-making. Its purpose was to ensure that advice rendered to the executive branch by the various advisory committees, task forces, boards, and commissions formed over the years by Congress and the president be both objective and accessible to the public. The act not only formalized a process for establishing, operating, overseeing, and terminating these advisory bodies, but also created the Committee Management Secretariat, whose task it is to monitor and report executive branch compliance with the act.[68]

In the field of CIP / CIIP, the delicate issue is that CIP is based on partnership with the DHS, which requires meetings. If these meetings are open to the public and subject to other government restrictions, the industry will be unwilling to be frank or overly commit itself, since businesses would be putting sensitive information in the public domain.

[67] http://onguardonline.gov/index.html.

[68] http://www.gsa.gov/Portal/gsa/ep/channelView.do?pageTypeId=8203&channelPage=/ep/channel/gsaOverview.jsp&channelId=-13170.

In the US, the challenge has been to ensure that the private sector and its representatives have the opportunity to provide comments and input on CIP policy without violating FACA considerations. One solution to this is found in Section 871 of the Homeland Security Act, which gives the secretary of homeland security the authority to create FACA-exempt advisory panels. Secretary Chertoff used the authority granted to him in Section 871 to create a FACA exempt organization to work on CIP issues. This is the Critical Infrastructure Partnership Advisory Council referred to earlier.[69]

## Computer Fraud and Abuse Act (CFAA) 1986

In the US, legislative awareness of computer crimes grew dramatically in the early 1980s as computers became increasingly important for the conduct of business and politics. The Computer Fraud and Abuse Act (CFAA) of 1986 was the conclusion of several years of research and discussion among legislators.[70] It established two new felony offenses of unauthorized access to "federal interest" computers[71] and unauthorized trafficking in computer passwords. Violations of the CFAA include intrusions into government, financial, medical, and "federal interest" computers.

The Computer Abuse Amendments Act of 1994 expanded the 1986 CFAA to address the transmission of viruses and other harmful code. The measures provided by this act were further tightened on 26 October 2001 by the USA PATRIOT antiterrorism legislation.[72] Violations of the CFAA are investigated by the National

[69] Information provided by a US expert involved.

[70] http://www4.law.cornell.edu/uscode/18/1001.html.

[71] "Federal interest computers" are defined as two or more computers involved in a criminal offense, if they are located in different states.

[72] "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act". For the full-text version, see: http://www.cdt.org/security/usapatriot/011026usa-patriot.pdf. Privacy and civil liberty advocacy groups have expressed concern over the USA PATRIOT Act and a number of other legislative developments.

Computer Crimes Squad at the FBI and supported by its Computer Analysis and Response Team (CART), a specialized unit for computer forensics.[73]

## Homeland Security Act 2002

Much of the federal legislation concerning CIP/CIIP was written before the emergence of "cyber-threats". Thus, it is questionable whether a timely and efficient response would be possible under the existing legal frameworks at both federal and state/local levels.[74]

While the overall act established the Department of Homeland Security (DHS), Title II of the Homeland Security Act (of 2002) specifically addresses information analysis and infrastructure protection. It transferred the various agencies (like CIAO, NIPC, and others mentioned above) into the DHS, and established the categories of information to which the secretary of homeland defense has access. In order to adequately protect the nation, the secretary has access to certain intelligence analysis, infrastructure vulnerabilities, and any "raw" data that the president discloses to the secretary.

## Freedom of Information Act (FOIA)

CIIP is an important issue in the US, primarily because many of the critical sectors are regulated by the government, but controlled by private entities. As part of the regulation, the private entities must regularly file reports and disclose sensitive information to the government. This could place such information in jeopardy, since under the Freedom of Information Act (FOIA), the public can request such information from the government. However, a FOIA exemption was included in the Homeland Security Act of 2002. Any information regarding

[73] http://www.fbi.gov/hq/lab/org/cart.htm. Of further importance is also the recent enactment of the Gramm-Leach-Bliley (GLB) Act and the regulations for implementing it, which address privacy concerns by setting forth a range of requirements to protect customer information. For the text of the GLB Act, see: http://www.ftc.gov/privacy/privacyinitiatives/glbact.html.

[74] President's Commission on Critical Infrastructure Protection (PCCIP), Critical Foundations, op. cit., p. 81.

critical infrastructures (including security systems, warnings, or interdependency studies) is exempt from disclosure.

After the attacks of 11 September 2001, the Federal Energy Regulatory Commission (FERC) removed certain information from its website and its public reading room. This included detailed maps and other information about electric power facilities and natural gas pipelines. Although exempt from FOIA procedures, this information had traditionally been open and available to anyone who requested it. In February 2003, the FERC ruled that individuals wanting access to this information would have to apply for it. The application requirements include identification information, and take into account the necessity or purpose of accessing the information. Access is granted on a case-by-case basis, and only to individual applicants.

## Critical Infrastructure Information Act: Procedures for Handling Critical Infrastructure Information

The Homeland Security Act of 2002 contained a provision called the Critical Infrastructure Information Act, which was designed to encourage the private sector to share information voluntarily with the DHS. In April 2003, the DHS released regulations for the implementation of this program, which the DHS has named the Protected Critical Infrastructure Information Program (PCIIP).[75] These regulations, which were authorized in the Homeland Security Act of 2002, provide rules for the receipt, care, and storage of critical infrastructure information, the maintenance of security and confidentiality, and methods for dealing with proprietary or business-sensitive information. The basic concept of the regulations again underscores the fundamental principles of public-private partnership. Their goal is to encourage the private sector to share sensitive security information with the DHS without fear that the information will be made public. It stipulates that business-sensitive information that businesses voluntarily submit to the DHS may be labeled CII and exempted from disclosure under the FOIA. Under this program, CII that the DHS shares with state and local

[75] Procedures for Handling Critical Infrastructure Information, 68 Fed. Reg. 18,524 (2003) (to be codified at 6 C.F.R. §29).

governments would be protected from state laws pursuant to the Freedom of Information Act. The final rules implementing this program have not yet been issued. This change in the law has potentially broad effects and requires a change of culture, as disclosure of information held by the government has traditionally been favored in the US.

## Terrorism Risk Insurance Act 2002

The Terrorism Risk Insurance Act of 2002 is a new law that creates a federal program for public and private compensation for insured losses resulting from acts of terrorism. All commercial insurance providers must offer terrorism risk insurance, and the federal government agrees to underwrite some of the losses in the event that a terrorist event takes place. Under this law, an act of terrorism includes any act of violence against elements of the infrastructure.[76] This could include catastrophic network assaults as well as physical attacks.

[76] Terrorism Risk Insurance Act of 2002, Pub. L. No. 107-297, 116 Stat. 2322.

# Part II

# International Organizations and Forums

# European Union (EU)

The European Union is a key player at the international level concerning information assurance. CIIP, the Information Society, and information security are considered key issues. Therefore, the EU has launched initiatives and research programs to study various aspects of the information revolution and its impact on education, business, health, and communications.

The terrorist attacks in Madrid in 2004 and London in 2005 have highlighted the risk of terrorist attacks against European infrastructures in a broader sense. The damage or loss of a piece of infrastructure in one state may have negative effects on several others, and on the European economy as a whole. The following chapter gives a short overview of important steps taken by the EU in the field of CIP and CIIP.[1]

## Critical Sectors

The Communication of the Commission of the European Communities (EU Commission) on Critical Infrastructure Protection in the Fight Against Terrorism, adopted on 20 October 2004, provides a definition of critical infrastructures (CI), enumerates the critical sectors identified, and discusses the criteria for determining potential CI. In the Communication, CI are defined as follows: "Critical infrastructures consist of those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in the Member States.

[*] The European Union Survey of 2008 was reviewed by Marcelo Masera, European Commission, Institute for the Protection and Security of the Citizen Joint Research Centre. The Chapter on Law and Legislation was reviewed by Martin Wählisch, Humboldt University Berlin.

[1] http://ec.europa.eu/information_society/index_en.htm.

Critical infrastructures extend across many sectors of the economy and key government services."[2]

In the follow-up publication of the EU Commission, the Green Paper on a European Program for Critical Infrastructure Protection (Green Paper on EPCIP),[3] CIIP is defined as: "The programs and activities of infrastructure owners, operators, manufacturers, users, and regulatory authorities which aim at keeping the performance of CII in case of failures, attacks or accidents above a defined minimum level of services and aim at minimizing the recovery and damage. CIIP should therefore be viewed as a cross-sector phenomenon rather than being limited to specific sectors. CIIP should be closely coordinated with CIP from a holistic perspective."[4]

The Green Paper on EPCIP identifies the following critical sectors and their products and services:

- Energy (Oil and Gas Production, Refining, Treatment and Storage, including Pipelines; Electricity Generation; Transmission of Electricity, Gas, and Oil; Distribution of Electricity, Gas, and Oil),
- Information and Communication Technologies (ICT) (Information System and Network Protection; Internet; Provision of Fixed Telecommunications; Provision of Mobile Telecommunications; Radio Communication and Navigation; Satellite Communication; Broadcasting),
- Water (Provision of Drinking Water; Control of Water Quality; Stemming and Control of Water Quantity),
- Food (Provision of Food and Safeguarding Food Safety and Security),
- Health (Medical and Hospital Care; Medicines, Serums, Vaccines, and Pharmaceuticals; Bio-Laboratories and Bio-Agents),

[2] Commission of the European Communities. Critical Infrastructure Protection in the Fight against Terrorism (Brussels, 20 October 2004), COM(2004)702 final, p. 3. http://europa.eu.int/comm/justice_home/doc_centre/criminal/terrorism/doc/com_2004_702_en.pdf.

[3] Commission of the European Communities. Green Paper on a European Programme for Critical Infrastructure Protection (Brussels, 17 November 2005), COM(2005) 576 final, p. 19. http://www.libertysecurity.org/IMG/pdf/EC_-_Green_Paper_on_CI_-_17.11.2005.pdf.

[4] Ibid., p. 19.

- Financial System (Payment Services/Payment Structures (private); Government Financial Assignment),
- Public and Legal Order and Safety (Maintaining Public and Legal Order, Safety and Security; Administration of Justice and Detention),
- Civil Administration (Government Functions; Armed Forces; Civil Administration Services; Emergency Services; Postal and Courier Services),
- Transport (Road Transport; Rail Transport; Air Traffic; Inland Waterways Transport; Ocean and Short-Sea Shipping),
- Chemical and Nuclear Industry (Production and Storage/Processing of Chemical and Nuclear Substances; Pipelines of Dangerous Goods (Chemical Substances),
- Space and Research.[5]

Although most infrastructures are owned and operated by the private sector, the EU Commission declared in its Communication 574/2001 of 10 October 2001: "The reinforcement of certain security measures by the public authorities in the wake of attacks directed against society as a whole and not at the industry players must be borne by the State. The public sector has therefore a fundamental role to play too."[6]

To determine the criticality of an infrastructure is a complex task. The EU Commission suggests that the following three factors be taken into consideration when identifying potential critical infrastructures:

- Scope: the loss of a critical infrastructure element is rated by the extent of the geographic area (international, national, provincial/territorial, or local) that could be affected by its loss or unavailability;
- Magnitude: the degree of the impact or loss can be categorized as "none", "minimal", "moderate", or "major". Among the criteria for assessing the potential magnitude of an incident are: public impact (number of citizens affected, loss of life, medical illness, serious injury, evacuation); economic impact (GDP effect, significance of economic loss and/or degradation

[5] Green Paper on CIP, op. cit., p. 24.

[6] CIP in the Fight against Terrorism, op. cit., p. 4.

of products or services); environmental impact (effect on the public and the environment); interdependency (with other critical infrastructure elements); and finally, political impact (confidence in the ability of the government to cope);

- Effects of time: this criterion ascertains at what point the loss of an element could have a serious impact (e.g., immediately, within 24 to 48 hours, within one week).

However, in most cases, psychological effects also need to be taken into consideration.[7]

## Initiatives and Policies

The European Commission plans to launch a policy initiative on Critical Communication and Information Infrastructure Protection (CIIP) in 2008.[8] The aim is to ensure an adequate and consistent level of protective security and the resilience of critical information infrastructure throughout the European Union. This initiative will be part of the broader framework of the European Programme for Critical Infrastructure Protection (EPCIP)[9] and managed independently by the Information and Media Directorate-General (DG INFSO).[10] This initiative is the latest development since the European Council recognized the vulnerability and interdependency of underlying infrastructures in June 2004 and asked the Commission and the member states to prepare an overall strategy on critical infrastructure protection.

In response to this request, the Commission issued a Green Paper on the EPCIP in November 2005.[11] It was followed, in December 2006, by a proposal

[7] Ibid., pp. 3–5.

[8] http://ec.europa.eu/dgs/information_society/index_en.htm, and: http://ec.europa.eu/information_society/index_en.htm.

[9] http://ec.europa.eu/justice_home/fsj/terrorism/protection/fsj_terrorism_protection_infrastruct_en.htm.

[10] http://ec.europa.eu/dgs/information_society/index_en.htm.

[11] http://ec.europa.eu/justice_home/fsj/terrorism/protection/fsj_terrorism_protection_infrastruct_en.htm.

for a directive of the Council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection.[12]

In parallel, the Commission's strategy[13] for a secure information society stressed that critical infrastructures are also becoming increasingly dependent on the security of their respective information systems. The strategy was acknowledged by a Council Resolution,[14] and the creation of an environment enhancing the reliability, resilience, and robustness of communication networks and information systems was promoted by the Council. The main activities undertaken so far by the European Union are addressed below.

## Study for the Commission on the Availability and Robustness of Electronic Communication Infrastructures (ARECI)

In preparation for this new action area, Lucent Technologies carried out a study for the Commission on the Availability and Robustness of Electronic Communication Infrastructures (ARECI). The study makes ten recommendations for key actions to be taken by the European Commission, member states, and the private sector to improve the reliability, resilience, and robustness of the underlying infrastructures. These recommendations include the areas of emergency preparedness, priority communications on public networks, formal mutual aid agreements, critical infrastructure information-sharing, inter-infrastructure dependencies, integrity and trusted operation of the supply chain, unified European voice standards, interoperability testing, vigorous ownership and partnering deals, and discretionary European expert best practices. The report was presented in January 2007. Stakeholders were invited to comment on its findings, and contributions were discussed in June 2007.[15]

[12] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52006PC0787:EN:NOT.

[13] http://ec.europa.eu/information_society/policy/nis/strategy/index_en.htm.

[14] http://eur-lex.europa.eu/LexUriServ/site/en/oj/2007/c_068/c_06820070324en00010004.pdf.

[15] Both the study and the discussions reports are available here: http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/areci_study/index_en.htm.

## Green Paper on a European Programme for CIP (EPCIP)

The EC Communication on CIP in the Fight Against Terrorism mentioned above discusses the EU Commission's efforts in the field of CIP and proposes additional measures to strengthen existing instruments, mainly by the establishment of a European Programme for Critical Infrastructure Protection (EPCIP). On 24 November 2005, the EU Commission published a "Green Paper on a European Programme for Critical Infrastructure Protection",[16] which outlines options to enhance prevention, preparedness, and responses in protecting the EU's critical infrastructure. The Green Paper provides options on how the EU Commission may respond to the EU Council's request to establish an EPCIP and a Critical Infrastructure Warning Information Network (CIWIN), and constitutes the second phase of the consultation process that began with the Commission Communication on CIP that was adopted in October 2004.

The Green Paper addresses such key issues as:

- EPCIP's protection aim;
- Key principles;
- The type of framework needed;
- Definitions and a comprehensive list of EU Critical Infrastructures (ECI);
- ECI versus National Critical Infrastructures (NCI);
- The role of CI owners, operators, and users;
- The role of CIWIN, and the evaluation and monitoring of critical infrastructure (interdependencies).

The options presented by the Green Paper on EPCIP are a combination of measures and should be seen as complementary measures to current national efforts.

[16] Green Paper on CIP, op. cit.

## Critical Infrastructure Warning Information Network (CIWIN)

In order to facilitate the exchange of information on shared threats and vulnerabilities within the EU, the EU Commission is setting up the Critical Infrastructure Warning Information Network (CIWIN). This EU network aims at helping member states, EU institutions, and owners and operators of critical infrastructure to exchange information on shared threats, vulnerabilities, and appropriate measures and strategies to mitigate risk in support of critical infrastructure protection.[17] The precise determination of the nodes of this network is still an open issue and will most likely include authorities at various levels.[18]

The EU Commission suggested the following three possible options for the development of the CIWIN in its Green Paper:

- The CIWIN could take the shape of a forum limited to the exchange of CIP ideas and best practices in support of CI owners and operators;
- The CIWIN could be a rapid alert system (RAS) linking member states with the EC;
- CIWIN could be a multi-level communication and alert system with two distinct functions: a rapid alert system (RAS) linking member states with the EU Commission, and a forum for the exchange of CIP ideas and best practices.

Regardless of the option finally chosen, the CIWIN will complement existing networks and not duplicate them.[19]

[17] CIP in the fight against terrorism, op. cit., p. 10. The US has a similar system, known as the Critical Infrastructure Warning Information Network (CWIN), which has been operational since 2003. http://www.gao.gov/new.items/d05434.pdf.

[18] Information provided by an expert.

[19] Green Paper on CIP, op. cit.

## European Network and Information Security Agency (ENISA)

The European Network and Information Security Agency (ENISA)[20] was created on 14 March 2004. By deciding on 5 June 2003 to set up ENISA as a legal entity, the EU reinforced its efforts to enhance European coordination on information security.

ENISA aims at ensuring a high level of network and information security within the community. Thus, the agency contributes to the development of network and information security for the benefit of the citizens, consumers, enterprises, and public-sector organizations of the EU. This work also contributes to the smooth functioning of the Internal Market.

The agency assists the EU Commission, the member states, and, consequently, the business community in meeting the requirements of network and information security, including present and future EU legislation. ENISA ultimately serves as a center of expertise both for member states and for EU institutions to seek advice on matters related to network and information security.

ENISA's work programs included several deliverables. It has created a Who is Who Directory on Network and Information Security[21] with contact information for authorities acting in the field of network and information security in the member states. ENISA has also published an Inventory of CERT Activities in Europe[22] and issues a quarterly newsletter. In addition, ENISA organizes workshops for outreach and dissemination of good practices in the member states. Moreover, ENISA defines customized information packages, including good practices for specific target groups (e.g., SMEs and home users). Finally, ENISA has created a network of liaison officers that helps ENISA to exchange information and cooperate on a day-to-day basis with member states.[23]

[20] http://www.enisa.europa.eu/index.htm.

[21] European Network and Information Security Agency (ENISA). Who is Who Directory on Network and Information Security (Version 2.0, December 2006). http://www.enisa.europa.eu/doc/pdf/deliverables/wiw_v2_2006.pdf.

[22] European Network and Information Security Agency (ENISA). ENISA Inventory of CERT Activities in Europe (Version 1.5, September 2007). http://www.enisa.europa.eu/cert_inventory/downloads/Enisa_CERT_inventory.pdf.

[23] http://www.enisa.europa.eu/index.htm.

ENISA's latest work program for 2008 is entitled Build on Synergies – Achieve Impact,[24] and was released in November 2007. It focuses on increasing the agency's impact in network and information security based on cooperation with relevant stakeholders. The Work Programme has been developed in a new approach of setting priorities in closer cooperation with all stakeholders. It also introduces three new key elements by defining so-called Multi-annual Thematic Programmes (MTP). The current three MTPs cover the following topics:[25]

- Improving resilience in European e-Communication networks;
- Developing and maintaining cooperation models;
- Identifying emerging risks for creating trust and confidence.

It offers an overview of ENISA's activities, including awareness-raising and promotion of best practices, and enhancing cooperation. ENISA is aware of the importance of its role and supports the strategy of the European Commission. In an effort to maximize the impact of its activities, the agency strives to leverage existing synergies and initiatives at the national and European levels and will follow a more focused impact-oriented approach.[26]

## Research and Development

### Information Society Technologies (IST) FP6 and FP7

The overall objective of the IST (Information Society Technologies) efforts within the EU's Sixth Framework Program (FP6) was to contribute directly to realizing European policies for the information society as agreed at the Lisbon European Council of 2000, the Stockholm European Council of 2001, and the Seville European Council of 2002, and as reflected in the eEurope Action Plan.

[24] European Network and Information Security Agency (ENISA). Work Programme 2008: "Build on Synergies – Achieve Impact." http://www.enisa.europa.eu/doc/pdf/management_board/decisions/enisa_wp_2008.pdf.

[25] http://www.enisa.europa.eu/pages/02_01_press_2007_11_21_wp_2008.html.

[26] ENISA. Work Programme 2008, op. cit., p. 3.

The IST component of FP6, which ran from 2002 to 2006, aimed at ensuring European leadership in the generic and applied technologies at the heart of the knowledge economy. The IST research efforts within FP6 reinforced and complemented the eEurope 2005 objectives. In this EU research program, IST had the first priority in terms of funding.[27] Among the strategic objectives of IST FP6 were: A global dependability and security framework; semantics-based knowledge systems; networked business and government; e-Safety for road and air transport; e-Health; cognitive systems; embedded systems; improving risk management; and e-Inclusion. As in the preceding FP5, the focus of these projects was mainly on technical issues, whereas policy aspects (such as organizational aspects, ethical questions, etc.) concerning CIIP were hardly discussed and somewhat undervalued in the strategic objectives.

Under FP7, which began in 2007 and runs until 2013, the EU Commission wishes to identify topical areas of interest that are continued after the end of FP6, as well as new and emerging topics, including space and security.[28] While the EU has been funding research into ICTs since 1986, the Seventh Research Framework Programme is the largest yet.[29] This is due to the commitment that Europe must master both the development and use of ICTs to generate economic growth required to fund its social model and protect its environment and quality of life.[30] More specifically, the objective of ICT research under the EU's FP7 is to improve Europe's competitiveness at all levels by focusing on the following three key areas of ICT:[31]

- Productivity and innovation, by facilitating creativity and management;
- Modernization of public services, such as health, education and transport;
- Advances in science and technology, by supporting cooperation and access to information.

[27] http://ec.europa.eu/information_society/research/index_en.htm.
[28] http://ec.europa.eu/research/future/themes/index_en.cfm.
[29] http://ec.europa.eu/information_society/research/eu_research/index_en.htm.
[30] http://ec.europa.eu/information_society/research/index_en.htm.
[31] http://cordis.europa.eu/fp7/ict.

CORDIS is the official portal for participating in FP7 and subsequent related developments in European science and technology.[32]

## European Security Research Programme (ESRP)

The goal of European security research is to make Europe more secure for its citizens while increasing its industrial competitiveness. By co-operating and coordinating efforts on a European scale, the EU can better understand and respond to risks in a constantly changing world.[33] For projects in the field of security research, the following priority missions were identified:

- Optimizing the security and protection of networked systems;
- Protecting CI against terrorism (including bio-terrorism and incidents involving biological, chemical, and other substances);
- Enhancing crisis management (including evacuation, search and rescue operations, control, and remediation);
- Achieving interoperability and integration of systems for information and communication;
- Improving situation awareness (e.g., in crisis management, anti-terrorism activities, or border control).[34]

Furthermore, the EU Commission set up the European Security Research Advisory Board (ESRAB) on 1 July 2005. ESRAB was attached to the EU Commission and could be consulted on any questions related to the content and implementation of the European Security Research Program. ESRAB carried out its work in full awareness of the European policy context, in particular of the research and development activities carried out at the national level and in

[32] See: http://cordis.europa.eu/ for general overview and http://cordis.europa.eu/ist/ for IST and http://cordis.europa.eu/fp7/ict/ for ICT, respectively.

[33] http://ec.europa.eu/enterprise/security/index_en.htm.

[34] http://cordis.europa.eu/fetch?CALLER=NEWS_SECURITY&ACTION=D&RCN=23324& DOC=6&CAT=NEWS&QUERY=1.

support of European research policy initiatives.[35] ESRAB published its final report on 22 September 2006 and ceased its activities on 31 December 2006.[36] In this report, it recommended the creation of the European Security Research and Innovation Forum (ESRIF) to foster greater dialog and a shared view of European security needs.[37] In the following, the creation of ESRIF was announced at the 2nd European Conference on Security Research in March 2007, and the forum was established as a public-private dialog in security research in September of the same year.

The main objective of ESRIF is the development of a mid- and long-term Joint Security and Research Agenda that will link security research with security policy-making and its implementation.[38] Based on the understanding that research and public-private partnerships have a role to play in protecting critical infrastructures, the aims of the ESRIF program are:[39]

- To bring together all the relevant stakeholders in order to discuss issues of cross-cutting and common concern;
- To identify proposals for forming a strategic security research and innovation agenda, involving national and European stakeholders, laying out a shared and clear view of European security research needs and priorities; and
- To share ideas, views, and best practices in order to make better use of existing capabilities and to enhance the use of technology in security-related domains.

One main focus of ESRIF is critical information protection. ESRIF is supposed to present a Joint Research Agenda towards the end of 2009, when the forum will be terminated.

[35] Official Journal of the European Union. Commission Decision of 22 April 2005 establishing the European Research Advisory Board (2005/516/EC).

[36] http://ec.europa.eu/enterprise/security/articles/article_2006-04-06_en.htm.

[37] http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/07/346&format=HTML&aged=0&language=EN&guiLanguage=en.

[38] http://www.esrif.eu/objectives.html.

[39] http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/07/346&format=HTML&aged =0&language= EN&guiLanguage=en.

## Critical Information Infrastructure Research Co-ordination (CI2RCO)

The EU has set up a task force[40] to explore the measures taken by its 25 member states to combat (cyber-) threats against critical infrastructure. As part of the EU's CI2RCO (Critical Information Infrastructure Research Coordination) project, announced in April 2005, the task force aims to identify research groups and programs focusing on IT security in critical infrastructures, such as telecommunications networks and power grids. The scope of the cooperation goes beyond the EU; the task force also wants to include the US, Canada, Australia, and Russia. The CI2RCO project was a Co-ordination Action co-funded under the IST FP6. The main objectives of the CI2RCO project are:[41]

- To encourage a coordinated Europe-wide approach for research and development on CIIP;
- To establish a European Research Area (ERA) on CIIP as part of the larger IST strategic objective of integrating and strengthening the ERA in terms of dependability and security.
- CI2RCO focuses on activities and actions across the EU-25 and associate candidate countries. Among other information, the CI2RCO website features the European CIIP Newsletter and upcoming events in the area of CIIP.[42]

[40] The European task force includes the Fraunhofer Institute for Secure Information Technology (FhG-SIT); the German Aerospace Center (DLR); the Industrieanlagen-Betriebsgesellschaft (IABG) company; the Italian National Agency for New Technologies, Energy and the Environment (ENEA); the Netherlands Organization for Applied Scientific Research (TNO); the École Nationale Supérieure des Télécommunications; and consulting firm Ernst Basler+Partner.

[41] http://www.attrition.org/pipermail/isn/2005-April/001454.html.

[42] http://www.ci2rco.org/index.asp.

## Service and Software Architectures, Infrastructures, and Engineering

In its Research Framework Programme 7, the European Commission will also provide substantial funding for research into service and software architecture, infrastructure, and engineering. This objective integrates research activities in the areas of services, software, grid, and virtualization technologies.[43] The challenge in achieving pervasive and trusted network and service infrastructures is to look at the converged communication and service infrastructure that will gradually replace the current internet, mobile, fixed, and audiovisual networks. The objective of this research project integrates and builds on the achievements of related work from the IST Programme in FP6. The integrated research effort aims at bringing in world-class participants including European industry, small- and medium-size enterprises, universities, and research institutes, each of which are to contribute their specific skills to ensure success.[44]

## Law and Legislation

In its legislation on CIIP, the EU went back to the basic principles already enshrined in European law, particularly with regard to the confidentiality of communications and the legal conditions for interception, traffic data retention, legality of content, or intellectual property.[45]

[43] http://cordis.europa.eu/fp7/ict/ssai/home_en.html.

[44] http://cordis.europa.eu/fp7/ict/ssai/overview_en.html.

[45] Alain Esterle, Hanno Ranck, and Burkard Schmitt (edited by Burkard Schmitt). "Information security. A new challenge for the EU". Chaillot Paper no. 76 (Paris, March 2005). http://www.iss.europa.eu/uploads/media/cp076.pdf. Overview of all legislative documents on EU data protection: http://ec.europa.eu/information_society/policy/ecomm/info_centre/documentation/legislation/index_en.htm, and http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm. Website of the EU Commission on Data Protection: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm.

## Data Protection Directive 1995

The Data Protection Directive (95/46/EC)[46] provides a regulatory framework to guarantee the secure and free movement of personal information across the national borders of EU member countries, and also establishes a baseline of security controls protecting this information.[47] The Data Protection Directive requires that any third country to which data is transferred provide "adequate" data protection.[48]

## Directive on Electronic Signature 1999

In to the area of e-Commerce, the Directive on Electronic Signatures (1999/93/CE)[49] has been duly incorporated into the national legislation of member states. This directive outlines requirements for certificates, certification service providers, and secure signature-creation devices, and provides recommendations for secure signature verification. The directive recognizes the potential variety of technologies used to generate signatures, but does not establish detailed technical standards or propose best practices. It also lays the groundwork for the international recognition of certificates.

## Directive on Privacy Protection in the Electronic Communications Sector 2002

Directive 95/46/EC has been complemented by Directive 97/6650 on the protection of personal data in the field of telecommunications and, of even

[46] http://europa.eu/scadplus/leg/en/lvb/l14012.htm. Status of implementation of Directive 95/46: http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm.

[47] Report on the Economic Evaluation of the Data Protection Directive 95/46/EC: http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/economic_evaluation_en.pdf.

[48] Cf. the US Safe Harbor Arrangement as a streamlined process for US companies to comply with the directive, developed by the US Department of Commerce in consultation with the EU. http://www.export.gov/safeharbor/.

[49] http://ec.europa.eu/information_society/eeurope/2002/action_plan/pdf/esignatures_en.pdf.

[50] http://www.spamlaws.com/f/docs/97-66-ec.pdf.

greater relevance, by the EU Directive on Privacy Protection in the Electronic Communications Sector (2002/58/CE).[51]

The directive clarifies policies on spamming, electronic data collection, and retention by requiring the member countries to adopt legislation providing data confidentiality, limiting the traffic data storage, and providing exceptions for reasons of national security. Moreover, the directive specifies that traffic data is to be deleted or depersonalized as soon as it is no longer needed for sending or preparing invoices, but nonetheless allows member states the possibility "of adopting legislative measures providing for the retention of data for a limited period".[52] These measures must be "appropriate or proportionate, within a democratic society, to safeguard national security, defense, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of electronic communication systems".[53]

## Framework Directive 2002

The objective of the Framework Directive (2002/21/EC)[54] is to establish a harmonized framework for the regulation of electronic communications networks and services. It lays the foundation in the form of horizontal provisions serving the other measures: the scope and general principles, basic definitions, general provisions on the national regulatory authorities, the new concept of significant market power, and rules for granting certain indispensable resources such as radio frequencies or rights of way.

[51] http://www.jura.uniaugsburg.de/prof/moellers/materialien/materialdateien/010_europaeische_gesetze/eu_richtlinien/ril_2002_058_eg_datenschutz_en/.

[52] Ibid., Article 15.

[53] Ibid., Article 15.

[54] http://www.bipt.be/ShowDoc.aspx?objectID=1020&lang=en.

## Council Framework Decision on Attacks Against Information Systems 2005

The European Council Framework Decision on attacks against information systems (2005/222/JHA)[55] of February 2005 aims to strengthen criminal judicial cooperation on attacks against information systems by developing effective tools and procedures. The criminal offences punishable under the framework decision are: illegal access to information systems, illegal system interference (the intentional serious hindering or interruption of the functioning of an information system by inputting, transmitting, damaging, deleting, degrading, altering, suppressing, or rendering inaccessible computer data) and illegal data interference. The member states will have to make provisions for such offences to be punished by effective, proportionate, and dissuasive criminal penalties. To enhance cooperation, the member states must establish operational points of contact that are available 24 hours a day and seven days a week.

## Directive on Data Retention 2006

In March 2006, the European Parliament and the Council enacted the Directive on the Retention of Data processed in connection with the provision of public electronic communication services or of public communications networks (2006/24/EC, following Commission proposal COM(2005)0438).[56] The directive is designed to harmonize member states' national legislation on the retention of

[55] http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2005/l_069/l_06920050316en00670071.pdf.

[56] This directive amends Directive 2002/58/EC: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri= OJ:L:2006:105:0054:0063:EN:PDF.
Member states had to transpose the requirements of the Directive into national laws by 16 September 2007; however, a grace period of 18 additional months is available. Until 15 March 2009, each member state may postpone application of the Directive to the retention of communications data relating to internet access, internet telephony, and e-mail. Any member state that intends to make use of this provision must notify the Council and the Commission to that effect by way of a declaration. The following member states have made such a declaration postponing application for differing lengths of time: the Netherlands, Austria, the United Kingdom, Estonia, Cyprus, Greece, Luxembourg, Slovenia, Sweden, Lithuania, Latvia, the Czech Republic, Belgium, Poland, Finland, and Germany.

telephone and e-mail data for investigating, detecting, and prosecuting serious crime, as defined by each member state in its national law. The directive applies to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user. It does not apply to the content of electronic communications, including information consulted using an electronic communications network. Member states must ensure that communications providers retain communication data for periods of not less than six months and not more than two years from the date of the communication. The measures, drafted by the United Kingdom after the London terrorist bombings in July 2005, require companies to keep a wide range of data, including incoming and outgoing phone numbers; the duration of phone calls; data that can be used to trace fixed or mobile telephone calls; information about text messages; IP addresses, which identify a computer's coordinates on the internet; login and logoff times; and details of e-mail traffic – but not the actual content of communications.[57] Details of connected calls that are unanswered, which can be used to send signals to accomplices or to detonate bombs, will also be archived where that data exists. Independent authorities will be designated to monitor the use of the data, which will have to be deleted at the end of the period unless it is kept for anti-terror investigation purposes.[58]

No later than 15 September 2010, the European Commission is required to submit an evaluation of the application of the Directive and its impact on economic operators and consumers, taking into account further developments in electronic communications technology and the statistics provided to the Commission with a view to determining whether it is necessary to amend the

[57] The following categories of data must be retained with regard to fixed network telephony and mobile telephony, as well as internet access, e-mail, and internet telephony (see Article 5 of the Directive): (a) data necessary to trace and identify the source of a communication; (b) data necessary to trace and identify the destination of a communication; (c) data necessary to identify the date, time and duration of a communication; (d) data necessary to identify the type of communication; (e) data necessary to identify the communication device; (f) data necessary to identify the location of mobile communication equipment.

[58] Each member state must designate a supervisory authority to be responsible for monitoring the application within its territory of the provisions adopted by the member states regarding the security of the stored data (see Article 9 of the Directive). Those authorities may be the same authorities as those referred to in Article 28 of Directive 95/46/EC. The supervisory authority must act with complete independence.

provisions of this Directive, in particular with regard to the list of data and the periods of retention.

## Treaty of Lisbon 2007

The Treaty of Lisbon, signed by the heads of state or government of the 27 member states in Lisbon on 13 December 2007, which was scheduled to enter into force on 1 January 2009 in order to reform the EU's constitutional framework, includes provisions for the protection of personal data.[59] The treaty reaffirms the "right to the protection of personal data" (Art. 16 B of the Treaty of Lisbon). Moreover, it states that the European Parliament and the Council shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by EU institutions, bodies, offices, and agencies, and by the member states when carrying out activities that fall within the scope of EU law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities. As an annex, the Declaration on Article 16 B of the Treaty on the Functioning of the European Union (No. 20) states that whenever rules on the protection of personal data could have direct implications for national security, due account will have to be taken of the specific characteristics of the matter. The Declaration on the Protection of Personal Data in the Fields of Judicial Cooperation in Criminal Matters and Police Cooperation (No. 21) acknowledges that specific rules on the protection of personal data and the free movement of such data in the fields of judicial cooperation in criminal matters and police cooperation may be necessary because of the specific nature of these fields.

[59] Full text of the Treaty of Lisbon (also known as "the Reform Treaty"): http://europa.eu/lisbon_treaty/full_text/index_en.htm.

# The Forum of Incident Response and Security Teams (FIRST)

FIRST is the global Forum for Incident Response and Security Teams. The organization is widely recognized as a global leader in incident response and brings together a variety of Computer Security Incident Response Teams (CSIRTs) from government, commercial, and education organizations. FIRST aims to foster cooperation and coordination in incident prevention, to stimulate rapid reaction to incidents, and to promote information-sharing among members and the community at large. FIRST's vision is that membership should enable incident response teams to respond more effectively to security incidents by providing best practices, tools, and trusted communication with member teams. FIRST's mission statement, which was originally adopted in 1995 and reissued in an updated version in June 2003, holds that FIRST is an international confederation of trusted CSIRTs that cooperatively handle programs to prevent computer security incidents. Moreover,

- FIRST members develop and share technical information, tools, methodologies, processes, and best practices;
- FIRST encourages and promotes the development of quality security products, policies, and services;
- FIRST develops and promulgates best computer and security practices;
- FIRST promotes the creation and expansion of incident response teams and membership from organizations around the world;
- FIRST members use their combined knowledge, skills, and experience to promote a safer and more secure global electronic environment.[1]

[1] http://www.first.org/about/mission/mission.html.

## FIRST History

FIRST was formed in 1990 in response to the occurrence of major incidents – a computer security incident known as the "internet worm", which brought the internet to its knees in 1988, and the "WANK worm", which highlighted the need for better communication and coordination in 1989. Since that time, it has continued to grow and evolve in response to the changing needs of incident response and security teams and their constituencies. By now, most companies rely on the internet in their daily business transactions. Incident response and security teams continue to form around the globe, covering the growing range of constituencies and member teams of FIRST, including entire countries as well as multi-national organizations and teams from educational and commercial establishments, vendors, the government, and the military.[2]

## Organization

FIRST consists of a network of individual CSIRTs that work together voluntarily to deal with computer security problems and their prevention. It operates under a formal Operational Framework that describes the governing principles and operating rules for the organization.[3] FIRST exercises no authority over the organization and operation of individual member teams. The general coordination of FIRST activities is provided by the Steering Committee, the Board of Directors, and the Secretariat. Every year, FIRST holds general meetings where members are expected to be represented and the Steering Committee members are elected. In order to address specific topics, special meetings can be called by the chair of the Steering Committee.

There are two types of participants in FIRST. The full members represent organizations that assist an information technology community or another defined constituency in preventing and handling computer-related incidents. Liaison members are individuals or representatives of organizations other than incident response or security teams that have a legitimate interest in and value to FIRST.[4]

[2] http://www.first.org/about/history.

[3] http://www.first.org/about/policies/index.html.

[4] http://www.first.org/members/index.html. For a comprehensive membership list, see: http://www.first.org/members/teams/index.html.

## Global Initiatives

FIRST is the only worldwide global CSIRT forum, and its members are experts from across the field and from all over the world. With its global scope and its heterogeneous character, FIRST supports and collaborates with existing initiatives to communicate with CSIRT members. As a global umbrella organization, it strives to bring together a wide variety of collaborative and cooperative approaches of the multiple disciplines involved in computer and network security incident response.[5]

Mainly, FIRST's global initiatives are introduced in Special Interest Groups (SIG) and in the Corporate Executive Programme (CEP). SIGs exist to provide a forum where FIRST members can discuss topics of common interest to the incident response community. A SIG is a group of individuals composed of FIRST members and invited parties, typically coming together to explore an area of interest or specific technology area, with the goal of collaborating and sharing expertise and experiences to address common challenges. SIGs generate papers and publications for the industry covering their area of interest. While these papers and publications are distributed by FIRST, they do not represent the official position of the FIRST members, or of FIRST itself.[6]

In June 2005, the board and membership of FIRST agreed to fund and establish a unique Corporate Executive Programme (CEP). The aim of the CEP is to bring together cross-functional senior executives with responsibility for decision-making in their organizations. The program caters for heads of departments in HR, finance, operations, technology, security, sales and marketing, research, logistics, legal affairs, and other key business disciplines in all sectors – public and private – across all global regions. The program aims to provide an environment where business leaders can fully appreciate the nature of future threats and risks that global organizations will be facing in the years ahead.[7]

[5] http://www.first.org/global.

[6] http://www.first.org/global/sigs.

[7] http://www.first.org/global/cep/index.html/ and http://www.globalcep.com.

# Group of Eight (G8)

Since 1995, the Group of Eight (G8) has become increasingly involved in issues relating to cyber-crime, the Information Society, and Critical Infrastructure Protection. At the Halifax summit in 1995, a group of senior experts was set up with the task of reviewing and assessing existing international agreements and mechanisms to fight organized crime. This G8 Senior Experts Group took stock extensively and critically before drawing up a catalog of 40 operative recommendations. These recommendations were approved at the G8 summit in Lyon in 1996. The G8 Senior Expert Group, known since then as the Lyon Group, was the first international political forum to fully recognize the significance of high-tech crime. The Lyon Group has since developed into a permanent multidisciplinary body with numerous specialized sub-working groups. Since October 2001, the Lyon Group meetings have been held together with the Roma Group dealing with combating terrorism (Lyon/Roma Group).[1]

A further important stage for the G8 and CIP/CIIP came in spring 2000. On 15–17 May 2000, government officials and industry participants from G8 countries and other interested parties attended the G8 Paris Conference on Dialogue Between the Public Authorities and Private Sector on Security and Trust in Cyberspace.[2] The aim was to discuss common problems and to find solutions associated with high-tech crime and the exploitation of the internet for criminal purposes. The G8 member states were convinced that a dialog between governments and the private sector was essential in the fight against the illegal or prejudicial use of ICT, and they agreed on defining a clear and transparent framework for addressing cyber-crime.[3]

[*] The Group of Eight Survey of 2006 was reviewed by Harry Hoverd, Home Office, UK. For this edition, the authors have thoroughly updated the Group of Eight survey by referring to open-source material.

[1] http://www.auswaertiges-amt.de/diplo/de/Aussenpolitik/Themen/TerrorismusOK/TerrorismusbekaempfungG8.html#t2l.

[2] http://www.g8.utoronto.ca/crime/paris2000.htm.

[3] Ibid.

## Okinawa Charter on Global Information Society

The Okinawa Charter on Global Information Society was published in July 2000.[4] The charter states that ICT is one of the most potent forces shaping the 21st century, enabling many communities to address social and economic challenges with greater efficiency. One of the key principles and approaches of the charter is that international efforts to develop a global Information Society must be accompanied by coordinated action to foster a crime-free and secure cyberspace. In this respect, the Okinawa charter refers to the OECD Guidelines for Security of Information Systems.[5] Moreover, in the Okinawa Charter, the G8 asked both the public and private sectors to make efforts to bridge the international information and knowledge gap.

## G8 Principles for Protecting Critical Information Infrastructures

G8 members met in Paris in March 2003 for the first multilateral meeting devoted to CIP/CIIP. Top-level experts from G8 member states, together with the major CIP/CIIP operators (e.g., France Telecom for France) came together to define common principles for the protection of vital CI/CII.[6] The 11 clearly defined CIIP principles were adopted on 5 May 2003 by the G8 justice and interior ministers. They cover the following topics:[7]

- Countries should have emergency warning networks regarding cyber-vulnerabilities, threats, and incidents;
- Countries should raise awareness to facilitate stakeholders' understanding of the nature and extent of their CII, and the role each must play in protecting them;

[4] http://www.g7.utoronto.ca/summit/2000okinawa/gis.htm.

[5] See the survey on the OECD in this volume.

[6] http://www.g7.utoronto.ca/summit/2003evian/press_statement_march24_2003.html.

[7] http://www.usdoj.gov/ag/events/g82004/G8_CIIP_Principles.pdf.

- Countries should examine their infrastructures and identify interdependencies among them, thereby enhancing protection of such infrastructures;
- Countries should promote partnerships among stakeholders, both public and private, to share and analyze information on their critical infrastructure in order to prevent, investigate, and respond to damage to or attacks on such infrastructures;
- Countries should create and maintain crisis communication networks and test them to ensure that they will remain secure and stable in emergency situations;
- Countries should ensure that data availability policies take into account the need to protect critical information infrastructures;
- Countries should trace attacks on critical information infrastructures and, where appropriate, disclose the results to other countries;
- Countries should conduct training and exercises to enhance their response capabilities and to test continuity and contingency plans in the event of an attack on the information infrastructure, and should encourage stakeholders to engage in similar activities;
- Countries should ensure that they have adequate substantive and procedural laws, such as those outlined in the Council of Europe Cybercrime Convention of 23 November 2001, and trained personnel to enable them to investigate and prosecute attacks on critical information infrastructures, and to coordinate such investigations with other countries as appropriate;
- Countries should engage in international cooperation, when appropriate, to secure critical information infrastructures, including by developing and coordinating emergency warning systems, by sharing and analyzing information regarding vulnerabilities, threats, and incidents, and by coordinat-

ing investigations of attacks on such infrastructures in accordance with domestic laws;

- Countries should promote national and international research and development and encourage the application of security technologies that are certified according to international standards.

With the adoption of these principles, the G8 member states suggested that the emergence of a new "security culture" should encourage them to strengthen international co-operation, to implement the best professional practices in the field of computerized surveillance and alert, to conduct common exercises to test the reaction capabilities in case of incidents, to make other countries aware of the problems, and to invite them to adopt the same main courses of action.[8] The 11 principles are intended to guide national responses to CIIP. However, to this end, it is crucial that the principles be communicated to all parties concerned.

The essential elements of the principles of protecting CII were adopted by the 78th United Nations General Assembly.[9] Resolution 58/199 of January 2004, entitled "Creation of a global culture of cyber security and the protection of critical information infrastructures", is complemented by the annex Elements for Protecting CII, which is based on the 11 principles defined by the G8 in 2003.[10]

The G8 justice and home affairs ministers (the ministerial meeting of the Lyon/Roma Group) met in Washington in May 2004 and endorsed Best Practices for Network Security, Incident Response and Reporting to Law Enforcement. This guide assists network operators and system administrators in responding to computer incidents.[11]

[8] "G8 Principles for Protecting Critical Information Infrastructures". In: NISCC Quarterly (April–June 2003), p. 9.

[9] http://www.usdoj.gov/ag/events/g82004/Communique_2004_G8_JHA_Ministerial_051204.pdf.

[10] http://www.itu.int/osg/spu/cybersecurity/docs/UN_resolution_58_199.pdf.

[11] http://www.usdoj.gov/ag/events/g82004/G8_Best_Practices_Network_Security.pdf.

## High-Tech Crime Sub-Group Activities

One of the sub-groups of the Lyon Group, called the High-Tech Crime subgroup, deals with issues concerning CIIP. The sub-group's goal for CIIP work is to find a way to protect the infrastructure that G8 countries are dependent on, and to provide a more unified approach to multinational companies that deal with a number of G8 countries for setting up an international information-sharing mechanism. Furthermore, the High-Tech Crime sub-group is active in a number of areas, including:

- A CIIP handbook of national contact points. This International CIIP Directory is compiled and maintained by CPNI (UK),[12] and its scope is limited to national governmental organizations. The directory is not available publicly, commercially, or to industry (except on government business);
- CIIP conferences;
- A summary of domestic legal frameworks and avenues of co-operation for addressing illegal internet content;
- Best practice for law enforcement in addressing criminal misuse of wireless networks;[13]
- A summary of countries' national legislation regarding law enforcement treatment of encrypted evidence and current trends in criminal use of encryption;
- A standard template for making and responding to requests for 24/7 high-tech investigative assistance;
- A work plan for tackling viruses, worms, and other malicious code.

During its presidency of the G8 for the year 2005, the UK defined the improvement of international co-operation in the field of CIIP as a main objective.

From 15–17 June 2005, a meeting of the justice and home affairs ministers was held in Sheffield. On the basis of this meeting, the justice and home affairs

[12] See the country survey on the UK in this volume.

[13] http://www.homeoffice.gov.uk/documents/G8-WLANBstPrcNov04.pdf?version=1.

ministers published a communiqué on CIIP. The communiqué refers to the Unified Response Tabletop Exercise hosted in New Orleans by the G8 High-Tech Crime sub-group in May 2005, where various experts in law enforcement, watch and warning, and industry met to find solutions to challenges in the field of CIIP. The communiqué also outlines areas where further action is required:

- To continue to enhance communication and information-sharing between watch and warning organizations and law enforcement agencies;
- To ensure that all G8 countries have, and encourage other countries to develop, watch and warning organizations able to detect vulnerabilities and threats;
- To ensure that law enforcement agencies can quickly respond to serious cyber-threats and incidents;
- To continue and strengthen cooperation with the private sector;
- To continue to conduct national and multinational training and exercises.

At the same meeting in Sheffield in June 2005, the High-Tech Crime sub-group released a further paper on Best Practices for Law Enforcement Interaction with Victim-Companies During a Cyber-Crime investigation.[14]

[14] http://www.libertysecurity.org/article396.html.

# North Atlantic Treaty Organization (NATO)

Critical Infrastructure Protection remains one of the key areas of work of the Civil Emergency Planning in NATO. The Ministerial Guidance for NATO Civil Emergency Planning (CEP) for 2007–2008 includes several references to critical infrastructure protection, while the Updated Civil Emergency Planning Action Plan for the improvement of civil preparedness against possible chemical, biological, radiological, and nuclear (CBRN) attacks includes several action items related to the CIP field of work. In line with the Concept Paper approved in 2003, the Senior Civil Emergency Planning Committee (SCEPC) and its eight Planning Boards and Committees (PB&Cs) will continue to examine critical infrastructure protection from a functional perspective, and to provide integrated contributions from the areas of expertise of all Planning Boards and Committees.

## Civil Communication Planning Committee (CCPC)

The Civil Communication Planning Committee (CCPC) is responsible for reviewing existing and planned electronic public and non-public communications infrastructures, services, associated facilities, postal services, and any related services with a view to determining their ability to meet the requirements of all vital users (civil and military) during emergencies. Recommendations are made to nations, taking into consideration new and emerging technology, national

* This chapter was reviewed by Dr Denisa-Elena Ionete, Civil Emergency Planning, NATO Headquarters, Brussels.

legislation and arrangements, and the role of international organizations in this field.

The CCPC has published a number of documents and studies on civil communications infrastructures, such as

- Critical telecommunications infrastructure protection;[1]
- CEP consequences of disruption of critical postal infrastructure;[2]
- New risks and threats to civil telecommunications;[3]
- CEP requirements for coordinated national telecommunications regulatory measures;
- New risks and threats to the postal services.[4]

In addition, the CCPC has contributed to the "North Atlantic Council's Action Plan on Cyber Defense", such as:

- CEP consequences of the introduction of the Computer Emergency Response Teams (CERTs)/CEP regarding cyber-attacks and information warfare on critical civil communication infrastructure;
- Identification and assessment of the interdependencies of other critical infrastructures on civil communication networks;
- Impact of Information Society developments and related opportunities for NATO CEP.

The Bucharest Summit declaration of 2008 in its paragraph 47 states that "NATO remains committed to strengthening key Alliance information systems against cyber attacks. We have recently adopted a Policy on Cyber Defence and are developing the structures and authorities to carry it out. Our Policy on Cyber Defence emphasis the need for NATO and nations to protect key information systems in accordance with their respective responsibilities; share best practices, and provide a capability to assist Allied nations, upon request, to counter a cyber attack. We

[1] NATO document: EAPC(CCPC)D(2002)8.

[2] NATO document: EAPC(CCPC)D(2003)2.

[3] NATO document: EAPC(CCPC)WP(2002)1, REV1.

[4] NATO document: EAPC(CCPC)D(2003)1.

look forward to continuing the development of NATO's cyber defence capabilities and strengthening the linkages between NATO and national authorities"[5]. On 15 May 2008, at the initiative of Estonia, top military commanders from seven NATO countries and the Allied Command Transformation signed an agreement to create a Cooperative Cyber Defense Center in Tallinn. The cyber-attacks on Estonia in 2007 highlighted for the first time the potential vulnerability of NATO countries, their institutions and societies, an even NATO itself to disruption by penetration of their information and communication systems.[6] The goal of NATO policy and of the center is to assist allied countries as needed in protecting their critical communication and information networks.[7]

## Civil Protection Committee (CPC)

The work of the Civil Protection Committee (CPC) in the CIP field started in 2001, when an Ad Hoc Group (AHG) on CIP was established. One of the first tasks of this AHG was to conduct a mapping survey of critical infrastructure. Nations were invited to indicate how they were structurally organized to deal with critical infrastructure protection, and to give indications about their state of readiness in terms of planning and infrastructure mapping.[8] Based on this initial mapping, definitional and conceptual work was undertaken by the AHG on CIP, resulting in a Critical Infrastructure Protection Concept Paper, approved by the SCEPC on 6 November 2003.

The Concept Paper not only proposed a way for work to be carried out by the CPC in this field, but also contained a road map detailing immediate, mid-term, and long-term actions. Also attached were a scenario to further explain the concept and a glossary of frequently-used CIP terms.

[5] Bucharest Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Bucharest on 3 April 2008. http://www.summitbucharest.ro/en/doc_201.html.

[6] For more information about these incidents, see the chapter on Estonia.

[7] Vladimir Socor. "NATO creates Cyber Defense Center in Estonia". Eurasia Daily Monitor, Vol. 5, No. 93 (15 May 2008). http://www.jamestown.org/edm/article.php?article_id=2373060.

[8] NATO document: EAPC(CPC)N(2002)6.

In 2005, the CPC conducted a seminar on the theme of Critical Infrastructure Protection (CIP) – Education, which aimed to raise awareness of the importance of CIP. The primary results expected from the seminar were sets of teaching points that could form part of a CIP course curriculum and recommendations for next steps regarding the CIP concept. The AHG is considering ways to develop further training and education activities on the basis of the seminar outcomes.[9]

Among other training activities, the CPC in 2007 organized a table-top exercise attended by representatives of more than 20 NATO, Euro-Atlantic Partnership Council (EAPC), Mediterranean Dialogue (MD), and Istanbul Cooperation Initiative (ICI) countries and by representatives of NATO Military Authorities. The exercise aimed at increasing the understanding of:

- The vulnerabilities of and interdependencies between various critical infrastructures, including energy-related critical infrastructures;
- The bottlenecks that arise in decision-making at the national and international levels;
- The best practices in disaster response with regard to CIP.

In early 2008, the AHG was reorganized. Its work priorities over the next two years will be to update the Road Map and, if needed, the Concept Paper; to set up an information exchange tool to be used by different civil emergency planning stakeholders and to step up the work on addressing CIP interdependencies.[10]

## Industrial Planning Committee (IPC)

In 2003, an Industrial Planning Committee (IPC) seminar in Slovakia was attended by senior officials and representatives from EAPC governments, industry, and trade. The aim of the seminar was to examine industrial interdependencies and resulting vulnerabilities, and to discuss potential preventive and/or consequence-management measures. These issues were introduced by plenary presentations,

[9] Information provided by an expert.
[10] Information provided by an expert.

including two case studies – a Canadian paper on industrial interdependencies and a Slovak case study on aspects of electricity, water, gas, and chemical utilities. Other presentations looked at

- Preventive measures for the protection of critical infrastructure;
- The military experience in infrastructure protection in France;
- Protecting critical infrastructure during disasters.

Following this initial seminar, and based on a questionnaire circulated in April 2003[11] and replies to it,[12] the IPC agreed to develop a guide containing criteria for identifying critical infrastructure in industry and the energy sector, and to compile active and passive methods of critical infrastructure protection. The IPC also established an Ad-Hoc Working Group on Energy CIP (AHWG) for appropriate action. The group agreed that energy-related CI consists of three main infrastructures:

- Systems of electricity generation, transmission, and delivery;
- Systems of natural gas production, transmission, and delivery; and
- Systems of oil production, transportation, refining, and delivery.

The IPC initially concentrated on the protection of critical electricity infrastructure. In 2005, it held a seminar on the topic of Protection of Electricity-Related Critical Infrastructure against Security Related Hazards". Subsequently, in October 2006, the IPC Vital Resources Seminar on Energy Critical Infrastructure Protection was held. Drawing on the discussions and recommendations of the seminar, the committee has compiled a collection of best practices on the protection of energy CIP as well as on the protection of electricity CIP. In 2007, the IPC seminar addressed the issue of CIP related to gas deliveries. A collection of best practices on protecting critical gas-related infrastructures is currently being drafted.[13]

[11] NATO document: EAPC(IPC)N(2003)6.

[12] NATO document: EAPC(IPC)WP(2003)2.

[13] Information provided by an expert.

The Bucharest NATO Summit Declaration states in Paragraph 48: "We have noted a report 'NATO's Role in Energy Security', prepared in response to the tasking of the Riga Summit. Allies have identified principles which will govern NATO's approach in this field, and outlines options and recommendations for further activities. Based on these principles, NATO will engage in the following fields: information and intelligence fusion and sharing; projecting stability; advancing international and regional cooperation; supporting consequence management; and supporting the protection of critical energy infrastructure".[14]

## Food and Agriculture Planning Committee (FAPC)

The Food and Agriculture Planning Committee (FAPC) looks at the impact of CIP on food, agriculture, and water production. In particular, the FAPC looks at threats, risks, and vulnerabilities affecting the water sector. In doing so, the FAPC has chosen a multi-disciplinary training approach, which will make better use of the wealth of knowledge of all NATO experts by bringing them together to work on this subject under exercise conditions. Other planning boards and committees, particularly the Transport and Telecommunications Committees, work jointly with the FAPC.

## Civil Aviation Planning Committee (CAPC)

The Civil Aviation Planning Committee (CAPC) has begun identifying critical infrastructure vulnerabilities and possible protective measures in the area of civil aviation. While the protection of airports, equipment, and resources is primarily a national responsibility, the Civil Aviation Working Group has discussed minimum standards that can help to make national efforts more effective. Any large-scale military deployment would require the transport capabilities of the civil

[14] Bucharest Summit Declaration, op. cit.

aviation sector and the related infrastructure elements, which together with the air traffic control network, the power grid, fuel supplies, and supporting surface transportation are essential parts of NATO's deployment capability.

## Planning Board for Inland Surface Transportation (PBIST)

The Planning Board for Inland Surface Transportation (PBIST) has conducted exploratory and definitional work on problems that may result from attacks on critical inland surface transport infrastructure. A PBIST report emphasizes that the civilian transport infrastructure is considered an attractive target, as global trade depends heavily on transportation.[15] The report aims to reach conclusions on threats to the inland transport infrastructure, characteristics of likely targets, possible protective measures, and the potential role of the PBIST.

## Planning Board for Ocean Shipping (PBOS)

At the behest of the NATO Council and the SCEPC, the Planning Board for Ocean Shipping (PBOS) continues to serve as the NATO focal point for advice and assistance on the protection of civilian maritime assets against acts of terrorism. This work includes: monitoring the work and activities of other international bodies, gathering and exchanging information from international and national sources, and providing advice and assistance as necessary.

## Coordination

Overall responsibility for coordinating CIP work lies with the SCEPC. However, on the initiative of the CPC, representatives of the Planning Boards & Committees

[15] NATO document: EAPC(PBIST)D(2003)8.

(PB&Cs) meet on a regular basis to discuss various issues related to CIP. These meetings are an opportunity for all PB&Cs to present work that is under way and/or planned within their respective areas of interest, in addition to fostering closer cooperation and coordination.

## Special Report to the NATO Parliamentary Assembly 2007

Lord Jopling from the United Kingdom was nominated Special Rapporteur and delivered a report on the protection of critical infrastructures[16] to the NATO Parliamentary Assembly in the 2007 annual session. This report strives to outline the critical infrastructure policies of NATO and also of its individual member countries. It collects the various definitions, highlights their commonalities and differences, and tries to attribute responsibilities by identifying the CIP stakeholders and the sectoral policies including CIIP; energy security, civil aviation security, and port security.

[16] http://www.nato-pa.int/default.asp?SHORTCUT=1165.

# Organisation for Economic Co-operation and Development (OECD)

The Organisation for Economic Co-operation and Development (OECD) has a long history and expertise in developing policy guidance for the security of information systems and networks, including critical information infrastructures. The OECD is also committed to the fight against cyber-crime; notably, it fights against the use of malicious software. The OECD produces analytical reports, statistics, and policy guidance (declarations and recommendations) to help governments and businesses develop consistent policies to strengthen information security, to raise public awareness about the importance of information security for the internet economy, and, more broadly, to develop a culture of security across society. There is a consensus among the member countries that secure and reliable (information) infrastructures and services are a necessary requirement for trustworthy e-Commerce, secure transactions, and personal data protection. This is the main reason why the OECD Working Party on Information Security and Privacy (WPISP) promotes a global approach to policy-making in these areas to help build trust online.[1] In addition, the Committee for Information, Computer and Communications Policy (ICCP) analyzes the broad policy framework underlying the e-Economy, information infrastructures, and the Information Society.[2]

[*] The OECD Survey of 2008 was reviewed by Anne Carblanc, OECD.

[1] http://www.oecd.org/document/46/0,3343,en_2649_34255_36862382_1_1_1_1,00.html.

[2] http://www.oecd.org/department/0,2688,en_2649_34223_1_1_1_1_1,00.html.

## OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security

The attacks of 11 September 2001 in the US marked a turning point for the OECD's efforts for information security and CIIP. In order to improve measures against cyber-crime, computer viruses, and hacking, the OECD drew up new guidelines. At its 1037th session on 25 July 2002, the OECD Council adopted the new Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security.[3] The guidelines are not binding. However, they are the result of a consensus between OECD governments and of discussions involving representatives of the information technology industry, business users, and civil society.[4] The OECD invites governments in other countries to adopt a similar approach to CIIP. Furthermore, the private-sector representatives are asked to improve security in their own environment and to provide security information and updates to the users. The individual users are urged to be more aware and responsible, and also to take the best preventive measures possible to decrease the risks to CI/CII. The OECD Guidelines include the following complementary principles at the policy and operational levels:[5]

1) Awareness: Participants should be aware of the need for security of information systems and networks and of options to enhance security;
2) Responsibility: All participants are responsible for the security of information systems and networks;
3) Response: Participants should act in a timely and co-operative manner to prevent, detect, and respond to security incidents;
4) Ethics: Participants should respect the legitimate interests of others;

[3] http://www.oecd.org/document/42/0,2340,es_2649_34255_15582250_1_1_1_1,00.html.

[4] http://www.oecd.org/dataoecd/23/11/31670189.pdf.

[5] OECD. "Guidelines for the Security of Information Systems and Networks. Towards a Culture of Security", (2002), pp. 10ff. http://www.ftc.gov/bcp/conline/edcams/infosecurity/popups/OECD_guidelines.pdf.

5) Democracy: The security of information systems and networks should be compatible with the essential values of a democratic society;
6) Risk assessment: Participants should conduct risk assessment;
7) Security design and implementation: Participants should incorporate security as an essential element of information systems and networks;
8) Security management: Participants should adopt a comprehensive approach to security management;
9) Reassessment: Participants should review and reassess the security of information systems and networks and make appropriate modifications to security policies, practices, measures, and procedures.

## OECD Guidelines for the Protection of Critical Information Infrastructures

In 2008, the OECD Council plans to adopt a Recommendation on the Protection of Critical Information Infrastructures (CII).[6] This document highlights the relevance of the Security Guidelines to CII. It provides guidance on national policies and proposes ways to improve international cooperation for the protection of CII. The guidance derives from best practices identified in an OECD comparative study of CII policies in seven countries.

The recommendation identifies the need for strengthened international cooperation to address cross-border issues, given the importance of the internet as a global infrastructure. It also identifies the need for a national operational infrastructure security capability, a willingness and ability to share information, close cooperation with the relevant parts of the private sector, and a strong culture of security in the face of rapid technological growth and consequential social

[6] The expression CII used in the OECD recommendation refers to those information networks and systems the failure of which would have a serious impact on the health, safety, security, and economic well-being of citizens, or the effective functioning of government or the economy. The adoption of this document is planned for the OECD Ministerial Meeting on the Future of the Internet Economy in Seoul, Korea, 16–18 June 2008. http://www.biac.org/members/iccp/mtg/2008-06-seoul-min/seoul2008_ministerial_documents.asp.

changes. The recommendation therefore calls on member countries to adopt a common approach in a number of areas to enable progress on some of these issues. Further, although the recommendation is addressed to governments, it stresses the need for collaboration with the private sector.

The OECD recommendation is timely. First, critical infrastructures are increasingly interdependent and reliant on the effective functioning of information and communication technologies. For example, the monitoring and control systems of power grids and hydroelectric power plants are often dependent on the functioning of underlying internet protocol-based networks. Further, most industrial control systems that monitor and control critical processes are now increasingly being connected directly or indirectly (through corporate networks) to the internet and therefore face a new set of threats. Also, as shown in the OECD-APEC Analytical Report on Malware,[7] there is increasing malicious activity online, which adversely affects all internet users and activities, and unfortunately, critical information systems have not proven immune to this phenomenon.[8]

## Culture of Security Website

In December 2003, the OECD launched the Culture of Security website as part of the organization's initiative to promote a global culture of security. The site primarily provides member and non-member governments with an international information-exchange tool on initiatives to implement the OECD Security Guidelines. The OECD website provides an overview of:[9]

- OECD work in the area of security of information systems and networks since the adoption of the Security Guidelines in 2002;
- National implementation initiatives: Activities in various countries to apply the OECD Security Guidelines at the national level;
- Selection of practical tools: Countries are developing various useful tools to encourage awareness, education, and individual responsibility;

[7] http://www.oecd.org/dataoecd/37/60/38738890.pdf.

[8] Information provided by an expert.

[9] http://webdomino1.oecd.org/COMNET/STI/IccpSecu.nsf?OpenDatabase.

- International co-operation: Action taken by governments and international organizations at the regional or international levels to co-operate among themselves and/or with other participants.

## OECD Forums and Workshops

Other OECD efforts concerning CIIP included the OECD-APEC Global Forum on Policy Frameworks for the Digital Economy, held in Honolulu in January 2003, and the OECD Global Forum on Information Systems and Network Security, which was convened in Oslo in October 2003.[10] The Honolulu Forum emphasized the importance of the security of information systems and networks, as well as the need for the OECD to implement the OECD Security Guidelines. Furthermore, it emphasized the importance of preparing for the World Summit on the Information Society (WSIS) in December 2003 in Geneva (Switzerland). Many Asia-Pacific Economic Cooperation (APEC) member countries were invited to the Oslo conference due to an agreement made in Honolulu to increase co-operation between the OECD and APEC. This was another major step towards international and transnational management of CIIP efforts.

Among the main intended policy impacts of the Oslo Forum were:

- Raising awareness of the importance of secure information systems and networks for safeguarding critical infrastructures, as well as business and consumer information;
- Increasing knowledge of the OECD Security Guidelines;
- Encouraging the development and the promotion of security architectures that effectively protect the information systems of organizations;
- Exploring the use of technology and security standards in safeguarding IT infrastructures.

[10] http://www.oecd.org/document/38/0,3343,es_2649_34255_16193702_1_1_1_1,00.html.

In September 2005, an OECD-APEC Workshop on Security of Information Systems and Networks was held in Seoul (South Korea). Topics discussed included spyware, reaching out to SMEs and individuals, promoting effective global incident response (e.g., the roles of governments and CERTs/CSIRTs), emerging security threats and the technologies being developed to address them, as well as the role of research and development, and finally, a comparison of legislative and policy approaches to improve the management and security of information systems and networks.[11]

In March 2006, the OECD together with the US National Science Foundation held a workshop on The Future of the Internet in Paris. The event marked the beginning of the project on the future of the internet by the OECD Committee for Information, Computer and Communications Policy (ICCP).[12] Following up on this workshop, in 2007, the OECD again co-organized a workshop together with the US National Science Foundation on the Social and Economic Factors Shaping the Future of the Internet. The goal of this second workshop was the discussion of strategic directions for the future of the internet, from both the technological and the policy viewpoints.[13]

From 16–18 June 2008, ministers, business leaders, technical experts, academics, and civil society representatives from the 30 OECD countries and more than 15 other economies will meet in Seoul, Korea, to discuss the Future of the Internet Economy and agree new ways to improve global dialog, co-ordination, and co-operation on policies and practices to form an enabling environment for the internet economy.

Strengthening the security of the internet and other information systems and networks, including CII, will be one of the key issues addressed at the ministerial meeting.

[11] http://www.oecd.org/document/25/0,2340,en_2649_201185_35481241_1_1_1_1,00.html.

[12] http://www.oecd.org/dataoecd/26/36/37422724.pdf.

[13] http://www.oecd.org/document/4/0,3343,es_2649_34255_39046340_1_1_1_1,00.html.

# United Nations (UN)

Issues related to CIIP have been discussed by the United Nations (UN) and its system of organizations since the end of the 1980s. However, formal CIIP efforts are a more recent phenomenon. Several initiatives have since been undertaken towards better work coordination. Among these are initiatives taken by UN institutions, several UN resolutions, and the results of the World Summit on the Information Society (WSIS).

## UN Institute for Disarmament Research (UNIDIR)

An important first step was the organization of a workshop in July 1999 by the UN Institute for Disarmament Research (UNDIR) in Geneva. The main topic was how to better achieve worldwide information security and assurance in a global digital environment. In this context, a variety of issues, such as the Revolution in Military Affairs (RMA) and the proliferation of offensive tools for attacking information systems and networks, were discussed in Geneva. There was consensus among the participants that the vulnerability of national and international information infrastructures to cyber-attacks was increasing, and that international cooperation had to be improved in order to meet this challenge. One other conclusion was that the issue of CIIP is not only of military or strategic importance, but that it is mainly a political, economic, and social issue.[2] Hence, it is crucial to achieve cooperation between public and private actors as well as between nations.

* The United Nations Survey of 2008 was reviewed by experts from the International Telecommunication Union (ITU).

[2] Dependability Development Support Initiative (DDSI). "International Organisations and Dependability-related Activities", 31 May 2002, p. 66. http://www.ddsi.org/htdocs/DDSI-F/main-fs.htm.

## UN General Assembly Resolutions

In December 2000 and 2001, the 55th and 56th UN General Assemblies issued Resolutions 55/63 and 56/121 on "Combating the criminal misuse of information technologies".[1] This was another important step in the efforts of the UN concerning CIIP. These resolutions emphasize in particular that the Commission on Crime Prevention and Criminal Justice is intended to make law enforcement more efficient and effective. Furthermore, the importance of cooperation among countries and between the public and private sectors was stressed once again. The resolutions also mention the Convention on Cybercrime of the Council of Europe and the work done by the G8 as crucial milestones in the international field.[2]

In December 2002, the 57th UN General Assembly issued Resolution 57/239 on the "Creation of a global culture of cyber-security".[3] This resolution emphasizes that effective cyber-security not only requires action at the governmental level, but must be supported throughout society. Therefore, it points out the different actors responsible in the field of cyber-security, namely, governments, businesses, and other organizations, as well as individual owners and users of information technologies. The resolution further recognizes once more the importance of international cooperation. The annex outlines nine complementary elements required to create a global culture of cyber-security. They range from awareness of the need for security of information systems and networks, to identifying adequate action in the field of CIIP (taking into account ethical and democratic principles), to security management and reassessment.[4]

In December 2003, the 28th UN General Assembly issued Resolution 58/199 on the "Creation of a global culture of cyber-security and the protection of

[1] UN General Assembly Resolution 55/63 and 56/121 (23 January 2002). "Combating the criminal misuse of information technologies". http://www.un.org/documents/.

[2] Ibid.

[3] UN General Assembly Resolution 57/239 (31 January 2003). "Creation of a global culture of cybersecurity". http://www.itu.int/osg/spu/cybersecurity/docs/UN_resolution_57_239.pdf.

[4] Ibid.

critical information infrastructure".[5] This resolution points out the increasing links among most countries' critical infrastructure and the growing number and variety of threats facing them. The resolution's annex outlines 11 principles for protecting CII, which are based on those adopted by the G8 Justice and Interior Ministers in Paris in 2003. The UN General Assembly invites member states and international organizations to consider these principles for protecting CII, as well as to share their best practices and measures that could assist other actors in their efforts to achieve cyber-security. Furthermore, the resolution asks that these principles be taken into account in preparations for the second phase of the World Summit on the Information Society (WSIS) in Tunisia in November 2005. Finally, the UN General Assembly outlines the necessity of involving the developing and the least developed countries in CIIP, which means that that the transfer of information technology and capacity-building efforts need to be strengthened.[6] In the subsequent years, the UN General Assembly regularly adopted a resolution on the "Developments in the field of information and telecommunications in the context of international security".[7] Referring to the earlier resolutions, the member states are repeatedly called upon to promote further the consideration of existing and potential threats in the field of information security, as well as possible measure to limit the threats emerging in the field. Moreover, the secretary-general, with the assistance of a group of experts (to be established by 2009), is requested to continue to study existing and potential threats in the sphere of information security and possible cooperative measures to address them.

In 2005 and 2006, two subsequent resolutions on WSIS were adopted. The first one urges member states to support and actively contribute to the success of the Tunis Summit, as well as its aims and goals. The second one requests that the Economic and Social Council (ECOSOC) oversee the system-wide follow-up

[5] UN General Assembly Resolution 58/199 (30 January 2004). "Creation of a global culture of cybersecurity and the protection of critical information infrastructures". http://www.itu.int/osg/spu/cybersecurity/docs/UN_resolution_58_199.pdf.

[6] Ibid.

[7] Resolutions 59/61 of 3 December 2004, 60/45 of 8 December 2005; 61/54 of 6 December 2006; 62/17 of 8 January 2008. http://www.un.org/documents.

of the Geneva and Tunis outcomes of the summit.[8] Furthermore, it proclaims an annual World Information Society Day (17 May) and calls for an overall review of the implementation of the summit outcomes in 2015.

## UN ICT Task Force

The establishment of the UN ICT Task Force in November 2001, in response to a request by the UN ECOSOC, was a further important step. The task force was mandated to mobilize worldwide support for attaining the Millennium Development Goals with the use of ICT. In April 2004, a seminar on "Policy and security issues in information technology" was held at the UN Headquarters. Part of the seminar series was on policy awareness and training in information technology, organized by the ICT Task Force and the UN Institute for Training and Research (UNITAR).[9] In 2005, the task force published a guide called "Information Insecurity – A Survival Guide to the Uncharted Territories of Cyber-Threats and Cyber-Security".[10] This publication depicts the problem of information insecurity in general, and provides possible solutions for prevention and response to security incidents (including standards and best practices). Moreover, it attempts to create a greater awareness about the growing dangers of cyber-hooliganism, cyber-crime, cyber-terrorism, and cyber-war, which are inherent aspects of the new opportunities (both positive and negative) that have been opened up by new information technologies.[11]

[8] Resolution 59/220 of 11 February 2005, and Resolution 60/252 of 27 April 2006. http://www.un.org/documents.

[9] http://www.unicttaskforce.org/perl/documents.pl?id=1352.

[10] Eduardo Gelbstein and Ahmad Kamal. „Information Insecurity – A Survival Guide to the Uncharted Territories of Cyber-Threats and Cyber-Security", New York, 2002. https://unp.un.org/details.aspx?entry=E04291#.

[11] Ibid.

# The World Summit on the Information Society (WSIS)

Recognizing that confidence and security in the use of information and communication technologies (ICT) are the main pillars of the information society, the first phase of the World Summit on the Information Society (WSIS) in December 2003 urged governments, in cooperation with the private sector, to consider legislation that allows for effective investigation and prosecution of misuse and strengthens institutional support at the international level. As a result, a number of recommendations were made in the WSIS Geneva 2003 first phase Declaration of Principles and Plan of Action[12] that relate to building confidence and security in the use of ICTs and promoting a global culture of cyber-security.

The outcomes of the second phase of the WSIS, held in Tunisia in November 2005, are summarized in the Tunis Agenda and Tunis Commitment. All governments, according to the Tunis Agenda,[13] should have an equal role and responsibility in internet governance, but must also ensure the internet's stability, security, and continuity. The document calls for enhanced cooperation to enable all governments to carry out these responsibilities, including the development of globally applicable principles on public policy issues associated with the coordination and management of critical internet resources.

The Tunis Agenda also recognizes the need for "national action and increased international cooperation to strengthen security while enhancing the protection of personal information, privacy and data." It underlines "the importance of the security, continuity and stability of the Internet, and the need to protect the Internet and other ICT networks from threats and vulnerabilities". It further emphasizes "the need for a common understanding of the issues of Internet security, and for further cooperation to facilitate outreach, the collection and

[12] World Summit on the Information Society (WSIS) Documents: "Geneva Declaration of Principles", "Geneva Plan of Action", "Tunis Commitment", and "Tunis Agenda for the Information Society". http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1161|1160|2266|2267.

[13] World Summit on the Information Society (WSIS). "Tunis Agenda for the Information Society". http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2267|0.

dissemination of security-related information and exchange of good practice among all stakeholders on measures to combat security threats, at national and international levels”.[14]

In a resolution passed on 28 July 2008, entitled Follow-up to the World Summit on the Information Society and Review of the Commission on Science and Technology for Development (CSTD),[15] ECOSOC indicated how it would oversee the system-wide follow-up of the summit outcomes, as requested by the Tunis outcomes. To this end, ECOSOC decided that CSTD would assist the council as the focal point in the system-wide follow-up of WSIS. It was agreed that this would entail a strong development orientation and that the Commission would be strengthened in its substantive capacity through the effective and meaningful participation of member states in its work. While preserving the inter-governmental nature of the commission, ECOSOC decided that CSTD should make use of the successful multi-stakeholder approach that was pioneered by WSIS. During the two sessions of 2007 and 2008, the deliberations of CSTD therefore were (and remain) open not only to NGOs in consultative states with ECOSOC, but also to other interested NGOs and civil society entities who were accredited to WSIS.[16]

## International Telecommunication Union (ITU)

At the WSIS, world leaders entrusted the International Telecommunication Union (ITU)[17] with the leading role in coordinating international efforts on cyber-security. As the sole facilitator for the action line related to Building Confidence and Security in the Use of ICT (WSIS Action Line C5),[18] the ITU

[14] Ibid., paragraphs 39 and 45.

[15] Resolution 2006/46 (28 July 2006). “Follow-up to the World Summit on the Information Society and review of the Commission on Science and Technology for Development”. http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2368|0.

[16] http://www.itu.int/wsis/follow-up/index.html.

[17] http://www.itu.int/net/home/index.aspx.

[18] World Summit on the Information Society: “Geneva Plan for Action”. http://www.itu.int/wsis/docs/geneva/official/poa.html.

launched the Global Cybersecurity Agenda (GCA) in May 2007 to provide a framework within which the international response to the growing challenges to cyber-security can be coordinated and addressed.[19] GCA benefits from the advice of a High-Level Experts Group (HLEG)[20] comprising more than one hundred (100) world-renowned specialists in cyber-security from governments, industry, international organizations, research organizations, and academia. The HLEG was established to advice the ITU secretary-general on concrete measures and strategies to address global challenges in the five work areas of the GCA:

- Legal Measures,
- Technical and Procedural Measures,
- Organizational Structures,
- Capacity-Building,
- International Cooperation.

In 2007 and 2008, the ITU carried out significant standardization work in security architecture, encryption and authentication, and information security management systems:[21]

- Three new recommendations on cyber-security were approved by ITU: Overview of cyber-security; vendor-neutral framework for automatic notification of security related information and dissemination of updates; and guidelines for telecommunication service providers for addressing the risk of spyware and potentially unwanted software.
- Three new recommendations on countering spam were approved by ITU: Technical strategies on countering spam; technologies involved in countering e-mail spam; and a technical framework for countering e-mail spam.
- Two new draft ITU recommendations have been submitted for the approval process:  Countering IP multimedia application spam; and requirements for global identity management trust and interoperability.

[19] http://www.itu.int/osg/csd/cybersecurity/gca/overview/index.html.

[20] http://www.itu.int/osg/csd/cybersecurity/gca/hleg/index.html.

[21] Information provided by an expert.

- Twenty-eight more security recommendations were approved by ITU, as of June 2008, in areas including: directory services, authentication, security architecture, security management, tele-biometrics, peer-to-peer communication security, and secure mobile data communication.
- An ITU Study Group leads the identity management (IdM) work and has made four ongoing draft recommendations, which cover topics such as: data models, interoperable frameworks, interchange frameworks, and entity authentication assurance. In addition to the above-mentioned topics, new issues such as a trusted service provider identifier (T-SPID) were introduced into discussion.
- Significant progress has been made on the security aspects of IPTV. The first IPTV security recommendation is expected to be completed by September 2008.

In addition, the ITU has launched the ICT Security Standards Roadmap,[22] an online database that provides information about existing ICT security standards and works in progress in key standards development organizations.

The ITU is also engaged in direct assistance to member states (particularly developing countries) building cyber-security capacities through a number of different activities. To this end, the ITU is developing a national cyber-security framework to coordinate national efforts, provide technical assistance, and organize capacity-building cyber-security forums. The ITU is also working with partners from the public and private sectors on specific cyber-security and Critical Information Infrastructure Protection development initiatives to assist developing countries in awareness and self-assessment, capacity-building, and expanding watch, warning, and incident response capabilities. Some relevant deliverables include the ITU National Cybersecurity/CIIP Self-Assessment Toolkit,[23] which aims to assist governments in enhancing their cyber-security and address CIIP requirements; the  Botnet Mitigation Toolkit;[24] as well as toolkits on the establishment of CERTs/CSIRTs, and promoting a culture of

[22] http://www.itu.int/ITU-T/studygroups/com17/ict/index.html.

[23] http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html.

[24] http://www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.htmlt.

cyber-security. Other ITU initiatives to assist developing countries include the development of anti-spam legislative surveys, assessment activities of national cyber-crime legislations, and research on the financial aspects of network security, malware, and spam.[25]

[25] Information provided by an expert.

# The World Bank Group

The growing incidence of computer and cyber-crime has a particularly strong bearing on the financial sector. In view of the growing amount of financial data stored and transmitted online, the ease of computer intrusions has added to the severity of the problem. Therefore, the World Bank Group has taken several steps over the last few years to face the challenges of information security, especially in developing countries.[1]

## The Global Information and Communication Technologies Department (GICT)

The Global Information and Communication Technologies Department (GICT)[2] promotes access to information and communication technologies in developing countries. It serves as the World Bank Group's core department for research, policy, investment, and programs related to ICT in developing countries. The GICT's aim is to expand access to a range of information infrastructure networks and support the development and application of information technologies to reduce poverty and improve people's lives. Linked to this mission are three goals aimed at:[3]

- Accelerating the participation of developing countries in the global information economy;
- Spreading the benefits of these technologies through increased competition and private investment in information infrastructure;

[1] http://info.worldbank.org/ict/index.cfm.

[2] http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/0,,contentMDK:20687836~menuPK:282840~pagePK:210058~piPK:210062~theSitePK:282823,00.html.

[3] http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/0,,contentMDK:20687829~menuPK:1785618~pagePK:210058~piPK:210062~theSitePK:282823,00.html.

- Fostering sustainable economic and social development through innovative technologies, with a special emphasis on the need of the poor in developing countries.

Moreover, the World Bank Group's ICT sector strategy is based on four pillars:[4] The broadening and deepening of sector and institutional reform, the improvement of access to information infrastructure, the support of human capacity to exploit ICT, and the support of ICT applications across a broad range of sectors.

The GICT group consists of six teams including[5] the office of the director, the strategy and business development team, the telecom and media division, the portfolio and technology division, the public sector policy and operations division, and the Information for Development (infoDev) Program[6].

## Information Technology Security Handbook

The Information Technology Security Handbook,[7] funded by the infoDev Program, provides technology-independent best practices and recommendations in the field of IT security. The handbook was published in 2003 and, as the technology evolves, the accompanying website[8] provides updates as appropriate. The book addresses private users of IT, small and medium-sized organizations, government, and technical administrators, especially in developing countries. The handbook is based on the premise that use of ICT is on the rise, while the knowledge of IT security practices is lagging behind.

[4] Ibid.

[5] http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/0,,contentMDK:20718594~menuPK:1786142~pagePK:210058~piPK:210062~theSitePK:282823,00.html.

[6] http://www.infodev.org/en/index.html.

[7] The International Bank for Reconstruction and Development/The World Bank (infoDev). "Information Technology Security Handbook", (Washington, D.C., 2003). http://www.infodev-security.net/handbook.

[8] http://www.infodev-security.net.

After a general introduction to IT security, the Information Technology Security Handbook deals with topics such as:[9]

- Security for individuals: keeping personal computers, data and operating systems, and applications secure; malicious software; securing services over networks; tools to enhance security; and the role of encoding and encryption;
- Security for organizations: risk evaluation and mitigation; planning; organizational security policy and personnel security; security outsourcing; mobile risk management; and best practices;
- Information security and government policies: various arrangements for protecting government systems; laws and legislation; and government policy in promoting better security in the private sector;
- IT security for technical administrators: physical security; information security; identification and authentication; server security; network security; attack and defenses; and detecting and managing break-ins.

## The World Bank's e-Security/ e-Finance efforts

The World Bank published a report on Electronic Security: Risk Mitigation in the Financial Transactions in June 2002, building on previous papers that identified e-security as a key component to the delivery of e-finance benefits. This paper and its technical annexes identify and discuss eight key pillars for a secure electronic environment.[10]

[9] "Information Technology Security Handbook", op. cit.

[10] The World Bank. "Electronic Security: Risk Mitigation in the Financial Transactions", Public Policy Issues (June 2002). http://wbln0018.worldbank.org/html/FinancialSectorWeb.nsf/(attachmentweb)/E-security-RiskMitigationInFinancialTransactionsv4/$FILE/E-security-Risk+Mitigation+In+Financial+Transactions+v+4.0.pdf.

In January and May 2004, a follow-up publication was published, entitled Technology Risk Checklist.[11] This World Bank publication describes 13 layers of e-security, covering both hardware and software pertaining to network infrastructures. These layers cover risk management, policy management, cyber-intelligence, access controls and authentication, firewalls, active content filtering, intrusion detection systems (IDS), virus scanners, encryption, vulnerability testing, systems administration, incident response plans (IRP), and wireless security.[12] In 2005, two further documents were published by the World Bank's e-security/e-finance section on the dangers emanating from BOTs – Cyber Parasites[13] and on the issue of Money Laundering in Cyberspace.[14]

[11] The World Bank. "Technology Risk Checklist", (May 2004, Version 7.3). http://www.infragard.net/library/pdfs/technologyrisklist.pdf.

[12] Ibid., pp. 2ff.

[13] http://wbln0018.worldbank.org/html/FinancialSectorWeb.nsf/(attachmentweb)/Bots/$FILE/Bots.pdf.

[14] http://wbln0018.worldbank.org/html/FinancialSectorWeb.nsf/(attachmentweb)/MoneyLaunderinginCyberspace/$FILE/MoneyLaunderinginCyberspace.pdf.

# Conclusion

# Conclusion

For a number of years, policymakers at the highest levels have been expressing their concern that insecure information systems threaten economic growth and national security. As a result of these concerns, a complex and overlapping web of national, regional, and multilateral initiatives has emerged. The International CIIP Handbook provides an overview of these initiatives in the field of critical information infrastructure protection (CIIP). Despite the sometimes substantial differences between these governmental protection policies, they offer a wealth of empirical material from which a variety of lessons can be distilled for the benefit of the international community.

For each country survey, five focal points of high importance covering conceptual and organizational aspects of CIIP were considered. In the following, we will wrap up each section: the definition of critical sectors and the CIP/CIIP conceptual framework; past and present initiatives and policy; organizational structures; early-warning approaches and public outreach; and law and legislation. We will also address how international organizations are dealing with CIIP.

## Critical Sectors

In the first section, the critical sectors identified by each country were listed and the definitions of CII and CIIP discussed. Some countries, such as Australia, Canada, Germany, the Netherlands, New Zealand, the UK, or the US, provide clear definitions of what constitutes CIP, while other countries – for example

Brazil, Korea, or Russia –, offer no definition. Everywhere, CIIP is understood more or less explicitly as a subset of CIP, including protection, detection, response, and recovery activities at both the physical and the virtual levels. However, a clear distinction between CIP and CIIP is lacking in most countries, and one finds both terms being used interchangeably. As was pointed out in the introduction, this reflects the continuing difficulties that arise from having to distinguish between physical and virtual aspects of critical infrastructures.

In designating critical sectors, all countries have followed the example of the Presidential Commission on Critical Infrastructure Protection (PCCIP), which was the first official publication to correlate critical infrastructures with specific business sectors or industries.[1] The choice of the "sector" as a unit of analysis is a pragmatic approach that roughly follows the boundaries of existing business/industry sectors. This approach reflects the fact that the majority of infrastructures is owned and operated by private actors. In addition, the decision on which infrastructures and sectors to include in the list of critical assets requires input from private-sector experts, besides experts and officials at various levels of government. More often than not, expert groups address the issue, either in larger or smaller groups.[2] A component or a whole infrastructure is usually defined as "critical" due to its strategic position within the whole system of infrastructures, and especially due to the interdependency between the component or the infrastructure and other infrastructures. However, as we show below, there is also a more symbolic understanding of criticality that influences the designation of critical assets.

It is broadly acknowledged, however, that the focus on sectors is too artificial to represent adequately the realities of complex infrastructure systems. For a more meaningful analysis, it is therefore deemed necessary to evolve beyond the conventional ”sector”-based focus and to look at the services, the physical and

[1] President's Commission on Critical Infrastructure Protection (PCCIP). "Critical Foundations: Protecting America's Infrastructures". Washington, October 1997. http://www.ihs.gov/misc/links_gateway/download.cfm?doc_id=327&app_dir_id=4&doc_file=PCCIP_Report.pdf [last accessed in June 2008]. Publication quoted in the following as PCCIP.

[2] Dunn, Myriam (2004). "Part II: Analysis of Methods and Models for CII Assessment". In: Dunn, Myriam and Isabelle Wigert. The International Critical Information Infrastructure Protection (CIIP) Handbook 2004. Zurich: Center for Security Studies, pp. 219–97.

electronic (information) flows, their role and function for society, and especially the core values that are delivered by the infrastructures. Therefore, experts groups often focus on four steps in the identification of what is critical: 1) critical sectors, 2) sub-sectors for each sector on the basis of organizational criteria, 3) core functions of the sub-sectors, and 4) resources necessary for the functioning of the sub-sectors.[3]

Table 1 shows which country defines which sectors as critical. One must be careful, however, to avoid misleading comparisons: While for instance Australia, Canada, the Netherlands, the UK, and the US are very precise in identifying critical sectors and sub-sectors as well as products and services that these sectors provide, other countries, such as Austria, Brazil, Poland, Russia, have no official list of critical sectors.

Variations between countries can be explained by differences in conceptualizations of what is critical, but also by country-specific peculiarities and traditions. Socio-political factors as well as geographical and historical preconditions determine whether or not a sector is deemed to be critical.

The most frequently mentioned critical sectors in all countries are listed below. These are the core sectors of modern societies, and possibly the areas where a large-scale interruption would be most devastating:

- Banking and Finance,
- Central Government/Government Services,
- (Tele-)Communication/Information and Communication Technologies (ICT),
- Emergency/Rescue Services,
- Energy/Electricity,
- Health Services,
- Food,
- Transportation/Logistics/Distribution, and
- Water (Supply).

[3] Ibid., pp. 227f.

| Country<br>Sector | AUS | A | BR | CAN | EST | F | FIN | GER | HUN |
|---|---|---|---|---|---|---|---|---|---|
| Banking and Finance | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| Central Government / Government Services |  | ● |  | ● | ● | ● |  | ● | ● |
| Chemical and Nuclear Industry |  |  |  | ● |  |  |  |  |  |
| Emergency / Rescue Services | ● |  | ● | ● | ● | ● |  |  | ● |
| Energy / Electricity | ● | ● |  | ● | ● | ● | ● | ● | ● |
| Food / Agriculture | ● |  |  | ● | ● | ● | ● | ● | ● |
| Health Services | ● |  | ● | ● | ● | ● | ● |  | ● |
| Information Services / Media | ● | ● |  |  |  | ● | ● |  | ● |
| Military Defense / Army / Defense Facilities |  |  |  |  |  | ● |  |  | ● |
| National Icons and Monuments | ● |  |  |  |  |  |  |  |  |
| Sewerage / Waste Management | ● |  |  |  |  |  |  |  |  |
| Telecommunications | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| Transportation (land, sea, air) / Logistics / Distribution | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| Water Infrastructure |  |  |  |  | ● |  |  |  |  |
| Water (Supply) | ● |  | ● |  | ● | ● | ● | ● | ● |

Table 1: Overview of the Critical Sectors and Sub-sectors Identified by Surveyed Countries

A comparison across time (see CIIP Handbooks 2002, 2004, and 2006) also shows that the concept of criticality has undergone change, and that the criteria for determining which infrastructures qualify as critical have expanded over time; the PCCIP, for example, defined eight sectors as critical for the US, while today, critical infrastructures in the US already include 18 sectors.

We can thus distinguish between two differing, but interrelated perceptions of criticality:[4]

- Criticality as systemic concept: This approach assumes that an infrastructure or an infrastructure component is critical due to its structural position in the whole system of infrastructures, especially when it constitutes an important link between other infrastructures or sectors, and thus reinforces interdependencies.

[4] Metzger, Jan (2004). "The Concept of Critical Infrastructure Protection (CIP)". In: Bailes, A. J. K. and Isabelle Frommelt (eds.). Business and Security: Public-Private Sector Relationships in a New Security Environment. Oxford: Oxford University Press, pp. 197–209.

| IND | IT | JAP | KOR | MAL | NL | NO | NZ | POL | RU | SE | SING | SPA | SWIT | UK | US | TOTAL |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | 24 |
|  | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● |  | ● | ● | ● | ● | 20 |
| ● |  |  |  | ● | ● |  |  | ● |  |  |  | ● | ● |  | ● | 8 |
| ● | ● |  | ● | ● |  | ● | ● | ● | ● |  |  |  | ● | ● | ● | 17 |
| ● | ● | ● | ● |  | ● | ● | ● | ● |  |  | ● | ● | ● | ● | ● | 21 |
|  | ● | ● |  |  | ● | ● |  |  |  |  | ● | ● | ● | ● | ● | 16 |
|  | ● |  |  | ● | ● | ● |  |  |  |  | ● | ● | ● | ● | ● | 16 |
|  | ● |  | ● |  | ● | ● |  |  | ● | ● | ● |  | ● |  | ● | 14 |
| ● |  |  | ● | ● |  | ● |  |  | ● |  |  |  |  | ● | ● | 9 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | ● | 2 |
|  | ● |  |  | ● | ● | ● |  | ● |  |  |  |  | ● | ● | ● | 9 |
| ● | ● | ● | ● |  | ● | ● | ● | ● | ● | ● | ● | ● |  | ● | ● | 22 |
| ● | ● | ● | ● | ● | ● | ● | ● | ● |  | ● | ● | ● | ● | ● | ● | 24 |
|  |  |  |  |  | ● |  |  |  |  |  |  |  |  |  | ● | 3 |
|  | ● | ● |  | ● | ● | ● |  |  |  | ● | ● | ● | ● | ● | ● | 18 |

- Criticality as a symbolic concept: This approach assumes that an infrastructure or an infrastructure component is inherently critical because of its role or function in society; the issue of interdependencies is secondary – the inherent symbolic meaning of certain infrastructures is enough to make them interesting targets.[5]

The symbolic understanding of criticality allows the integration of non-interdependent infrastructures as well as objects that are not man-made into the concept of critical infrastructures, including significant personalities or natural and historical sites with a strong symbolic character. Additionally, the symbolic approach allows essential assets to be defined more easily than the systemic one,

[5] For an example (critical assessment without interdependencies), see: United States General Accounting Office (GAO). Testimony before the Subcommittee on National Security, Veterans Affairs, and International Relations; House Committee on Government Reform. "Homeland Security: Key Elements of a Risk Management". Statement of Raymond J. Decker, Director Defense Capabilities and Management. 12 October 2001, p. 6. http://www.gao.gov/new.items/d02150t.pdf [last accessed in June 2008].

because in a socio-political context, the defining element is not interdependency as such, but the role, relevance, and symbolic value of specific infrastructures.[6]

The emphasis on the interconnectedness of various sectors, in connection with this symbolic understanding, creates a specific set of problems for decision-makers: Basically, everything is networked, and even a discrete event of little apparent significance could potentially set off unpredictable cascading effects throughout a large number of sectors. When the concept of criticality, and accordingly the scope of what is to be secured, is expanded from interconnected physical networks like the electrical grid and road networks to include everything with emotional significance, ranging from schools to national monuments, almost everything becomes potentially critical. In this situation, decision-makers must be careful not to follow the natural impulse to increase security ad absurdum and aim to protect everything that could possibly be at risk, because total protection will never be possible, and the effects on society will likely be negative. Prioritization must be based on careful risk assessment that comprises calculations of the likelihood of a given threat source displaying a particular potential vulnerability, and the resulting impact of that adverse event.[7]

At the same time, one must be aware of the fact that current methodologies for analyzing CII – and first and foremost among them risk analysis – are insufficient in a number of ways: One of the major shortcomings is that the majority of them do not pass the "interdependency test". In other words, they fail to address, let alone understand, the issue of interdependencies and possible cascading effects. Besides, the available methods are either too sector-specific or too focused on single infrastructures and do not take into account the strategic,

[6] Metzger, op. cit.

[7] Stoneburner, Gary, Alice Goguen, and Alexis Feringa (2002). "Risk Management Guide for Information Technology Systems". Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-30. Washington: US Government Printing Office, p. 8. http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf [last accessed in June 2008].

security-related, and economic importance of CII.[8] Moreover, there are both theoretical and practical difficulties involved in estimating the probabilities and consequences of high-impact, low-probability events – and this is the scenario we are dealing with in the context of CI(I)P. It also appears that there is no way of apolitically cataloguing objects, vulnerabilities, and threats on a strategic policy level, such as the economy at large, in a meaningful way.

Clearly, therefore, long-term research into CIP and CIIP matters is needed. A holistic and strategic threat and risk assessment at the physical, virtual, and psychological levels is the basis for a comprehensive protection and survival strategy, and will thus require a comprehensive and truly interdisciplinary research and development agenda that encompasses fields ranging from engineering and complexity sciences to policy research, political science, and sociology.

## Past and Present Initiatives and Policy

In the second section, the CIIP Handbook gave an overview of the most important initiatives and the main elements of CIIP policy in the surveyed countries. This included descriptions of specific committees, commissions, task forces, and working groups as well as the main findings of key official reports and fundamental studies, and important national programs. Many of the national CIIP efforts were triggered or at least accelerated by the Presidential Commission on Critical Infrastructure Protection (PCCIP) set up by US President Bill Clinton in 1996, and to some extent by the preparations for anticipated problems on the threshold of the year 2000 (Y2K problem). This led to the establishment of (interdepartmental) committees, task forces, and working groups. Their mandate often included scenario work, the evaluation of a variety of measures, or assessments of early-warning systems. These efforts resulted in policy statements – such as

[8] This issue is addressed in additional detail in by Myriam Dunn, who argues that shortcomings include the lack of data to support objective probability estimates, persistent value questions, and conflicting interests within complex decisionmaking processes. Dunn, Myriam (2006). "Understanding Critical Information Infrastructures: An Elusive Quest". In: Dunn, Myriam and Victor Mauer (eds.). International CIIP Handbook 2006. Vol. II. Analyzing Issues, Challenges, and Prospects. Zurich: Center for Security Studies, pp. 27–53.

recommendations for the establishment of independent organizations dealing with information society issues – and reports laying down basic CIIP policies.

In the aftermath of 11 September 2001 ("9/11"), several countries launched further initiatives to strengthen and allocate additional resources to their CIP/CIIP efforts. Prior to 9/11, for many people, critical infrastructure protection was synonymous with cyber-security. The attacks of 9/11, however, highlighted the fact that terrorists could cause enormous damage by attacking critical infrastructures directly and physically, and thus demonstrated the need to re-examine physical protection, especially in the US.[9] The perception that the cyber-dimension had been unduly prioritized before 9/11 subsequently led to a shift in focus from the virtual to the physical domain, and from CIIP to CIP. Subsequently, CIP became a key component of Homeland Security and is currently discussed predominantly with a view to developing strategies against Muslim terrorism. The physical aspects of CIP have been moved to the forefront, while the importance of information aspects has diminished. This CIP focus on counterterrorism has also become a hallmark of debates in the EU, which has recently begun to develop a CIP policy that consists mainly of coordinating the measures adopted by member states.

CIIP policies are at various stages of implementation – some are already being enforced, while others are just a set of suggestions – and come in various shapes and forms, ranging from a regulatory policy focus concerned with the smooth and routine operation of infrastructures and questions such as privacy or standards, to the inclusion of cyber-security into more general counter-terrorism efforts. Most countries consider CIIP to be a national-security issue of some sort. In parallel, however, they often pursue a business continuity strategy under the "information society" label. The law enforcement/crime prevention perspective is also found in all countries. Furthermore, data protection issues are a major topic for civil rights groups. While all of the perspectives can be found

[9] Moteff et al., op. cit., p. 3.

in all countries, the emphasis given to one or more of the perspectives varies to a considerable degree.[10]

All countries examined have recognized the importance of public-private partnerships (PPP). Governments actively promote information-sharing with the private sector, since large parts of critical infrastructures are owned and operated by the business sector. Different types of such partnerships are emerging, including government-led partnerships, business-led partnerships, and joint public-private initiatives. In Switzerland, Korea, the UK, and the US, strong links have already been established between the private business community and various government organizations. One of the future challenges in many countries will be to achieve a balance between security requirements and business efficiency imperatives. Satisfying shareholders by maximizing company profits has often led to minimal security measures. This is because like many political leaders, business leaders tend to view cyber-attacks on infrastructures as a tolerable risk.

Despite the general consensus on the positive aspects of PPPs, their implementation remains difficult. It has been shown that it is relatively easy for the government and private actors in a PPP to agree on the existence of a problem and on the need for a remedy. It is, however, much harder to agree on actual measures to be taken, on the actors responsible for implementing them, on the party that will assume legal responsibility for such measures, and on the party that will bear the costs for implementing them.[11]

[10] This issue is also addressed by Isabelle Abele-Wigert, who shows how practical and academic dialog is hampered by vastly differing terminology and viewpoints of what constitutes the problem. Wigert, Isabelle (2006). "Challenges Governments Face in the Field of Critical Information Infrastructure Protection (CIIP): Stakeholders and Perspectives". In: Dunn, Myriam and Victor Mauer (eds.). International CIIP Handbook 2006. Vol. II. Analyzing Issues, Challenges, and Prospects. Zurich: Center for Security Studies, pp. 55–68.

[11] Andersson, Jan Joel and Andreas Malm (2006). "Public-Private Partnerships and the Challenge of Critical Infrastructure Protection". In: Dunn, Myriam and Victor Mauer (eds.). International CIIP Handbook 2006. Vol. II. Analyzing Issues, Challenges, and Prospects. Zurich: Center for Security Studes, pp.139–67.

## Organizational Overview

The third section gave an overview of important public actors in the national CIIP organizational framework and presented the most important public-private partnerships. Only in a few countries have central governmental organizations been created to deal specifically with CIIP. The US, France, Switzerland, Singapore, and Korea have all made provisions in this regard. Mostly, responsibility lies with multiple authorities and organizations in different governmental departments. Very often, responsibility for CIIP protection is given to well-established organizations or agencies that appear suitable for the task. Depending on their key assignment, these agencies bring their own perspective to bear on the problem and shape policy accordingly.

In countries such as France and New Zealand, CIIP efforts are mainly led by the defense establishment, whereas in other countries, such as the UK or Switzerland, approaches to CIIP are jointly led by the business community and public agencies. Furthermore, in Australia as well as in the US and New Zealand, CIIP is integrated into the overall counterterrorism efforts, where the intelligence community plays an important role. In India, Korea, Japan, Singapore, and Estonia, the fostering of the information society and economic growth through safe information infrastructures is at the forefront.

The establishment of these organizational units and their location within the government structures are influenced by various factors such as civil defense tradition, the allocation of resources, historical experience, and the general threat perception of key actors in the policy domain. Depending on their influence or on the resources at hand, various key players shape the issue in accordance with their view of the problem. Different groups, whether they be private, public, or a mixture of both, do not usually agree on the exact nature of the problem or on what assets need to be protected with which measures. There are at least four (overlapping) typologies for how CIIP issues are viewed: an IT-security perspective, an economic perspective, a law enforcement perspective, and a national-security perspective. While all typologies can be found in all countries, the emphasis given to one or more of them varies to a considerable degree. Ultimately, the dominance of one or several typologies has implications for the shape of the protection policies and, subsequently, for determining appropriate protection efforts, goals, strategies, and instruments for solving problems.

In the end, the distribution of resources and the technical and social means for countering the risk are important for the outcome. We can observe that the different actors involved – ranging from government agencies and the technology community to insurance companies – have divergent interests and compete with one another by means of scenarios describing how they believe the threat will manifest itself in the future.[12] Furthermore, the selection of policies seems to depend largely upon two factors: One is the varying degree to which resources are available to the different groups. The other factor is the impact of cultural and legal norms, because they restrict the number of potential strategies available for selection.[13] In general, we can identify two influential discourses: On the one hand, law enforcement agencies emphasize their view of the risk as "computer crime", while on the other hand, the private sector running the infrastructures perceives the risk mainly as a local, technical problem or in terms of economic costs.[14] Because the technology generating the risk makes it very difficult to fight potential attackers in advance, protective measures focus on preventive strategies and on trying to minimize the impact of an attack when it occurs. Here, the infrastructure providers are in a strong position, because they alone are in the position to install technical safeguards for IT security at the level of individual infrastructures.

Norms are also important in selecting the strategies. Most importantly, the general aversion of the new economy to government regulation as well as legal restrictions limits the choice of strategies.[15] Besides these cultural differences with regard to strategy, the nature of cyber-attacks naturally positions law

[12] Bendrath, Ralf (2003). "The American Cyber-Angst and the Real World – Any Link?" In: Robert Latham (ed.). Bombs and Bandwidth: The Emerging Relationship between IT and Security. New York: The New Press, pp. 49–73; id. (2001). "The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection". In: Wenger, Andreas (ed.). The Internet and the Changing Face of International Relations and Security. Information & Security: An International Journal. Vol. 7, pp. 80–103.

[13] Dunn, Myriam. "Cyber-Threats and Countermeasures: Towards an Analytical Framework for Explaining Threat Politics in the Information Age". Conference paper, SGIR Fifth Pan-European IR Conference, The Hague, 10 September 2004.

[14] Bendrath, "The Cyberwar Debate", op. cit., p. 97.

[15] Ibid., p. 98.

enforcement at the forefront: It is often impossible to determine at the outset whether an intrusion is an act of vandalism, computer crime, terrorism, foreign intelligence activity, or some form of strategic attack. The only way to determine the source, nature, and scope of the incident is to investigate. The authority to investigate such matters and to obtain the necessary court orders or subpoenas clearly resides with law enforcement. As a consequence of the nature of cyber-threats, the cyber-crime/law enforcement paradigm is emerging as the strongest viewpoint in most countries.

## Early Warning and Public Outreach

The fourth section described national organizations responsible for CIIP early warning. The earlier a potential risk is identified, the greater the chance to act in a timely, resource-efficient, and strategically adequate manner. Therefore, timely warning of attacks is an indispensable component of ensuring that a breakdown of important infrastructure, or even only of certain components of ICT, will be limited to an incident that is short, rare, controllable, geographically isolated, or with as little consequences as possible for the national economy and security.

Early-warning systems are designed for the following purposes: understanding and mapping the hazard; monitoring and forecasting impending events; processing and disseminating understandable warnings to political authorities and the population; and undertaking appropriate and timely actions in response to the warnings. In CIIP, early warning is focused mainly on IT security incidents. The general trend in CIIP early warning points towards establishing central contact points for the security of information systems and networks. Among the existing early-warning organizations are various forms of Computer Emergency Response Teams (CERTs), e.g., special CERTs for government departments, CERTs for small and medium-sized businesses, CERTs for specific sectors, and others. CERT functions include handling of computer security incidents and vulnerabilities or reducing the probability of successful attacks by publishing security alerts.[16] Internationally, CERTs primarily exchange information at the Forum of Incident Response and Security Teams (FIRST).

In some countries, permanent analysis and intelligence centers have been developed in order to make tactical or strategic information available to the decision-makers within the public and private sectors more efficiently. Tasks of early-warning system structures include analysis and monitoring of the situation as well as the assessment of technological developments. Examples can be found in Canada (Integrated Threat Assessment Center)[17] and in Switzerland (Reporting and Analysis Center for Information Assurance, MELANI).[18]

Often, these entities manage outreach, cyber-security awareness, and partnership efforts to disseminate information to key constituencies and build collaborative actions with key stakeholders. Generally, many private enterprises, public entities, and home users lack the resources to manage cyber-security risks adequately. Many entrepreneurs and home users are unaware of the extent to which their individual cyber-security preparedness affects overall security, and internet users must be made aware of the importance of sound cyber-security practices and require more user-friendly tools to implement them. Public outreach efforts therefore entail cataloguing existing best practices, developing strategies to market those practices to specific audiences, creating incentive plans to ensure acceptance of those practices, contributing to the development of a national advertising campaign, and developing a strategy to communicate the importance of cyber-security and their role in enhancing it to public and private CEOs across the country.

[16] The issue is further addressed by Thomas Holderegger, who examines early-warning players in the CIIP sector and specifies their tasks and responsibilities, with a specific focus on the role of the nation state. Holderegger, Thomas (2006). "The Aspect of Early Warning in Critical Information Infrastructure Protection (CIIP)". In: Dunn, Myriam and Victor Mauer (eds.). International CIIP Handbook 2006. Vol. II. Analyzing Issues, Challenges, and Prospects. Zurich: Center for Security Studies, pp. 111–35.

[17] http://www.itac-ciem.gc.ca/index-eng.asp.

[18] http://www.melani.admin.ch/

## Legal Issues

The fifth section focused on legislation in the field of cyber-security. Although many countries have been concerned with the protection and security of information (infrastructures) and related legislation for some years, they have begun to review and adapt their cyber-security legislation after 9/11. Because national laws are developed autonomously, some countries have preferred to amend their penal or criminal code, whereas others have passed specific laws on cyber-crime.

The following is an overview of important common issues currently discussed in the context of legislation procedures in the countries covered in the handbook:

- Data protection and security in electronic communications (including data transmission, safe data storage, etc.);
- IT security and information security requirements;
- Fraudulent use of computer and computer systems, damage to or forgery of data, and similar offences;
- Protection of personal data and privacy;
- Identification and digital signatures;
- Responsibilities in e-commerce and e-business;
- International harmonization of cyber-crime law;
- Minimum standards of information security for (e-)governments, service providers, and operators, including the implementation of security standards such as BS7799, the code of practice for information security management ISO/IEC 17799, the Common Criteria for Information Technology Security Evaluation ISO/IEC 15408, and others;
- Public key infrastructure and its regulation.

Across all boundaries, there are two main factors that influence and sometimes even hinder efficient law enforcement – one with a national, the other with an international dimension:

- Lack of know-how or of functioning legal institutions: Even if a country has strict laws and prohibits many practices, the enforcement of such laws is often difficult. Frequently, the necessary means to prosecute misdemeanors effectively are lacking due to resource problems, inexistent or emerging cyber-crime units, or a lack of supportive legislation, such as the storing of rendition data.[19]
- Lack or disparity of legal codes: While most crimes, such as theft, burglary, and the like are punishable offenses in almost every country of the world, some rather grave disparities still remain in the area of cyber-crime.[20]

## International Issues

From the discussion of legal issues, it becomes obvious that like other security issues, the vulnerability of modern societies – caused by dependency on a spectrum of highly interdependent information systems – has global origins and implications. To begin with, the information infrastructure transcends territorial boundaries, so that information assets that are vital to the national security and the essential functioning of the economy of one state may reside outside of its sphere of influence on the territory of other nation-states. Additionally, "cyberspace" – a huge, tangled, diverse, and universal blanket of electronic interchange – is present wherever there are telephone wires, cables, computers, or electromagnetic waves, a fact that severely curtails the ability of individual states to regulate or control it alone. Any adequate protection policy that extends to strategically important information infrastructures will thus ultimately require transnational solutions.

[19] Goodman, Seymour E., Pamela B. Hassebroek, Davis King, and Andy Azment. "International Coordination to Increase the Security of Critical Network Infrastructures", Document CNI/04. Paper presented at the ITU Workshop on Creating Trust in Critical Network Infrastructures. Seoul, 20–22 May 2002.

[20] Gelbstein, Eduardo and Ahmad Kamal. "Information Insecurity. A Survival Guide to the Uncharted Territories of Cyber-Threats and Cyber-Security". United Nations ICT Task Force and United Nations Institute for Training and Research. New York, November 2002. http://www.un.int/unitar/patit/dev/old%20site/curriculum/Information_Insecurity_Second_Edition_PDF.pdf.

There are four possible categories of initiatives that may be launched by multilateral actors: deterrence, prevention, detection, and reaction.

- Deterrence – or the focus on the use of multilateral cyber-crime legislation: Multilateral initiatives to deter the malicious use of cyberspace include initiatives a) to harmonize cyber-crime legislation and to promote tougher criminal penalties (e.g. the Council of Europe Convention on Cyber-crime),[21] and b) to improve e-commerce legislation (e.g., the efforts of the United Nations Commission on International Trade Law (UNCITRAL) for electronic commerce).[22]
- Prevention – or the design and use of more secure systems and better security management, and the promotion of more security mechanisms: Multilateral initiatives to prevent the malicious use of cyberspace center around a) promoting the design and use of more secure information systems (e.g., the Common Criteria Project);[23] b) improving information security management in both public and private sectors (e.g., the ISO and OECD standards and guidelines initiatives);[24] c) legal and technological initiatives, such as the promotion of security mechanisms (e.g., electronic signature legislation in Europe).
- Detection – or cooperative policing mechanisms and early warning of attacks: Multilateral initiatives to detect the malicious use of cyberspace include a) the creation of enhanced cooperative policing mechanisms (e.g., the G-8 national points of contact for cyber-crime); and b) early warning through information exchange with the aim of providing early warning of cyber-attacks by exchanging information between the public and private sectors (e.g., US Information Sharing & Analysis Centers, the European

[21] Council of Europe Convention on Cybercrime. http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm [last accessed in June 2008].

[22] http://www.uncitral.org/english/workinggroups/wg_ec/index.htm.

[23] http://www.commoncriteriaportal.org [last accessed in June 2008].

[24] The International Organization for Standardization ISO has developed a code of practice for information security management (ISO/IEC 17799:2000). http://www.iso.org/iso/en/prods-services/popstds/informationsecurity.html; the Organisation for Economic Co-operation and Development (OECD) promotes a "culture of security" for information systems and networks. http://www.oecd.org/document/42/0,2340,en_2649_33703_15582250_1_1_1_1,00.html [last accessed in June 2008].

Early Warning & Information System, and the European Network and Information Security Agency (ENISA)).

- Reaction – or the design of stronger information infrastructures, crisis management programs, and policing and justice efforts: Multilateral initiatives to react to the malicious use of cyberspace include a) efforts to design robust and survivable information infrastructures; b) the development of crisis management systems; and c) improvement in the coordination of policing and criminal justice efforts.

The most important legislative instrument in this area is the Council of Europe Cybercrime Convention (CoC). This convention is the first international treaty on crimes committed via the internet and other computer networks. Its main objective is to pursue a common law enforcement policy aimed at the protection of society against cyber-crime, especially by adopting appropriate legislation and fostering international cooperation.[25] An additional protocol to the CoC outlaws racist and xenophobic acts committed through computer systems.

While other politically powerful entities such as the G8 also try to foster collaboration and a more efficient exchange of information when it comes to cyber-crime and terrorism, the CoC goes one step further. It lays out a framework for future collaboration between the prosecution services of the signature states. It achieves this mainly by harmonizing the penal codes of the CoC signatory states. As a result, crimes such as hacking, data theft, and distribution of pedophile and xenophobic material, etc., will be regarded as illegal actions per se, thus resolving the problem of legal disparities between nations that was mentioned above. This also allows the authorities to speed up the process of international prosecution. Since certain activities are defined as illegal by all CoC member states, the sometimes long and painful task of crosschecking supposed criminal charges committed in a foreign country becomes obsolete if the offence is already included in the national penal code. Consequently, reaction times will be shortened and the parties to the CoC will establish a round-the-clock network

[25] Convention on Cybercrime, op. cit.

within their countries to handle aid requests that demand swift intervention.[26] While the implementation of the CoC will most likely be a slow and sometimes thorny process, the idea of finding a common denominator and harmonizing the response to at least some of the most crucial problems is certainly a step in the right direction.

[26] Taylor, Greg (no date). "The Council of Europe Cybercrime Convention. A civil liberties perspective". http://www.crime-research.org/library/CoE_Cybercrime.html [last accessed in June 2008].

# Appendix

# A1 Countries at a Glance

## Australia

**Past and Present Initiatives and Policies**

National Counter-Terrorism Plan (2003, revised 2005)

E-Security National Policy Statement (2007)

**Organizational Overview**

*Public Agencies*

Attorney-General's Department (AGD)

E-Security Policy and Coordination Committee (ESPaC)

Department of Broadband, Communications and the Digital Economy (DBCDE)

IT Security Expert Advisory Group (ITSEAG)

Communications Sector Infrastructure Assurance Advisory Group (CSIAAG)

Australian Government Computer Emergency Readiness Team (Gov.CERT.au)

Australian Government Information Management Office (AGIMO)

Defence Signals Directorate (DSD)

DSD's Information Security Group (INFOSEC)

Australian Security Intelligence Organisation (ASIO)

Australian Federal Police (AFP)

Australian High Tech Crime Centre (AHTCC)

*Public Private Partnerships*

Trusted Information Sharing Network for Critical Infrastructure Protection (TISN)

Infrastructure Assurance Advisory Groups (IAAGs)

### Early Warning and Public Outreach

DSD Information Security Incident Detection Reporting and Analysis Scheme (ISIDRAS)

Australian Computer Emergency Response Team (AusCERT)

AusCERT's National Information Technology Alert Service (NITAS)

### Law and Legislation

Electronic Transactions Act (1999)

Cybercrime Act (2001)

Security Legislation Amendment (Terrorism) Act (2002)

Spam Act 2003 (revised 2006)

## Austria

### Past and Present Initiatives and Policies

Security and Defense Doctrine (2001)

New Structuring of the IT Strategy of the Government (2001)

Platform Digital Austria (2005)

Austrian Citizen Card Concept

Zentrales Ausweichsystem (ZAS)

Austrian Information Security Handbook (continually updated)

Official Austrian Data Security Website

### Organizational Overview

*Public Agencies*

Ministry of Internal Affairs (BMI)

Federal Agency for State Protection and Counter-Terrorism (BVT)

Ministry of Defense (Department II/Control Department)

Ministry for Traffic, Innovation, and Technology (BMVIT)

Commission on Data Protection (DSK)

*Public Private Partnerships*

Center for Secure Information Technology Austria (A-SIT)

Stopline.at

Early Warning and Public Outreach

Computer Incident Response Coordination Austria (CIRCA)

Austrian Computer Emergency Response Team (CERT.at)

**Law and Legislation**

Information Security Law (BGBl I Nr. 23/2002) (2002)

Information Security Order (BGBl II Nr. 548/2003) (2003)

The Data Security Law (DSG) (BGBl 165/99) (2000)

Security Police Law (SPG) (BGBl 566/91 idF BGBl 85/2000)

Military Competence Law (MBG) (BGBl 86/2000)

Telecommunication Law (TKG) (BGBl 100/1997 idF BGBl 134/02)

Austrian Penal Code (StGB) (Paragraphs 118a, 119, 119a, 126a, 126b, 126c)

Penal Procedure (StPO)

Electronic Signature Law (SigG) (BGBl 1999/190) (1999)

## Brazil

**Past and Present Initiatives and Policies**

Brazilian Internet Steering Committee (CGI)

Internet Security Best Practices (2000+)

Best Practices for Internet Network Administrators

Brazilian Electronic Government Program (e-gov)

Survey on the Use of Information and Communication Technologies in Brazil – ICT Enterprises and ICT Households. (2006)

Information Society Program (2000)

**Organizational Overview**

*Public Agencies*

Computer Emergency Response Team Brazil (CERT.br)

Institutional Security Cabinet

Information Security Steering Committee (CGSI)

Ministry of Science and Technology

Ministry of Communications

Brazilian Network Information Center (NIC.br)

Center of Studies on Information and Communication Technologies (CETIC.br)

*Public Private Partnerships*

Serviço Federal de Processamento de Dados (SERPRO)

Agência Nacional de Telecomunicações (Anatel)

CERT.br partnerships

**Early Warning and Public Outreach**

Computer Security and Incident Response Team (CTIR Gov)

CERT.br (NBSO / Brazilian CERT)

Renato Archer Research Centre (CenPRA)

Brazilian Honeypots Alliance

National Education and Research Network (RNP) (RNP2 2000)

Security Incidents Attendance Center (CAIS)

**Law and Legislation**

Decree No. 3505 (2000)

Brazilian Penal Code (Amended 2000)

Senate Bill PLS 00152 (1991)

Cybercrime Bill (Potentially)

## Canada

**Past and Present Initiatives and Policies**

National Strategy and Action Plan for Critical Infrastructure (2007)

Information Sharing Practices

**Organizational Overview**

*Public Agencies*

Public Safety Canada

Integrated Threat Assessment Centre (ITAC)

Federal Provincial High-Level Forum on Emergencies

*Public Private Partnerships*

Various partnerships within the framework of the National Strategy for Critical Infrastructure

**Early Warning and Public Outreach**

Canadian Cyber Incident Response Centre (CCIRC)

Government Operations Centre (GOC)

**Law and Legislation**

Canadian Criminal Code Sections

Emergency Management Act 2007

The Department of Public Safety and Emergency Preparedness Act 2005

# Estonia

### Past and Present Initiatives and Policies

Emergency Preparedness Act (EPA) (2002)

Estonian IT Policy: Towards a More Service-Centered and Citizen Friendly State: Estonian Information Policy 2004–2006

Principles of Estonian Information Society (1998)

Estonian Information Society Strategy 2013

National Security Concept (2004)

National Information Security Policy

Information Technology in Public Administration of Estonia (2005)

Estonian ID Cards

Estonian IT Interoperability Framework

Estonian Cybersecurity Strategy

### Organizational Overview

*Public Agencies*

Ministry of Economic Affairs and Communication (MEAC)

Department of State Information System (RISO)

Estonian Informatics Centre (RIA)

Ministry of the Internal Affairs

Ministry of Defense

Estonian Computer Emergency Response Team (CERT)

The Estonian National Communications Board

Security Police Board

Information Board

*Public Private Partnerships*

Computer Protection 2009

Look@World Foundation

**Early Warning and Public Outreach**

Computer Emergency Response Team Estonia (CERT Estonia)

Infosecurity Portal

**Law and Legislation**

Emergency Preparedness Act

State Secrets Act

Personal Data Protection Act

Public Information Act

Electronic Communications Act

Information Society Services Act

Estonian Penal Code

## Finland

**Past and Present Initiatives and Policies**

Information Society Programme (2005)

National Knowledge Society Strategy for 2007-2015 (2006)

Strategy for Securing the Functions Vital to Society (2003, revised 2006)

National Security and Defense Policy (2004, 2008)

National Information Security Strategy Proposal (2002)

National Information Security Day (11th February annually)

**Organizational Overview**

*Public Agencies*

Finnish Communications Regulatory Authority (FICORA)

National Emergency Supply Agency (NESA)

Steering Committee for Data Security in State Administration (VAHTI)

Ministry of Transport and Communications

*Public Private Partnerships*

National Emergency Supply Council

Ubiquitous Information Society Advisory Board

Finnish Information Society Development Centre (TIEKE)

Early Warning and Public Outreach

Computer Emergency Response Team Finland (CERT-FI)

**Law and Legislation**

Act on the National Board of Economic Defense (NBED) (238/1960)

Act on the National Board of Economic Defense (2008)

Emergency Powers Act (1080/1991)

Bill for amendment to above act (2008)

Security of Supply Act (1390/1992) (Amended 688/2005)

Decree of the National Emergency Supply Agency (NESA) (1391/1992)

Finnish Penal Code (Chapter 38 - Amendments 578/1995 & 540/2007)

Act on Television and Radio Operations (744/1998)

Act on Provision of Information Society Services (458/2002)

Communications Market Act (393/2003)

Act on the Protection of Privacy in Electronic Communications (516/2004)

(Amendment to above act 198/2006)

## France

### Past and Present Initiatives and Policies

Government Action Program for an Information Society (PAGSI) (1997)

Expression of the Needs and Identification of Security Objects (EBIOS) (1997)

Plan for a Digital Republic within the Information Society (2002)

State Information System Security Reinforcement Plan (2004-2007)

### Organizational Overview

*Public Agencies*

Center for Training and Advanced Studies on Information Systems Security (CESSSI)

Central Directorate for Information Systems Security (DCSSI)

Central Office for the Fight against Cyber-Crime

General Secretariat for National Defense (SGDN)

Information System Security Operation center (COSSI)

Information Systems Security Training Center's (CFSSI)

Inter-Ministerial Commission for the Security of Information Systems (CISSI)

*Public Private Partnerships*

The Strategic Advisory Board on Information Technologies (CSTI)

### Early Warning and Public Outreach

Computer Emergency Response Teams (CERTs)

CERT - National Network of Telecommunications for Technology, Education, and Research (CERT-RENATER)

Computer Emergency Response Team (CERTA)

CERT - Industry, Services, and Tertiary (CERT-IST)

VIGIPIRATE Plan

Web Portal for Citizens and Small and Medium Enterprises

**Law and Legislation**

French Penal Code 2004

National Security Directive (DNS)

Decree No. 2006-212

## Germany

**Past and Present Initiatives and Policies**

National Plan for Information Infrastructure Protection (NPSI) (2005)

Critical Infrastructures Protection – Baseline Protection Concept (2005)

AG KRITIS (1997)

Comprehensive Report on Threats and Hazards (2001)

Kirchbach Report (2002)

Critical Infrastructure Protection – Risk and Crisis Management (Guideline for Enterprises and Government) (2008)

CIIP Implementation Plan (2007)

IT Security Situation in Germany (2005, 2007)

IT Security Guidelines (2004)

Secure e-Government and BundOnline (2005)

e-Government Manual and e-Government 2.0 Program (2006)

Action Plan Germany Online (2007)

International Watch and Warning Network

**Organizational Overview**

*Public Agencies*

Federal Ministry of the Interior (BMI)

Federal Office for Information Security (BSI)

Federal Agency of Civil Protection and Disaster Assistance (BBK)

Federal Criminal Police Agency (BKA)

Federal Police (BPOL)

AK KRITIS

Federal Ministry of Economics and Technology (BMWi)

Federal Chancellery

Federal Ministry of Justice (BMJ)

Federal Ministry of Foreign Affairs

Federal Ministry of Defense (BMVg)

Federal Network Agency (Bundesnetzagentur)

German Emergency Preparedness Information System (deNIS)

Joint Reporting and Notification Center (GMLZ)

*Public Private Partnerships*

Germany Secure in the Web

CIP Implementation Plan

Initiative D21

**Early Warning and Public Outreach**

International Watch and Warning Network

CERT-Verbund

IT situation center

IT Crisis Response Center

Citizens' CERT

BSI for the citizen

CERT-Bund

**Law and Legislation**

Telecommunications Act (Enacted 1996, Revised 2004, Amended 2007)

Telecommunications and Media Act (2007)

Electronic Signatures Act 2001

German Penal Code revision 2007

## Hungary

**Past and Present Initiatives and Policies**

Hungarian Green Book

National Security Strategy of the Republic of Hungary

The Hungarian Information Society Strategy

The National Information Infrastructure Development Program

Hungarian Information Security Evaluation and Certification Scheme (MIBETS)

Information Security Management Framework (MIBIK)

**Organizational Overview**

*Public Agencies*

Ministry of Economy and Transport

Prime Minister's Office - Electronic Government Center

Ministry of Defense

Ministry of Justice and Law Enforcement

National Communications Authority

Information Security Inspectorate (ISI)

National Alert Service (NAS)

The National Frequency Allocation Board

*Public Private Partnerships*

The Theodore Puskás Foundation

Early Warning and Public Outreach

Computer Security Incidents Response Team of the National Information Infrastructure Development Program (NIIF-CSIRT)

CERT-Hungary

Hun-CERT

Hungarian Financial Services Information Sharing and Analysis Center (ISAC)

e-Inclusion, be part of it! campaign

**Law and Legislation**

Hungarian Penal Code (Articles 300/C, 300/E)

Personal Data Protection Act (Act LXIII, Article 10) (1992)

Act on Electronic Commerce and Information Society Services (2001)

Act on Electronic Signature (2001)

Act no. CXII (1996)

Act no. LXXXV (1998)

Government Decree 180/2003

Ministerial Decrees 24/2004 and 27/2004

Government Decree 84/2007

## India

**Past and Present Initiatives and Policies**

National Task Force on Information Technology and Software Development (1998)

National Informatics Policy

Information Technology Action Plan (1998)

National e-Governance Plan (NeGP) (2006)

‘E-District’

Core Group on Standards for e-Governance

**Organizational Overview**

*Public Agencies*

National Information Board (NIB)

National Security Council Secretariat (NSCS)

Information Infrastructure Protection Centre (IIPC) (planned)

Ministry of Communications and Information Technology (MOC): Department of Information Technologies (DIT)

Standardisation, Testing, and Quality Certification (STQC) Directorate

Information Security Technology Development Council (ISTDC)

*Public Private Partnerships*

Indo-US Cyber Security Forum

**Early Warning and Public Outreach**

Indian Computer Emergency Response Team (CERT-In) (Additional 5 sectoral CERT’s)

**Law and Legislation**

Information Technology Act (IT Act) (2000)

Indian Penal Code

## Italy

**Past and Present Initiatives and Policies**

Working Group on Critical Information Infrastructure Protection (2003)

Report on Critical Information Infrastructure Protection: The Case of Italy (2004)

The Network Security of Critical Infrastructures (2005)

Network Security: From Risk Analysis to Protection Strategies (2005)

Guideline on Managing Local Emergencies (2006)

**Organizational Overview**

*Public Agencies*

Ministry of Communication

Permanent Working Group on Network Security and Communications Protection

Ministry of the Interior

Postal and Communications Police

Centro Nazionale Anticrimine Infrmatico per la Protezione delle Infrastrutture Critiche (CNAIPIC)

Ministry for Innovation and Technologies

Department for Innovation and Technologies (DIT)

National Technical Committee for ICT Security in the Public Administration

National Technical Committee on ICT Security

National Center for Informatics in the Public Administration (CNIPA)

*Public Private Partnerships*

Association of Italian Experts for Critical Infrastructures (AIIC)

**Early Warning and Public Outreach**

The Italian Computer Emergency Response Team (CERT-IT)

GovCERT.it

GARR Network Computer Emergency Response Team (GARR-CERT)

CERT Difesa

**Law and Legislation**

Italian Penal Code Article 420

Italian Penal Code Article 615

Privacy Law (Law 675/96 Article 15)

Legislative Decree 518

Law 155/2005 Article 7

Law 438/2001

Law 547 (23 December 1993)

Law 675 (31 December 1996)

## Japan

**Past and Present Initiatives and Policies**

Action Plan of the Basic Guidelines Toward the Promotion of an Advanced Information and Telecommunications Society (1998)

Special Action Plan on Countermeasures to Cyber-terrorism of Critical Infrastructure (2000)

Comprehensive Strategy on Information Security (2003)

Action Plan on Information Security Measures for Critical Infrastructures (2005)

First National Strategy on Information Security (2005)

Standards for Information Security Measures for the Central Government Computer Systems

**Organizational Overview**

*Public Agencies*

Cabinet Secretariat and IT Strategic Headquarters

Information Security Policy Council (ISPC)

The National Information Security Centre (NISC)

Ministry of Economy, Trade and Industry (METI)

National Police Agency

National Police Agency Technology Center

The High-Tech Crime Technology Division (HTCTD)

Ministry of Internal Affairs and Communications (MIC)

*Public Private Partnerships*

Capabilities for Engineering of Protection, Technical Operation, Analysis and Response (CEPTOAR)

**Early Warning and Public Outreach**

National Incident Response Team (NIRT)

Japan Computer Emergency Response Team Coordination Center (JPCERT/CC)

Asia Pacific Security Incident Response Coordination (AP-CIRT/AP-CERT)

Telecom Information Sharing and Analysis Center Japan (Telecom-ISAC Japan)

Cyber Force

@police

Ministry of Economy, Trade and Industry (METI)

**Law and Legislation**

Unauthorized Computer Access Law No. 128 (1999)

Japanese Penal Code Article 258

Act on Electronic Signatures and Certification Business No. 102 (2000)

Basic Law on Formation of an Advanced Information and Telecommunication Network Society (2001)

## Republic of Korea

**Past and Present Initiatives and Policies**

Report on the status of the Critical Information Infrastructure (2001)

e-Korea Vision 2006

Cyber Korea 21 (1999)

Mid- to Long-Term Roadmap for Information Protection (2005)

Basic Strategy for Ubiquitous Information Security (2006)

**Organizational Overview**

*Public Agencies*

National Cyber Security Center (NCSC)

Internet Crime Investigation Center (ICIC)

Ministry of Public Administration and Security (MOPAS)

Korea Communications Commission (KCC)

Korea Internet Security Center (KISC; KrCERT/CC)

Korean Information Security Agency (KISA)

Ministry of Knowledge and Economy

Ministry of Korea Communication Commission

Korea Spam Response Center (KSRC)

Korea IT Security Evaluation Center (KISEC)

Electronics and Telecommunications Research Institute (ETRI)

Information Security Research Division

Information and Telecommunication Infrastructure Protection Committee

Joint Working Group for Security Incident Response

*Public Private Partnerships*

National Information Security Alliance (NISA)

Financial Information Security Alliance

Information Security Practice Alliance

Korea Information Security Industry Association (KISIA)

**Early Warning and Public Outreach**

National Cyber Security Center (NCSC)

Korean Internet Security Center (KISC or KrCERT/CC)

KS-ISAC (Korean Security Information Sharing and Analysis Center)

KF-ISAC (Korea Financial Information Sharing and Analysis Center)

Korean Telecommunication Information Sharing and Analysis Center

**Law and Legislation**

National Cyber Security Management Regulation (2005)

Act on Promotion of Electronic Administration for e-Government (2001)

Digital Signatures Act (1997)

Act on Promotion of Utilization of Information and Communication Network and Information Protection (1999, Revised 2007)

Act on Personal Information Protection by Public Organization (1994)

Critical Information Infrastructure Protection Act (2001, revised 2007) (Article 28 refers to Cyber-Attacks)

Act on Private Information Protection of Public Organizations,

Act on Promotion of Electronic Administration for e-Government

Resident Registration Act

Act on Promotion of Utilization of Information and Communication Network and Information Protection (Article 62  refers to Cyber-Attacks)

e-Commerce Framework Act

The Framework Act on Information Promotion

Critical Information Infrastructure Protection Act

e-Government Act

Act on Trade Automation Promotion (Article 25 refers to Cyber-Attacks)

Act on Industrial Infrastructure

Freight Distribution Promotion Act (Sections 2 & 4 of Article 54 refer to Cyber-Attacks)

## Malaysia

**Past and Present Initiatives and Policies**

National IT Agenda (NITA)

National Information Technology Council (NITC) Strategic Agenda

e-Secure Malaysia 2005 International Conference

**Organizational Overview**

*Public Agencies*

Malaysian Communications and Multimedia Commission (MCMC)

Malaysian Administrative Modernization and Management Planning Unit (MAMPU)

Police Cybercrime Unit

Ministry of Science, Technology and Innovation (MOSTI)

Ministry of Energy, Water and Communications (MEWC)

*Public Private Partnerships*

Information Sharing Forum (ISF)

Early Warning and Public Outreach

National ICT Security and Emergency Response Center (NISER)

Malaysian Computer Emergency Response Team (MyCERT)

**Law and Legislation**

Computer Crimes Act 1997

Communications and Multimedia Act (CMA) 1998

## The Netherlands

**Past and Present Initiatives and Policies**

Critical Infrastructure Protection Project (2001)

The Digital Delta (1999)

Defence Whitepaper (2000)

BITBREUK (In Bits and Pieces) (2000)

Kwetsbaarheid op Internet – Samen werken aan meer veiligheid en betrouwbaarheid (KWINT) Report (2001)

KWINT Program (2002-2005)

Vulnerability of the Internet (2001)

Veilige Elektronische Communicatie (VEC) (2006)

Protection of the Dutch Critical Infrastructure (2002)

National Security Strategy and Work Programme (2007-2008)

**Organizational Overview**

*Public Agencies*

Ministry of the Interior and Kingdom Relations (MoI)

National Co-ordination Centre (NCC)

Dutch Ministry of Economic Affairs (EA)

Ministry of Transport, Public Works, and Water Management (V&W)

Ministry of Housing, Spatial Planning, and the Environment (VROM)

Ministry of Health, Welfare, and Sport (VWS)

General Intelligence and Security Service (AIVD)

*Public Private Partnerships*

Platform Electronic Commerce in the Netherlands (ECP.NL)

Digibewust programme (Digital Awareness)

National Continuity Plan for Telecommunications (NACOTEL)

National Continuity Consultation Platform Telecommunications (NCO-T)

The Strategic Board for CIP (SOVI)

National Advisory Centre Critical Infrastructures (NAVI)

National Infrastructure against Cyber Crime (NICC)

**Early Warning and Public Outreach**

SURFCERT (Computer Emergency Response Team of SURFnet)

GOVCERT.NL

Waarschuwingsdienst.nl

**Law and Legislation**

Penal Code

Computer Crime Law II (2006/2007)

Telecommunications Law

Criminal Code (Articles 138a/138b)

## New Zealand

**Past and Present Initiatives and Policies**

Defence Policy Framework (2000)

Protecting New Zealand's Infrastructure from Cyber-Threats (2008)

Towards a Centre for Critical Infrastructure Protection (CCIP) (2001)

Security in the Government Sector (2002)

Security Policy and Guidance Website

Standards New Zealand (SNZ)

New Zealand Security of Information Technology (NZSIT)

**Organizational Overview**

*Public Agencies*

Domestic and External Security Group (DESG)

Officials Committee for Domestic and External Security Co-ordination (ODESC)

Interdepartmental Committee on Security (ICS)

Centre for Critical Infrastructure Protection (CCIP)

Government Communications Security Bureau (GCSB)

e-Government Unit

*Public Private Partnerships*

New Zealand Security Association (NZSA)

New Zealand Computer Society's Special Interest Group on Security (NZCS SigSec)

**Early Warning and Public Outreach**

AusCERT

**Law and Legislation**

Crimes Amendment Act (2003) (Section 249-252)

## Norway

**Past and Present Initiatives and Policies**

Defense Review 2000

Defense Policy Commission 2000

A Vulnerable Society (1999-2000)

ICT Vulnerability Project

National Strategy for Information Security (2003)

Safety and Security of Society (2002)

National guidelines to strengthen information security, 2007 - 2010

Report on the Protection of Critical Infrastructures and Critical Societal Functions in Norway (2006)

An Information Society for All (2006)

### Organizational Overview

*Public Agencies*

Directorate for Civil Protection and Emergency Planning (DSB)

National Security Authority (NSM)

Norwegian Post and Telecommunications Authority (NPT)

National Information Security Co-ordination Council (KIS)

*Public Private Partnerships*

NorCERT

NorSIS

### Early Warning and Public Outreach

Norwegian Computer Emergency Response Team (NorCERT)

UNINETT CERT

Norwegian Center for Information Security (NorSIS)

Norwegian Post and Telecommunications Authority (NPT)

### Law and Legislation

The Security Act

The Electronic Communications Act

Personal Data Act

## Poland

### Past and Present Initiatives and Policies

ePoland

Aims and Directions of the Information Society Development in Poland (2001)

Plan for the Information Society Development in Poland for the years 2001–2006 – ePoland (2001) ePoland – The Strategy on the Development of the Information Society in Poland for the years 2004–2006 (2004)

The Proposed Direction of the Information Society Development to the year 2020 (2004)

E-government

Informatization of the Public Administration Bill (2003)

G2C/C2G and G2B/B2G

Polish National Foresight Program (2003)

### Organizational Overview

*Public Agencies*

Ministry of Science and Higher Education

Ministry of the Interior

*Public Private Partnerships*

The Polish Competence Center for eGovernment and eEducation

Cisco networking Academy Program (Poland)

### Early Warning and Public Outreach

Research and Academic Computer Network in Poland (NASK)

CERT Polska

CERT GOV PL

ARAKIS-gov

PIONIER-CERT

### Law and Legislation

Articles 267 to 269 of the Penal Code

# Russia

**Past and Present Initiatives and Policies**

Strategy for the Development of Information Society in Russia (2008)

Measures for Ensuring the Information Security of the Russian Federation in the Field of Information and Communication Systems use for International Information Exchange (2008)

Information Security Doctrine (2000)

National Security Concept (2000)

Electronic Russia (2001, Revised 2006)

Electronic Moscow (2002)

**Organizational Overview**

*Public Agencies*

Security Council of the Russian Federation

Federal Security Service of the Russian Federation (FSB)

Computer and Information Security Directorate

Federal Guard Service of the Russian Federation

Special Communication and Information Service

Federal Agency for Government Communications and Information (FAPSI)

Federal Technical and Export Control Service

Ministry of Information Technologies and Communications

*Public Private Partnerships*

Russian Association of Networks and Services (RANS)

PRIOR

Russia Development Gateway

**Early Warning and Public Outreach**

Russian Computer Emergency Response Team (RU-CERT)

Russian Institute for Public Networks (RIPN)

Russian Backbone Networks (RBNet)

RBNet Network Operation Center (NOC)

Institute Information Security Issues (IISI)

**Law and Legislation**

Electronic Digital Signature (EDS) Law

Russian Law on Technical Regulation

The Russian Criminal Code (1996, Revised 2004)

The Criminal Code of the Russian Federation

## Singapore

**Past and Present Initiatives and Policies**

National Emergency System (NEST)

National Critical Infrastructure Assurance (NCIA)

The Fight Against Terror – Singapore's National Security Strategy (2004)

Infocomm Security Masterplan (2005-2008)

National Authentication Infrastructure

Business Continuity Readiness Assessment Framework

Vulnerability Study of National Critical Infrastructures

**Organizational Overview**

*Public Agencies*

Ministry of Information, Communications, and the Arts (MICA)

Infocomm Development Authority of Singapore (IDA)

IDA's Infocomm Security Division (iSec)

National Infocomm Security Committee (NISC)

Singapore Police Force Technology and Crime Division (TCD)

*Public Private Partnerships*

Critical Infocomm Infrastructure Surety Assessment (CII-SA)

Information Technology Standards Committee (ITSC)

Governmentware IT Security seminar series

**Early Warning and Public Outreach**

Singapore Computer Emergency Response Team (SingCERT)

National Cyberthreat Monitoring Centre (NCMC)

**Law and Legislation**

Computer Misuse Act (CMA) 1993/1998

Computer Misuse (Amendment) Act 2003 – (New section 15A)

Electronic Transactions Act (ETA)

## Spain

**Past and Present Initiatives and Policies**

National Plan for the Protection of the Critical Infrastructures (2007)

INFO XXI: La Sociedad de la Inform@ción para todos (2000)

España.es (2003)

Ingenido2010 (Plan Avanza)

E-Government Action Plan (2003)

Public Administration Technological Modernization Plan 2004–2007 (2004)

MODERNIZA (2006)

## Organizational Overview

*Public Agencies*

Ministry of Industry, Tourism, and Trade

General Directorate of Telecommunications and Information Technologies (DGTTI)

General Directorate for the Development of the Information Society (DGDSI)

Advisory Council of Telecommunications and of the Information Society

Special Study Commission for the Development of the Information Society

Interministerial Commission of the Information Society and of the New Technologies in Spain

Red.es

Telecommunications Market Commission

State Agency for Radiocommunications

Ministry for Public Administration

e-Government Council

The Technical Committee for the Security of Information Systems and Personal Data Processing (SSITAD)

TECNIMAP Conferences

Ministry of the Interior

National Police Information Technology Crime Unit

Guardia Civil High Technology Crime Department

National Center for the Protection of the Critical Infrastructures (CNPIC)

*Public Private Partnerships*

Information Society and Telecommunications Analysis Center (ENTER)

Spanish Electronics, Information Technology, and Telecommunications Industries Association (AETIC)

### Early Warning and Public Outreach

The Antivirus Early-Warning Center (CATA)

CERT of the National Cryptology Center (CERT -CNN

Spanish National Research Network (RedIRIS) IRIS-CERT

### Law and Legislation

Spanish Penal Code (Articles; 197, 248, 264, 256, 270, 273)

Law on Citizens' Electronic Access to Public Services (2007)

## Sweden

### Past and Present Initiatives and Policies

Commission on Vulnerability and Security (Findings presented 2001 and 2005)

Bill on Swedish Security and Preparedness Policy (2002)

Information Security Policy proposals by the Committee on Information Assurance

Swedish Emergency Management Agency (SEMA) action plan for information security

### Organizational Overview

*Public Agencies*

Ministry of Defense

The Swedish Civil Contingencies Agency (SCAA)

The Swedish Emergency Management Agency (SEMA)

SEMA/Information Assurance Council

SEMA/Agency cooperation forum

Swedish Defense Materiel Administration (FMV)

Swedish Certification Body for IT Security (CSEC)

FRA/Information Security Technical Support Team

Swedish Armed Forces

Swedish Military Intelligence

Swedish Secret Service (SÄPO)

National Communications Security Group (TSA)

Centre for Asymmetric Threat Studies (CATS)

Swedish Defense Research Agency (FOI)

Ministry of Industry, Employment, and Communications

Swedish National Post and Telecom Agency (PTS)

Department of Justice

Swedish National Police Board (NPB)

*Public Private Partnerships*

SEMA Private Sector Partnership Advisory Council

SEMA Board of Information Assurance

Industry Security Delegation (NSD)

Confederation of Swedish Enterprise

Swedish Information Processing Society (DFS)

**Early Warning and Public Outreach**

Swedish IT Incident Centre (SITIC)

**Law and Legislation**

The Swedish Penal Code

Personal Data Act

Electronic Communications Act

## Switzerland

**Past and Present Initiatives and Policies**

First Report to the Federal Council on the Protection of Critical Infrastructures (2007)

Strategic Leadership Exercise (SFU 97) (1997)

INFORMO 2001 (2001)

Concept of Information Assurance (2000)

Swiss Federal Strategy Unit for Information Technology (FSUIT) model (2001)

InfoSurance (Risk Analysis 2002+)

Federal Office for National Economic Supply (NES) (Risk Analysis 2004+)
Federal Office for Civil Protection (FOCP) (Report 2009, Strategy 2011)

**Organizational Overview**

*Public Agencies*

Federal Department of Defence, Civil Protection, and Sports (DDPS)

Federal Office for Civil Protection (FOCP)

Federal Department of Finance (FDF)

Federal Strategy Unit for Information Technology (FSUIT)

Federal Office of Communications (OFCOM)

Federal Department of Economic Affairs

Federal Office for National Economic Supply (NES)

Federal Department of Finance

Federal Office of Information Technology, Systems, and Telecommunication (FOITT)

Coordination Unit for Cybercrime Control (CYCO)

Federal Office of Police (fedpol)

*Public Private Partnerships*

InfoSurance Association

Federal Office for National Economic Supply (NES): ICT Infrastructure Unit (ICT-I)

CLUSIS

**Early Warning and Public Outreach**

The Reporting and Analysis Center for Information Assurance (MELANI)

Special Task Force on Information Assurance (SONIA)

**Law and Legislation**

Swiss Penal Code (Articles 143/143bis, 144/144bis, 147)

## United Kingdom

**Past and Present Initiatives and Policies**

National Information Assurance Strategy (2003 and continually revised)

Interim Report on Government Data Security (2007) (expected final report 2008)

O'Donnell Data Handling Review

Poynter Review (expected 2008)

Walport/Thomas Review (expected 2008)

Burton Report (expected 2008)

**Organizational Overview**

*Public Agencies*

Home Office

Central Sponsor for Information Assurance (CSIA)

Centre for the Protection of the National Infrastructure (CPNI)

Combined Security Incident Response Team (CSIRTUK)

National Counter Terrorism Security Office (NaCTSO)

Counter Terrorism Security Advisers (CTSAs)

Prime Minister's Security Adviser

Civil Contingencies Secretariat (CCS)

Emergency Planning College

Cabinet Office Security Policy Division

Government Communications Headquarters (GCHQ)

*Public Private Partnerships*

Warning Advice and Reporting Points (WARPs)

The Information Assurance Advisory Council

The British Computer Society

The Internet Security Forum

The National Computing Centre

Internet Watch Foundation

The Confederation of British Industry.

The Institute of Information Security Professionals

EURIM

Royal United Services Institute

Chatham House

**Early Warning and Public Outreach**

Computer Emergency Response Team (CERT)

Combined Security Incident Response Team (CSIRTUK)

GovCertUK

Ministry of Defence CERT (MODCERT)

GetSafeOnline

**Law and Legislation**

Telecommunications (Fraud) Act (1997)

Data Protection Act (1998)

Electronic Communications Bill (2000)

Terrorism Act (2000)

## United States

**Past and Present Initiatives and Policies**

Presidential Commission on Critical Infrastructure Protection (PCCIP) Report (1997)

Presidential Decision Directives (PDD) 62 & 63 (1998)

Defending America's Cyberspace. National Plan for Information Systems Protection – An Invitation to Dialogue Version 1.0 (2000)

Establishing the Office of Homeland Security and the Homeland Security Council (EO 13228, 2001)

Critical Infrastructure Protection in the Information Age (EO 13231, 2001)

Homeland Security Presidential Directive/HSPD-7 (2003)

National Strategy for Homeland Security (2002)

National Strategy to Secure Cyberspace (NSSC)

National Strategy for Physical Protection of Critical Infrastructure and Key Assets

National Infrastructure Protection Plan (NIPP) (2006)

National Strategy for Information Sharing (2007)

**Organizational Overview**

*Public Agencies*

Critical Infrastructure Assurance Office (CIAO)

National Infrastructure Protection Center (NIPC)

Department of Homeland Security (DHS)

Office of Infrastructure Protection (OIP)

Office of Cybersecurity and Communications (CS&C)

National Communications System

National Cyber Security Division (NCSD)

Office of Emergency Communications (OEC)

Department of State

House of Representatives' Committee on Homeland Security

Subcommittee on Transportation Security and Critical Infrastructure Protection

Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology

Subcommittee on Emergency Communications, Preparedness, and Response

Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment

Senate Homeland Security and Government Affairs Committee

Federal Financial Management, Government Information, and International Security

Senate Committee on the Judiciary

Subcommittee on Terrorism, Technology, and Homeland Security

Government Accountability Office (GAO)

Department of Defense (DoD)

Computer Crime and Intellectual Property Section (CCIPS)

*Public Private Partnerships*

DHS National Infrastructure Advisory Council (NIAC)

Critical Infrastructure Partnership Advisory Council (CIPAC)

Protected Critical Infrastructure Information Program (PCIIP)

Information Technology Information Sharing and Analysis Center (IT-ISAC)

National Coordinating Center Information Sharing and Analysis Center (NCC-ISAC)

North American Electricity Reliability Council Information Sharing and Analysis Center (NERC-ISAC)

Financial Services Information Sharing and Analysis Center (FS/ISAC)

ISAC Council

InfraGard

National Cyber Security Alliance (NCSA)

Partnership for Critical Infrastructure Security (PCIS)

Cross Sector Cyber Security Working Group (CSCSWG)

Institute for Information Infrastructure Protection (I3P)

**Early Warning and Public Outreach**

Computer Emergency Response Team Coordination Center (CERT/CC)

US-CERT

National Cyber Alert System

FBI National Infrastructure Protection Center (NIPC)

Information Sharing and Analysis Centers (ISACs)

OnGuardOnline.gov

**Law and Legislation**

Federal Advisory Committee Act (FACA) (1972)

Computer Fraud and Abuse Act (CFAA) (1986)

Computer Abuse Amendments Act (1994)

USA PATRIOT Act (2001)

Homeland Security Act (HSA) (2002)

Freedom of Information Act (FOIA) (exemption included in 2002 HAS Act)

Critical Infrastructure Information Act

Protected Critical Infrastructure Information Program (PCII) (2002)

Terrorism Risk Insurance Act (2002)

## European Union (EU)

**Past and Present Initiatives and Policies**

Critical Infrastructure Protection in the Fight Against Terrorism (2004)

Green Paper on a European Program for Critical Infrastructure Protection (Green Paper on EPCIP) (2005)

Critical Communication and Information Infrastructure Protection (CIIP) Initiative (2008)

European Programme for Critical Infrastructure Protection (EPCIP)

Study for the Commission on the availability and robustness of electronic communication and infrastructures (ARECI) (Presented 2007)

Critical Infrastructure Warning Information Network (CIWIN)

European Network and Information Security Agency (ENISA)

eEurope Action Plan

**Research and Development**

Information Society Technologies (IST) (Framework Program 6 – FP6 – and Framework Program 7 – FP7)

European Security Research Program (ESRP)

European Security Research Advisory Board (ESRAB)

European Security Research and Innovation Forum (ESRIF)

Critical Information Infrastructure Research Coordination (CI2RCO)

**Law and Legislation**

The Data Protection Directive (95/46/EC) (1995)

Directive on Electronic Signatures (1999/93/CE) (1999)

Framework Directive (2002/21/EC) (2002)

European Council Framework Decision on Attacks Against Information Systems (2005/222/JHA) (2005)

Directive on the Retention of Data (2006)

Treaty of Lisbon (2007)

## Group of Eight (G8)

G8 Paris Conference on Dialogue Between the Public Authorities and Private Sector on Security and Trust in Cyberspace (2000)

Okinawa Charter on Global Information Society (2000)

G8 Principles for Protecting Critical Information Infrastructures (2003)

Best Practices for Network Security, Incident Response and Reporting to Law Enforcement (2004)

High-Tech Crime Sub-Group

International CIIP Directory

Best Practices for Law Enforcement Interaction with Victim-Companies during a Cyber-Crime Investigation (2005)

## North Atlantic Treaty Organization (NATO)

Senior Civil Emergency Planning Committee (SCEPC)

Concept Paper (2003)

Planning Boards and Committees (PB&Cs)

Civil Communication Planning Committee (CCPC)

North Atlantic Council's Action Plan on Cyber Defense

Cooperative Cyber Defense Center

Civil Protection Committee (CPC)

Ad Hoc Group on Critical Infrastructure Protection (AHG on CIP)

Critical Infrastructure Protection Concept Paper (2003)

Industrial Planning Committee (IPC)

Ad-Hoc Working Group on Energy Critical Infrastructure Protection (AHWG on CIP)

Food and Agriculture Planning Committee (FAPC)

Civil Aviation Planning Committee (CAPC)

Planning Board for Inland Surface Transportation (PBIST)

Planning Board for Ocean Shipping (PBOS)

Special Report to the NATO Parliamentary Assembly (2007)

## Organization for Economic Cooperation and Development (OECD)

Working Party on Information Security and Privacy (WPISP)

Committee for Information, Computer and Communications Policy (ICCP)

Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (2002)

Recommendation on the Protection of Critical Information Infrastructures (CII) (Potentially 2008)

OECD-APEC Analytical Report on Malware

Culture of Security Website (2003)

OECD-APEC Global Forum on Policy Frameworks for the Digital Economy (2003)

OECD Forums and Workshops

The Future of the Internet (2006)

Social and Economic Factors Shaping the Future of the Internet (2007)

Future of the Internet Economy (June 2008)

## United Nations (UN)

UN Institute for Disarmament Research (UNIDIR)

UN General Assembly Resolutions

Combating the criminal misuse of information technologies

Creation of a global culture of cybersecurity

Creation of a global culture of cybersecurity and the protection of critical information infrastructure

UN ICT Task Force

UN and the World Summit on the Information Society (WSIS)

International Telecommunication Union (ITU)

## The World Bank Group

Global Information and Communication Technologies Department (GICT)

Information Technology Security Handbook

Electronic Security: Risk Mitigation in the Financial Transactions Report (2002)

Technology Risk Checklist (2004)

BOTs – Cyber Parasites Report (2005)

Money Laundering in Cyberspace Report (2005)

# A2 Bibliography/ Important Documents

## Australia

Athol Yates. "National Security Briefing Notes" Australian Homeland Security Research Centre (2007). http://www.homelandsecurity.org.au/files/2007_e-security_agenda.pdf.

Australian Government Attorney-Generals Department. "Critical Infrastructure Protection". http://www.ag.gov.au/www/agd/agd.nsf/Page/Nationalsecurity_CriticalInfrastructureProtection.

Australian Government Attorney-Generals Department. "Security and Critical Infrastructure Division". http://www.ag.gov.au/agd/WWW/securitylawHome.nsf/Page/e-commerce_Electronic_Transactions_Act_-_Advice_for_Commonwealth_Departments.

Australian Government. "2007 E-Security National Agenda" (2007). http://www.homelandsecurity.org.au/files/2007_e-security_agenda.pdf.

Australian Government. "Security Legislation Amendment (Terrorism) Act 2002; An Act to enhance the Commonwealth's ability to combat terrorism and treason, and for related purposes" (2002). http://scaleplus.law.gov.au/html/comact/11/6499/pdf/0652002.pdf.

Commonwealth of Australia. "National Counter-Terrorism Plan (2nd ed.)" (2005). http://www.nationalsecurity.gov.au/agd/WWW/rwpattach.nsf/VAP/(5738DF09EBC4B7EAE52BF217B46ED3DA)~NCTP_Sept_2005.pdf/$file/NCTP_Sept_2005.pdf.

Department of Broadband, Communications and the Digital Economy. "Main Features of the Spam Act". http://www.dbcde.gov.au/__data/assets/pdf_file/0015/34431/Main_Features_of_the_spam_act.pdf.

Ian Dudgeon. "Australia's National Information Infrastructure: Threats and Vulnerabilities (Report)". Defence Signals Directorate (1997).

Trusted Information Sharing Network. "Critical Infrastructure Protection Projects". http://www.tisn.gov.au/agd/WWW/tisnhome.nsf/Page/CIP_Projects.

## Austria

Bundesheerreformkommission. "Endbericht" (2004).

Der Standard. "Österreichs Hochsicherheits-Datenspeicher wird 25 Jahre alt" (2007).

Resolution by the Austrian Parliament. "Security and Defence Doctrine: Analysis. Draft expert report of the 23 January 2001." http://www.austria.gv.at/2004/4/18/doktrin_e.pdf.

Walter J. Unger and Heinz Vetschera. "Cyber War und Cyber Terrorismus als neue Formen des Krieges". Österreichische Militärische Zeitschrift No. 2 (2005).

Walter J. Unger. "Angriff aus dem Cyberspace I-III". Truppendienst No. 2 (2004) No. 3 (2004), No. 4 (2004).

## Brazil

2nd COLAIS. "2nd Latin American Conference for Security Incident Response" (2006). http://www.rnp.br/en/events/colaris/.

Brazilian Internet Steering Committee, Brazilian Network Information Center (ed.) "Survey on the Use of Information and Communication Technologies in Brazil – ICT Households and ICT Enterprises 2006" (2nd ed.) (2007). http://www.cetic.br/tic/2006/indicadores-2006.pdf.

Christine Hoeppers and Klus Steding-Jessen. "Information Security in Brazil". In: Brazilian Internet Steering Committee/Mariana Balboni (ed.). Survey on the Use of Information and Communication Technologies in Brazil 2005 – ICT HOUSEHOLDS and ICT ENTERPRISIS (2006). http://www.cetic.br/tic/2005/indicadores-2005.pdf.

Claudio Pinhanez. “Internet in Developing Countries: The Case of Brazil” (1995). http://www.research.ibm.com/people/p/pinhanez/publications/netbrasil.htm.

Marc D. Goodman and Susan W. Brenner. “The Emerging Consensus on Criminal Conduct in Cyberspace”. In: UCLA Journal of Law and Technology vol. 6: issue 1 (2002).

Regina Maria De Felice Souza. “Critical telecommunication infrastructure project”. In: InfoCitel Electronic Bulletin no. 33 (2007). http://www.citel.oas.org/newsletter/2007/marzo/infraestructura_i.asp.

Robert Bruce et al. “International Policy Framework for Protecting Critical Information Infrastructure: A discussion Paper Outlining Key Policy Issues”. TNO Report 33680 Tuck School of Business at Dartmouth (2005).

Robert Shaw. “Creating Trust in Critical Network Infrastructures: The Case of Brazil”. ITU Workshop on Creating Trust in Critical Network Infrastructures (Seoul) (2002).

## Canada

Public Safety Canada. “Information Sharing and Protection under the Emergency Management Act” (2007). http://www.publicsafety.gc.ca/prg/em/cip/_fl/information-sharing-and-protection-under-the-ema-eng.pdf.

Government of Canada. “Securing an Open Society: Canada’s National Security Policy” (2004). http://www.publicsafety.gc.ca/pol/ns/secpol04-eng.aspx.

Public Safety Canada. “Working Towards a National Strategy and Action Plan for Critical Infrastructure. Draft for Consultation” (2008). http://www.publicsafety.gc.ca/prg/em/cip/_fl/nat-strat-critical-infrastructure-eng.pdf.

## Estonia

Estonian Emergency Preparedness Act (2000). http://www.legaltext.ee/text/en/X40064K1.htm.

Meelis Atonen. "Preface". In: Ministry of Economic Affairs and Communication. "Estonian IT Policy: Towards a More Service-Centered and Citizen-Friendly State. Principles of the Estonian Information Policy 2004–2006". http://www.riso.ee/en/files/Principles%20of%20the%20Estonian%20Information%20Policy%202004–2006_0.pdf.

Ministry of Economic Affairs and Communications of Estonia. "Information Technology in Public Administration of Estonia 2005" (2005). http://www.riso.ee/en/pub/yearbook_2005.pdf.

Ministry of Economic Affairs and Communications. "Estonian Information Society Strategy 2013". http://www.riso.ee/en/files/IYA_ENGLISH_v1.pdf.

Estonian Government. "National Security Concept of the Republic of Estonia 2004". http://merln.ndu.edu/whitepapers/Estonia-2004.pdf.

## Finland

Advisory Committee for Information Security. "National Information Security Strategy Proposal" (2002). http://www.ficora.fi/englanti/document/infos.pdf.

Finnish Government. "National Knowledge Society Strategy for 2007-2015" (2006). http://www.tietoyhteiskuntaohjelma.fi/esittely/en_GB/introduction/_files/76222690188788831/default/Strategia.

Finnish Government Policy Programmes. "Information Society Programme" (2005). http://www.tietoyhteiskuntaohjelma.fi/esittely/en_GB/introduction/_files/11233297000000607/default/tietoyhteiskuntaojelma_en_2005.pdf.

Finnish Government. "Strategy for Securing the Functions Vital to Society" (2003). http://www.defmin.fi/files/168/2587_2047_Government_Resolution_On_Securing_The_Functions_Vital_To_Society_1_.pdf.

Finnish Government. "Strategy for Securing the Functions Vital to Security" (2006).

http://www.defmin.fi/files/858/06_12_12_YETTS__in_english.pdf.

Ministry of Justice. "Act on the National Board of Economic Defence (NBED)" (238/1960) (unofficial English translation). http://www.finlex.fi/fi/laki/alkup/1960/19600238.

Ministry of Justice. “Emergency Powers Act” (1080/1991) (unofficial English translation). http://www.finlex.fi/en/laki/kaannokset/1991/en19911080.pdf.

Ministry of Justice. “Government decision on the Goals of Security of Supply” (2002). http://www.finlex.fi/fi/laki/alkup/2002/20020350

Ministry of Justice. “Penal Code Chapter 38 Amendment” (578/1995) (unofficial English translation). http://www.finlex.fi/pdf/saadkaan/E8890039.PDF

Ministry of Justice. “Security of Supply Act” (1390/1992) (unofficial English translation). http://www.finlex.fi/fi/laki/ajantasa/1992/19921390.

Ministry of Justice. “The Amendment of the Security of Supply Act” (688/2005).http://www.finlex.fi/fi/esitykset/he/2005/20050044.

Ministry of Justice. “The Decree of the National Emergency Supply Agency (NESA) (1391/1992). http://www.finlex.fi/fi/laki/ajantasa/1992/19921391.

## France

Neue Zürcher Zeitung. “Weniger Personal, mehr Geld für militärische Raumfahrt. Frankreichs Präsident Sarkozy präsentiert Pläne für den Umbau der Armee” (2008). http://www.nzz.ch/nachrichten/international/frankreich_sarkozy_armee_plaene_1.760795.html.

Prime Minister’s Office. “Serveur thématique sur la sécurité des systèmes d’information”. http://www.ssi.gouv.fr/fr/confiance/ebiospresentation.html.

Prime Minister’s Office. “State Information System Security Reinforcement Plan (2004–2007)” (2004). http://www.ssi.gouv.fr/site_documents/PRSSI/PRSSI-en.pdf.

RAND Europe Dependability Development Support Initiative (DDSI). “National Dependability Policy Environments; France” (2002).

Service d’Information du Gouvernement. “Four years of government measures to promote the information society” (2001).

## Germany

AG KRITIS. “Informationstechnische Bedrohungen für Kritische Infrastrukturen in Deutschland. Kurzbericht der Ressortarbeitsgruppe KRITIS” (Entwurfsversion 7.95) (1999).

Federal Ministry of the Interior. “National Plan for Information Infrastructure Protection” (2005). http://www.bmi.bund.de/cln_012/nn_148138/Internet/Content/Common/Anlagen/Nachrichten/Pressemitteilungen/2005/08/National__Plan__for__Information__Infrastructure__Protection,templateId=raw,property=publicationFile.pdf/National_Plan_for_Information_Infrastructure_Protection.

Federal Ministry of the Interior. “Protection of Critical Infrastructures – Baseline Protection Concept” (2005). http://www.bmi.bund.de/nn_121894/Internet/Content/Common/Anlagen/Broschueren/2007/Basisschutzkonzept__kritische__Infrastrukturen__en,templateId=raw,property=publicationFile.pdf/Basisschutzkonzept_kritische_Infrastrukturen_en.pdf.

Federal Ministry of the Interior. “Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen” (2007). http://www.bmi.bund.de/cln_012/nn_122688/Internet/Content/Broschueren/2007/Kritis.html.

Federal Ministry of the Interior. “Zweiter Gefahrenbericht der Schutzkommission beim Bundesminister des Innern. Bericht über mögliche Gefahren für die Bevölkerung bei Grosskatastrophen und im Verteidigungsfall” (2001). http://www.bbk.bund.de/cln_027/nn_402322/SharedDocs/Publikationen/Publikationen_20Forschung/Band_2048,templateId=raw,property=publicationFile.pdf/Band%2048.pdf.

Federal Ministry of Justice. “Bundesgesetzblatt” (Teil I Nr. 38) (2007).http://www.computerundrecht.de/6758.html.

Federal Office for Information Security (BSI). “IT Security Guidelines: IT Baseline Protection in Brief” (2004). http://www.bsi.bund.de/english/gshb/guidelines/guidelines.pdf.

Federal Office for Information Security (BSI). “The IT Security Situation in Germany 2007” (2007). http://www.bsi.bund.de/english/publications/securitysituation/Lagebericht_2007_englisch.pdf.

Günther Ennen. "CERT-Bund – eine neue Aufgabe des BSI". In: KES Zeitschrift für Kommunikations- und EDV-Sicherheit. Bundesamt für Sicherheit in der Informationstechnik (BSI) (2001).

Official Journal of the European Union (L 69/67-71) (2005).http://eur-lex.europa.eu/JOHtml.do?uri=OJ:L:2005:069:SOM:en:html.

Sächsischen Staatsregierung. "Bericht der Unabhängigen Kommission der Sächsischen Staatsregierung. Flutkatastrophe 2002" (Saxony 2003). http://home.arcor.de/schlaudi/Kirchbachbericht.pdf.

## Hungary

Ákos Detreköi. "Information Society in Hungary". http://www.agile2006.hu/papers/detrekoi_agile_welcome.pdf.

Council of Europe. "Project on Cybercrime, Cybercrime Legislation – Country Profile: Hungary" (2007). http://www.coe.int/cybercrime.

European Commission. "EGovernment in Hungary, Legal Framework" (2008). http://ec.europa.eu/egov.

Government of Hungary. "The National Security Strategy of the Republic of Hungary". http://www.mfa.gov.hu/kum/en/bal/foreign_policy/security_policy/national_sec_strategy_of_hun.htm.

Suba, Ferenc and János Drencsán. "Hungary's National NIS Projects". In: ENISA Quarterly no. 12 (2005).

## India

Ministry of Communications and Information Technology. Department of Information Technology. "Annual Report 2006-2007". http://mit.gov.in/download/annualreport2006-07.pdf.

National Task Force on Information Technology and Software Development. "Information Technology Action Plan, Preamble" (1998). http://it-taskforce.nic.in/infplan.htm#aa.

(Presentation) Commander Mukesh Saini. National Security Council. The Indo-US Cyber-Security Forum in Washington, DC (9-10 November 2004).

(Presentation) Shri R. Chandrashekhar "On The National E-Governance Plan - Approach & Key Components". National e Governance Plan - Workshop with States and UTs New Delhi (11-12 March 2005). http://www.mit.gov.in/default.aspx?id=115.

Vineeta Mishra. "Critical sectors to be Y2K ready in time: govt report". India Times (19 October 1999). http://www.apnic.net/mailing-lists/s-asia-it/archive/1999/10/msg00050.html.

## Italy

Cybercrime Law. "Italy". http://www.cybercrimelaw.net/laws/countries/italy.html.

Minister for Innovation and Technologies. "Government Guidelines for the Development of the Information Society" (2002). http://www.innovazione.gov.it/eng/intervento/allegati/docu_base130202.pdf.

Ministry of Communications. "Network Security – From Risk Analysis to Protection Strategies" (2005). http://www.isticom.it/documenti/news/pub_002_eng.pdf.

Ministry of Communications. "Network Security in Critical Infrastructures" (2005). http://www.isticom.it/documenti/news/pub_003_eng.pdf.

## Japan

Advanced Information and Telecommunications Society Promotion. "Outline of the First Follow-up of the Action Plan of the Basic Guidelines Toward the Promotion of an Advanced Information and Telecommunications Society" (2000). Provisional translation: http://www.kantei.go.jp/foreign/it/2000/0706outline.html.

Information Securirty Policy Council. "Action Plan on Information Security Measures for Critical Infrastructures" (2005). http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng.pdf.

Information Security Policy Council "Secure Japan 2006: First Step Towards a Trustworthy Society" (2006). http://www.nisc.go.jp/eng/pdf/sj2006_eng.pdf.

Information Security Policy Council. "Secure Japan 2007: upgrading of information security measures in order to create an environment in which people can use IT safely and securely" (2007). http://www.nisc.go.jp/eng/pdf/sj2007_eng.pdf.

Information Security Policy Council. "The First National Strategy on Information Security – Toward the realization of a trustworthy society" (2006). http://www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf.

IT Strategic Headquarters. "e-Japan 2002 Program - Basic Guidelines Concerning the IT Priority Policies in FY2002" (2001). http://www.kantei.go.jp/foreign/it/network/0626_e.html.

Ministry of Internal Affairs and Communications, "Information and Communications in Japan." (2007). http://www.johotsusintokei.soumu.go.jp/whitepaper/eng/WP2007/contents.pdf.

National Information Security Center. "Japanese Government's Efforts to Address Information Security issues – Focusing on the Cabinet Secretariat's Efforts" (2007). http://www.nisc.go.jp/eng/pdf/overview_eng.pdf.

Prime Minister of Japan and His Cabinet. "Special Action Plan on Countermeasures to Cyber-terrorism of critical infrastructure" (2000). Provisional translation: http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN009986.pdf.

"Special Action Plan on Countermeasures to Cyber-terrorism of Critical Infrastructure (Summary)". http://www.kantei.go.jp/foreign/it/security/2001/cyber_terror_sum.html.

Yutaka Hayami (METI). "Realizing a World-Class Highly Reliable Society" (2004). http://www.aavar.org/2004web/AVAR2004/Presentations/ps011.ppt.

## Republic of Korea

Chaeho Lim. "Creating Trust in Critical Network Infrastructures: Korean Case Study" (PAPER) ITU Workshop on Creating Trust in Critical Network Infrastructures (2002). http://www.itu.int/osg/spu/ni/security/docs/cni.05.doc.

Chaeho Lim. "Creating Trust in Critical Network Infrastructures: Korean Case Study" (SLIDES) (2002). http://www.itu.int/osg/spu/ni/security/workshop/presentations/cni.14.pdf.

Heung Youl Youm. "Countermeasures for Combating Cyber Attacks in Korea" (2007). http://www.itsc.org.sg/pdf/6thmtg/Korea-Malaysia-Singapore-S.pdf.

Korean Information Security Agency (KISA). "Report on the status of the Critical Information Infrastructure" (2001). http://www.kisa.or.kr.

Ministry of Information and Communication. "e-Korea Vision 2006. Advancing the Information Infrastructure". http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN008975.pdf.

Ministry of Information and Communication. "e-Korea Vision 2006. The Third Master Plan for Informatization Promotion 2002-2006" (2002). http://www.nca.or.kr/homepage/ehome/ehome.nsf/0/4f84e7068921413ec9256ce80024c20a/$FILE/e-Korea%20Vision%202006.pdf.

National Computerisation Agency. "Informatization White Paper 2006" (2006). http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN027266.pdf.

Yang-Shin Cha. "Korea's Approach to Network Security" (2002). http://www.itu.int/osg/spu/ni/security/workshop/presentations/cni.21.pdf.

## Malaysia

Anti-Spam Activities in Malaysia – Current Situation, Regulatory Environment and Future Developments. Presentation held at the ITU Global Symposium for Regulators (Geneva 8-10 December 2004). http://www.itu.int/ITUD/treg/Events/Seminars/2004/GSR04/documents/ NurAbdullah.pdf.

Bistamam Siru Abdul Rahman (MCMC). Malaysia's Approach to Network Security. Presentation held at ITU Workshop on "Creating Trust in Critical Network Infrastructures" (Seoul, May 2002). http://www.itu.int/osg/spu/ni/security/workshop/presentations/cni.19.pdf.

Malaysia Communications and Multimedia Act 1998. http://www.mcmc.gov.my/mcmc/the_law/ViewAct.asp?cc=4446055&lg=e&arid=900722.

Malaysian Administrative Modernisation and Management Planning Unit, Prime Minister's Department (MAMPU). Malaysian Public Sector Management of Information & Communications Technology Security Handbook (MyMis) (2002). http://www.mampu.gov.my/mampu/bm/program/ict/mymis/mymis.htm.

## The Netherlands

Cybercrime Law. "The Netherlands". http://www.cybercrimelaw.net/laws/countries/netherlands.html.

Dick Schoof. "National Security Strategy – The Netherlands" (Presentation) (September 2007). http://www.hightechconnections.org/files/HTC_homeland_security_Dick_Schoof.pdf.

Eric Luiijf. "SCADA Security Good Practices for the Dutch Drinking Water Sector" report TNO DV 2008 C096) (2008).

Eric Luiijf and Marieke Klaver. "In Bits and Pieces: Vulnerability of the Netherlands ICT-Infrastructure and Consequences for the Information Society" (translation of the Dutch Infodrome essay "'BITBREUK', de kwetsbaarheid van de ICT-infrastructuur en de gevolgen voor de informatiemaatschappij") (2000).

Eric A.M Luiijf, Helen H. Burger and Marieke H.A. Klaver. "Critical Infrastructure Protection in The Netherlands: A Quick-scan". In: Gattiker, Urs E., Pia Pedersen, and Karsten Petersen (eds.): "EICAR Conference Best Paper Proceedings 2003". http://cipp.gmu.edu/archive/2_NetherlandsCIdefpaper_2003.pdf.

House of Parliament (Tweede Kamer) 2006–2007, 26 643, nr. 85.

Marjolijn Durinck and Willem Boersma. "Public-Private Partnership in Awareness Raising: Internet Safety Awareness in The Netherlands." http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_public_awareness_raising_in_the_netherland_boersma_durincks.pdf.

Ministry of Defence. "Defensienota 2000" (1999).

Ministry of the Interior and Kingdom Relations. "Critical Infrastructure Protection in the Netherlands" (2003). http://cipp.gmu.edu/archive/NetherlandsCIreport_0403.pdf.

Ministry of the Interior and Kingdom Relations. "Critical Infrastructure Protection" (2005).

Ministry of the Interior and Kingdom Relations. "National Security Strategy and Work Programme 2007-2008". http://www.minbzk.nl/aspx/download.aspx?file=/contents/pages/88474/natveiligh.bwdef.pdf.

Ronald De Bruin. "From Research to Practice: A Public-Private Partnership Approach in the Netherlands on Information Infrastructure Dependability". Dependability Development Support Initiative (DDSI) Workshop (2002).

## New Zealand

Cybercrimelaw. "New Zealand" http://www.cybercrimelaw.net/laws/countries/new_zealand.html.

Department of the Prime Minister and Cabinet. "Security in the Government Sector" (2002). http://www.security.govt.nz/sigs/index.html.

Domestic and External Security Group. "Securing our Nation's Safety: How New Zealand manages its security and intelligence agencies" (2000). http://www.dpmc.govt.nz/dpmc/publications/securingoursafety/index.html.

Hon. Trevor Mallard. "Government Addressing Cyber Crime & IT Based Threats" (2001). http://www.ccip.govt.nz/about-ccip/background/mediarelease-cybercrime.pdf.

Ministry of Defence. "New Zealand Defence Policy" (2000). http://www.defence.govt.nz/defence-policy.html.

Minister of State Services. "Government addressing cyber-crime and IT-Based Threats" (2001). http://www.ccip.govt.nz/about-ccip/background/mediarelease-cybercrime.pdf.

Phil Goff. "Protecting New Zealand's Borders – The Government's Approach" (2007). http://www.beehive.govt.nz/speech/protecting+new+zealand%E2%80%99s+borders+%E2%80%93+government%E2%80%99s+approach.

State Services Commission. "E-Government: Protecting New Zealand's Infrastructure From Cyber Threats" (2000). http://www.ccip.govt.nz/about-ccip/background/niip-report-final.pdf.

State Services Commission. "Towards a Centre for Critical Infrastructure Protection" (2001). http://www.ccip.govt.nz/about-ccip/background/ccip-final-report.pdf.

## Norway

Avgitt til Justis- og Politidepartementet. "Et sårbart samfunn Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet" (2000). http://www.regjeringen.no/Rpub/NOU/20002000/024/PDFA/NOU200020000024000DDDPDFA.pdf.

Commission for the Protection of Critical Infrastructures. "Protection of Critical Infrastructures and Critical Societal Functions in Norway" (2006). English Summary: http://www.regjeringen.no/upload/JD/Vedlegg/Norwegian_CIP_Commision_Report_NOU_2006_No_6_English_summary.pdf.

Jan Hovden. "Public Policy and Administration in a Vulnerable Society: Regulatory Reforms Initiated by a Norwegian Commission" Journal of Risk Research (7:6 629-641) (2004).

Ministry of the Justice and the Police. "Statement on Safety and Security of Society" (2002). (Report No. 17 to the Storting) (2000-2001). http://www.regjeringen.no/en/dep/jd/Documents-and-publications/Reports/Reports/2002/Statement-on-Safety-and-Security-of-Soci.html?id=420173.

Ministry of Government Administration and Reform "An information Society for All". (Report No. 17 to the Storting) (2006-2007). http://www.regjeringen.no/en/dep/fad/Documents/Government-propositions-and-reports-/Reports-to-the-Storting-white-papers/20062007/Report-No-17-2006---2007-to-the-Storting.html?id=441497.

Norwegian Government. "National Strategy for Information Security: Challenges, Priorities and Measures." (2003). http://webdomino1.oecd.org/COMNET/STI/IccpSecu.nsf/viewHtml/index/$FILE/Norway_Nat%20strat%20info%20security.pdf.

The Office of the Auditor General. "The Office of the Auditor General's Investigation into the Authorities' Work to Secure IT Infrastructure." (2006). http://www.riksrevisjonen.no/NR/rdonlyres/2E806C9B-CB55-4F65-9BBA 09D23E3D6044/0/Eng_Doc_3_4_2005_2006.pdf.

## Poland

Elbzbieta Stefanczyk. "Polish libraries in the information society". http://www.svkbb.sk/colloquium/zbornik/data/stefanczyk.pps.

Mieczyslaw Borysiewicz and Slawomir Potempski. "Critical Infrastructure Protection: actions to be implemented shortly". In: ECN European CIIP Newsletter Vol.1 No. 2 (2005). http://www.irriis.org/ecn/European%20CIIP%20Newsletter%20No%202.pdf.

Ministry of Scientific Research and Information Technology. "ePoland - The Strategy on the Development of the Information Society in Poland for the years 2004-2006" (2004). http://www.itu.int/wsis/stocktaking/scripts/documents.asp?project=1103559107&lang=en.

Piatkowski, Marcin. "Information Society in Poland. A Prospective Analysis." Transformation, Integration and Globalization Economic Research, Leon Kozminski Academy of Entrepreneurship and Management, Warsaw (2004). http://www.tiger.edu.pl/onas/piatkowski/Information_Society_in_Poland_A_Prospective_Analysis.pdf.

Skulimowski, Andrzej M.J. “The Information Society in Poland: recent developments and future perspectives”. http://www.scholze-simmel.at/starbus/r_d_ws1/poland.pdf.

## Russia

Arkadiy Kremer. “Cyber Security in Russia” (Presentation held at ITU-T Cybersecurity Symposium, Florianopolis) (4 October 2004). http://www.itu.int/ITU-T/worksem/cybersecurity/presentations/CsecS2-p2-kremer.ppt.

Baker and McKenzie. “Legal Alert. Electronic Digital Signature Law” (2002). http://www.bakernet.com/ecommerce/Russia-E-Signature-Alert.doc.

Federal Target Program. “Electoral Russia (years 2002 – 2010)” (2002). http://www.developmentgateway.org/download/182707/erussia_final_en_jr28-02.doc.

GeoPowers. “Russland” (2000). http://www.geopowers.com/Machte/Russland/russland.html.

Gordon Bennet. “FAPSI - The Federal Agency of Government Communications & Information”. http://www.agentura.ru/english/dosie/brit/fapsi.

Ian Leigh. “Information Security Doctrine of the Russian Federation.” http://www.isn.ethz.ch/news/dossier/ssg/pubs/books/FluriSulakshin/05A_LEIGH.pdf.

L. Thomas Timothy. “Information Security Thinking: A Comparison of U.S., Russian and Chinese Concepts” (2001). http://fmso.leavenworth.army.mil/documents/infosecu.htm.

L. Thomas Timothy. “Russian Views on Information Based Warfare”. http://www.shaneland.co.uk/ewar/docs/dissertationsources/russiansource1.pdf.

Mikhail B Ignatyev. “Analysis of the Threat of Cyberattacks to Major Transportation Control Systems in Russia” (2004). http://www.nap.edu/openbook/0309089719/html/85.html#pagetop.

Ministry of Information Technologies and Communications of the Russian Federation. “Regulation on the RF Ministry for communications and informatization”. http://english.minsvyaz.ru/site.shtml?id=17&page=1.

Sergey Filippov. “Policy for ICT Adoption in Moscow – ‘Electronic Moscow’ Programme” (2004). http://www.telecities.nl/call_for_papers/paper_sergey_filippov_-_electronic_moscow.pdf.

Vladimir Putin. “Doctrine of the Information Security of the Russian Federation” (no. Pr-1895) (2000). http://www.medialaw.ru/e_pages/laws/project/d2-4.htm.

Yevgenia Albats. “Information Security Doctrine Redux” (The Moscow Times) (14 September 2000). http://www.themoscowtimes.com/stories/2000/09/14/007.html.

Yuri Hohlov. “e-Russia and e-Moscow Programs”. Institute of the Information Society. http://www.tedbr.com/apresentacoes/e-Brasil/e-russia_and_e-moscow_programs_2005-10-14.pdf.

## Singapore

Asia-Pacific Conference on Cybercrime and Information Security. “Country Report on Singapore” (2002). http://www.unescap.org/icstd/cybercrime%20meeting/Presentations/Session%203%20-%20country%20and%20org.%20reports/Singapore/Singapore%20written%20report.doc.

Arabinda Acharya. “Defending Singapore’s Vital Infrastructure Against Terrorism” Institute of Defence and Strategic Studies (2004). http://se1.isn.ch/serviceengine/FileContent?serviceID=PublishingHouse&fileid=1A3BA5E1-F1AA-226F-7CEC-C0096894A6ED&lng=en.

Clement Leong. “Security Initiatives in the Computerisation of the Singapore Government”. http://www.gsa.gov/gsa/cm_attachments/GSA_DOCUMENT/13-Homeland-Security-Singapore_R2GVIV_0Z5RDZ-i34K-pR.htm.

Ho Peng Kee. Senior Minister Of State For Law and Home Affairs. Speech at the “Monoc Seminar” (2002). http://app3.mha.gov.sg/news_details.aspx?nid=876.

IDA press release. “Singapore Gears Up for Cyber Security. Three-year Infocomm Security Masterplan Unveiled” (2005). http://www.ida.gov.sg/News%20and%20Events/20050712110643.aspx?getPagetype=2.

iGov.sg. "2006 Report on Singapore e-Government" (2006). http://www.igov.gov.sg/NR/rdonlyres/0D5EE595-4D44-4B02-948C-07FB18239313/0/2006ReportonSporeeGov.pdf.

Lee Boon Yang. Minister for Information, Communications, and the Arts. Speech at the 17th Annual FIRST Conference (2005). http://www.mica.gov.sg/pressroom/press_050629.html.

National Security Coordination Centre. "The Fight Against Terror – Singapore's National Security Strategy". (2004). http://app-stg.nscc.gov.sg/data/25fight-terror.pdf.

Peter Ho. "Singapore's Strategy in Securing Cyberspace." Infocomm Security Seminar (2005). http://www.ida.gov.sg/News%20and%20Events/20050717164621.aspx?getPagetype=21.

Valerie D Costa. "Singapore's Internet Policy". Workshop on Internet Governance at the National Level (2005). http://www.wgig.org/docs/Singapore%20Internet%20Policy%2019%20Jul%2005.ppt.

## Spain

"Action Program for the development of an Information Society in Spain". http://www.gemeinsamlernen.de/euconet/Projects/Spanien/espana?language=en.

Information Society Technologies. "National Dependability Policy Environments SPAIN" (IST-2000-29202) (2002).

Invertia. "El Congreso insta al Gobierno a concluir en seis meses el catálogo de infraestructuras críticas" (12 July 2007). http://www.invertia.com/noticias/noticia.asp?subclasid=&clasid=&idNoticia=1764166.

Spanish Ministry of Public Administration "Law on Citizens' Electronic Access to Public Services" (2007). http://www.map.es/iniciativas/mejora_de_la_administracion_general_del_estado/moderniza/Administracion_Electronica/parrafo/04/document_es/a7%20(121-116)%202007-06-14%20Texto_definitivo_aprobado_Congreso.pdf.

## Sweden

Government Offices of Sweden. "Informationssäkerhetspolitik – Organisatoriska konsekvenser" (SOU 2005:71) (2005). http://www.regeringen.se/sb/d/108/a/49614.

Government Offices of Sweden. "Organizational consequences" (SOU 2005:71) (2005). http://www.regeringen.se/sb/d/108/a/49614.

Government Offices of Sweden. "Secure information – proposals on information security policy" (SOU 2005:42) (2005). http://www.regeringen.se/sb/d/108/a/44381.

Ministry of Defence. "Vulnerability and Security in a New Era – A Summary" (SOU 2001:41) (2001). http://www.sweden.gov.se/sb/d/574/a/25658.

SEMA's Educational Series 2008:2. "Large scale Internet attacks. The Internet attack on Estonia. Sweden's emergency preparedness for Internet attacks" (2008). http://www.krisberedskapsmyndigheten.se/upload/3040/Large%20scale%20Internet%20attacks_utb-ser_2008-2.pdf.

## Switzerland

Federal Office for Civil Protection. "Erster Bericht an den Bundesrat zum Schutz Kritischer Infrastrukturen" (2007).

Rolph L. Haefelfinger. "The Swiss Perspective on Critical Infrastructure" (Presentation at the PfP Seminar on Critical Infrastructure Protection and Civil Emergency Planning – New Concepts for the 21st Century) (2003).

Ruedi Rytz and Jürg Römer. "MELANI – An Analysis Centre for the Protection of Critical Infrastructures in the Information Age", (Paper for the Workshop on Critical Infrastructure Protection) (2003).

Swiss Federal Chancellery. "Strategische Führungsübung 1997 – Kurzdokumentation über die SFU 97" (1997).

Swiss Federal Strategy Unit for Information Technology. "Vulnerable Information Society – Challenge Information Assurance" (2002).

## United Kingdom

United Kingdom Cabinet Office. “Civil Contingencies Secretariat”. http://www.cabinetoffice.gov.uk/secretariats/civil_contingencies.aspx.

The Confederation of British Industry. “Our Mission”. http://www.cbi.org.uk/ndbs/staticpages.nsf/StaticPages/home.html/?OpenDocument.

## United States

Centre for Democracy and Technology. “Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act”. http://www.cdt.org/security/usapatriot/011026usa-patriot.pdf.

Department of Homeland Security. “Information Technology: Critical Infrastructure and Key Resources Sector-Specific Plan as Input to the National Infrastructure Protection Plan” (2007).

Department of Homeland Security. “National Infrastructure Protection Plan” (2006). http://cipp.gmu.edu/archive/NIPP_Plan6-06.pdf.

George W Bush. “Critical Infrastructure Protection in the Information Age” (Executive Order 13231) (2001). http://www.fas.org/irp/offdocs/eo/eo-13231.htm.

George W Bush. “Establishing the Office of Homeland Security and the Homeland Security Council” (Executive Order 13228) (2001). http://www.fas.org/irp/offdocs/eo/eo-13228.htm.

Office of Homeland Security. “National Strategy for Homeland Security” (2002). http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf.

The President’s Commission on Critical Infrastructure Protection (PCCIP). “Critical Foundations: Protecting America’s Infrastructures” (1997).

The White House. “Homeland Security Presidential Directive/HSPD-7” (2003). http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html.

The White House. “National Strategy for Homeland Security” (2007). http://www.whitehouse.gov/infocus/homeland/nshs/NSHS.pdf.

The White House. "National Strategy for Information Sharing" (2007). http://www.whitehouse.gov/nsc/infosharing/NSIS_book.pdf.

The White House. "National Strategy for the Physical Protection of Critical Infrastructures and Key Assets" (2003).

The White House. "National Strategy to Secure Cyberspace" (2003). http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf.

United States Government Accountability Office (GAO). "Critical Infrastructure Protection and Improving Information Sharing with Infrastructure Sector"s (GAO-04-780) (2004). http://www.gao.gov/new.items/d04780.pdf.

United States Government Accountability Office (GAO). "Critical Infrastructure Protection. Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilites" (GAO-05-434) (2005). http://www.gao.gov/new.items/d05434.pdf.

United States Government Accountability Office (GAO). "Report to the Congressional Requesters, Information Security. Emerging Cybersecurity Issues Threaten Federal Information Systems" (GAO-05-231) (2005). http://www.gao.gov/new.items/d05231.pdf.

William J Clinton. "Defending America's Cyberspace: National Plan for Information Systems Protection. An Invitation to a Dialogue. Version 1.0" (2000).

William J Clinton. "Protecting America's Critical Infrastructures: Presidential Decision Directive 63." (1998). http://www.usdoj.gov/criminal/cybercrime/white_pr.htm.

## European Union (EU)

Alain Esterle, Hanno Ranck, and Burkard Schmitt (edited by Burkard Schmitt). "Information security. A new challenge for the EU". Chaillot Paper no. 76 (2005). http://www.iss.europa.eu/uploads/media/cp076.pdf.

Commission of the European Communities "Commission Decision of 22 April 2005 establishing the European Research Advisory" Official Journal of the European Union. Board (2005/516/EC) (2005).

Commission of the European Communities. "Critical Infrastructure Protection in the Fight against Terrorism" (COM(2004)702) (2004). http://europa.eu.int/comm/justice_home/doc_centre/criminal/terrorism/doc/com_2004_702_en.pdf.

Commission of the European Communities. "Green Paper on a European Programme for Critical Infrastructure Protection" (COM(2005) 576) (2005). http://www.libertysecurity.org/IMG/pdf/EC_-_Green_Paper_on_CI_-_17.11.2005.pdf.

Council of the European Union, "Council Resolution of 22 March 2007 on a Strategy for a Secure Information Society in Europe". Official Journal of the European Union. (C68/01) (2007). http://eur-lex.europa.eu/LexUriServ/site/en/oj/2007/c_068/c_06820070324en00010004.pdf.

European Commission Information Society. "Availability and Robustness of Electronic Communication Infrastructures (ARECI) Study". http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/areci_study/index_en.htm9.

European Commission Justice and Home Affairs. "Freedom, Security and Justice; Protect Infrastructures". http://ec.europa.eu/justice_home/fsj/terrorism/protection/fsj_terrorism_protection_infrastruct_en.htm.

European Commission Justice and Home Affairs. "Proposal for a Directive of the Council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection" (2006). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52006PC0787:EN:NOT.

European Network and Information Security Agency (ENISA). Work Programme 2008: "Build on Synergies – Achieve Impact." http://www.enisa.europa.eu/doc/pdf/management_board/decisions/enisa_wp_2008.pdf.

## Group of Eight (G8)

Deutsch Auswärtiges Amt. "Die Rolle der G8 bei der Bekämpfung des Internationalen Terrorismus". http://www.auswaertigesamt.de/diplo/de/Aussenpolitik/Themen/TerrorismusOK/TerrorismusbekaempfungG8.html#t2l.

G8 Justice and Interior Ministers. “Best Practices for Network Security, Incident Response and Reporting to Law Enforcement” (2004). http://www.usdoj.gov/ag/events/g82004/G8_Best_Practices_Network_Security.pdf.

G8 Justice and Interior Ministers. “Communiqué” (2004). http://www.usdoj.gov/ag/events/g82004/Communique_2004_G8_JHA_Ministerial_051204.pdf.

G8 Justice and Interior Ministers. “G8 Principles for Protecting Critical Information Infrastructures” (2003). http://www.usdoj.gov/ag/events/g82004/G8_CIIP_Principles.pdf.

NISCC. “G8 Principles for Protecting Critical Information Infrastructures” NISCC Quarterly (2003).

United Kingdom Home Office. “Challenges Associated with Emerging Technologies For Law Enforcement Wireless Local Area Networks (WLANs)” (2004). http://www.homeoffice.gov.uk/documents/G8-WLANBstPrcNov04.pdf?version=1.

United Nations General Assembly. “Creation of a global culture of Cybersecurity and the protection of critical information infrastructures” [Resolution 58/199] (2004). http://www.itu.int/osg/spu/cybersecurity/docs/UN_resolution_58_199.pdf.

## North Atlantic Treaty Organization (NATO)

Lord Jopling. “162 CDS 07 E rev 1 – The Protection of Critical Infrastructures.” (2007). http://www.nato-pa.int/default.asp?SHORTCUT=1165.

NATO.“Bucharest Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Bucharest on 3 April 2008.” (2008). http://www.summitbucharest.ro/en/doc_201.html.

Vladimir Socor. “NATO creates Cyber Defense Center in Estonia”. Eurasia Daily Monitor, Vol. 5, No. 93 (2008). http://www.jamestown.org/edm/article.php?article_id=2373060.

## Organization for Economic Cooperation and Development (OECD)

Organization for Economic Co-operation and Development (OECD). "Culture of Security for Information Systems and Networks". http://webdomino1.oecd.org/COMNET/STI/IccpSecu.nsf?OpenDatabase.

Organization for Economic Co-operation and Development (OECD). "OECD-APEC Workshop on Security of Information Systems and Networks - Seoul, 5-6 September 2005". http://www.oecd.org/document/25/0,2340,en_2649_201185_35481241_1_1_1_1,00.html.

Organization for Economic Co-operation and Development (OECD). "OECD Global Forum on Information Systems and Network Security: Towards a Global Culture of Security, Hotel Bristol, Oslo, Norway, 13-14 October 2003". http://www.oecd.org/document/38/0,3343,es_2649_34255_16193702_1_1_1_1,00.html.

Organization for Economic Co-operation and Development (OECD). "Social and Economic Factors Shaping the Future of the Internet" (2007). http://www.oecd.org/document/4/0,3343,es_2649_34255_39046340_1_1_1_1,00.html.

Organization for Economic Co-operation and Development (OECD). "Working Party on Information Security and Privacy; Implementation Plan for OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security" (2003). http://www.oecd.org/dataoecd/23/11/31670189.pdf.

Organization for Economic Co-operation and Development (OECD). "Working Party on the Information Security and Privacy; APEC-OECD Workshop on Malware Summary Record" (2007). http://www.oecd.org/dataoecd/37/60/38738890.pdf.

Organization for Economic Co-operation and Development (OECD). "Workshop 'The Future of the Internet': Proceedings" (2006). http://www.oecd.org/dataoecd/26/36/37422724.pdf.

## United Nations (UN)

World Summit on the Information Society (WSIS) Documents. "Geneva Declaration of Principles" (2003). http://www.itu.int/wsis/docs/geneva/official/dop.html.

World Summit on the Information Society (WSIS) Documents. "Geneva Plan of Action" (2003). http://www.itu.int/wsis/docs/geneva/official/poa.html.

World Summit on the Information Society (WSIS) Documents. "Tunis Commitment" (2005). http://www.itu.int/wsis/docs2/tunis/off/7.html.

World Summit on the Information Society (WSIS) Documents. "Tunis Agenda for the Information Society" (2005). http://www.itu.int/wsis/docs2/tunis/off/6rev1.html.

International Telecommunication Union (ITU). ITU Initiatives related to cybersecurity. http://www.itu.int/osg/spu/cybersecurity/ituevents.html.

UN General Assembly Resolution 57/239. "Creation of a Global Culture of Cybersecurity" (31 January 2003). http://www.itu.int/osg/spu/cybersecurity/docs/UN_resolution_57_239.pdf.

UN General Assembly Resolution 58/199 (30 January 2004). "Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures". http://www.itu.int/osg/spu/cybersecurity/docs/UN_resolution_58_199.pdf.

## The World Bank Group

The International Bank for Reconstruction and Development/The World Bank "Information Technology Security Handbook" (2003). http://www.infodev-security.net/handbook/.

World Bank Group. "About GICT".
http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS

# A3 Important Links

## Australia

Attorney-General's Department
(http://www.ag.gov.au/)

Attorney-General's Department on Critical Infrastructure Protection.
(http://www.ag.gov.au/www/agd/agd.nsf/Page/Nationalsecurity_CriticalInfrastructureProtection.)

Australian Computer Emergency Response Team (AusCERT) (http://www.auscert.org.au/)

Australian Government Information Management Office (AGIMO)

(http://www.agimo.gov.au)

Australian Government Onsecure
(http://www.onsecure.gov.au)

Australian High Tech Crime Centre (AHTCC)
(http://www.ahtcc.gov.au)

Australian Homeland Security Research Centre
(www.homelandsecurity.org.au)

Australian National Security
(http://www.nationalsecurity.gov.au/)

Australian Security Intelligence Organisation (ASIO)
(http://www.asio.gov.au)

Department of Broadband, Communications and the Digital Economy
(http://www.dbcde.gov.au/)

Defence Signals Directorate (DSD)
(http://www.dsd.gov.au)

Trusted Information Sharing Network
(http://www.tisn.gov.au)

## Austria

Austrian Computer Emergency Response Team (CERT.at)
(http://www.cert.at/)

Austrian Information Security Handbook
(http://www.a-sit.at/pdfs/OE-SIHA_I_II_V2-3_2007-05-23.pdf)

Austrian Parliament
(http://www.parlament.gv.at)

Center for Secure Information Technology Austria (A-SIT)
(http://www.a-sit.at/)

Federal Chancellery
(http://www.bundeskanzleramt.at)

ICT-Strategy Unit of the Federal Government
(http://www.digitales.oesterreich.gv.at)

Ministry for Traffic, Innovation, and Technology (BMVIT)
(http://www.bmvit.gv.at)

Ministry of Internal Affairs
(http://www.bmi.gv.at/)

Official Austrian Data Security Website
(http://www.dsk.gv.at/indexe.htm)

Stopline.at
(http://www.stopline.at/)

The Austrian Citizen Card
(http://www.buergerkarte.at)

## Brazil

Brazilian Electronic Government Program (e-Gov)
(http://www.governoeletronico.gov.br)

Brazilian Honeypots Alliance
(http://www.honeypots-alliance.org.br)

Centre for Research on Information Technology and Communication
(http://www.cetic.br)

Centre for Research, Treatment of Incident Response and Security in Brazil
(http://www.cert.br/mission.html)

Centre for Treatment of Security Incidents in Computer Networking of Federal Public Administration
(http://www.ctir.gov.br)

Ministry of Communications
(www.mc.gov.br)

Ministry of Science and Technology
(www.mct.gov.br)

Presidential Administration
(http://www.presidencia.gov.br)

SecGov
(http://www.secgov.com.br.)

The Renato Archer Research Centre
(http://www.cenpra.gov.br.)

## Canada

Public Safety Canada
(http://publicsafety.gc.ca)

Integrated Threat Assessment Centre
(http://www.itac-ciem.gc.ca/index-eng.asp)

Public Safety Canada's Canadian Cyber Incident Response Centre (http://www.publicsafety.gc.ca/prg/em/ccirc/index-eng.aspx)

## Estonia

Estonian Informatics Centre
(http://www.ria.ee)

Estonian Information Socety
(http://www.esis.ee)

Estonian National Security Concept 2004
(http://merln.ndu.edu/whitepapers/Estonia-2004.pdf)

Guideline on reform to Estonian Regulatory and Surveillance Authority
(http://www.sa.ee/atp/index_en.html)

Ministry of Economic Affairs and Communications
(http://www.mkm.ee/index.php)

Ministry of Justice
(http://www.just.ee)

Ministry of the Interior
(http://www.siseministeerium.ee)

National Identity Cards
(http://www.id.ee)

State Information System
(http://www.riso.ee)

## Finland

Computer Emergency Response Team Finland (CERT-FI)
(http://www.cert.fi)

Finland's Public Authority Network
(http://www.virve.com)

Finnish Communications Regulatory Community
(http://www.ficora.fi/)

Finnish Information Society Development Centre (TIEKE) (http://www.tieke.fi)

Information Society Program (http://www.tietoyhteiskuntaohjelma.fi)

Ministry of Defence (http://www.defmin.fi)

Ministry of Finance (http://www.vm.fi)

Ministry of Transport and Communications (http://www.lvm.fi/web/en)

National Emergency Supply Agency (NESA) (http://www.nesa.fi.)

Ubiquitous Information Society Advisory Board (http://www.arjentietoyhteiskunta.fi)

Unofficial English translations of Finnish legislation (http://www.finlex.fi/en)

## France

Central Directorate for Information Systems Security (DCSSI) (http://www.ssi.gouv.fr/en/dcssi/index.html)

Computer Emergency Response Team Industry, Services, and Trade (CERT-IST) (http://www.cert-ist.com)

Conseil Stratégique des Technologies de l'Information (CSTI) (http://www.csti.pm.gouv.fr/)

Index of Expression, Needs and Goals and Identification Security (EBIOS) (http://www.ssi.gouv.fr/fr/confiance/ebiospresentation.html)

Information Systems Security Training Center (CFSSI) (http://www.formation.ssi.gouv.fr/)

La mise en oeuvre du Programme d'Action Gouvernemental pour la Société de l'Information.
(http://www.education.gouv.fr/realisations/communication/samra.htm)

Le Portail Socièté de l'Information Internet gouv.fr
(http://www.internet.gouv.fr)

National Network of Telecommunications for Technology, Education, and Research (RENATER)
(http://www.renater.fr)

Portail de la Sécurité Informatique
(http://www.securite-informatique.gouv.fr.)

Secrétariat Général de la Défense Nationale (SGDN)
(http://www.sgdn.gouv.fr/sommaire.php)

Serveur Thématique Sécurité des Systèmes d'Information (SSI) (http://www.ssi.gouv.fr/fr/index.html)

## Germany

Federal Ministry of Economic and Technology/ Bundesminister für Wirtschaft und Technologie
(http://www.bmwi.de)

Federal Ministry of Justice/ Bundesministerium der Justiz
(www.bmj.bund.de)

Federal Ministry of the Interior/ Bundesministerium des Innern (http://www.bmi.bund.de)

Federal Network Agency/ Die Bundesnetzagentur
(www.bundesnetzagentur.de)

Federal Office for Civil Protection and Disaster Response/Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
(www.bbk.bund.de)

Federal Office for Information Security/Bundesamt für Sicherheit in der Informationstechnik
(http://www.bsi.bund.de/)

German Emergency Preparedness Information System/ deutsche Notfallvorsorge-Informationssystem
(www.denis.bund.de)

German CERT-Verbund
(www.cert-verbund.de)

Initiative D21
(www.initiatived21.de)

## Hungary

CERT Hungary
(http://www.cert-hungary.hu/index.php?newlang=english)

Computer and Automation Research Institute of the Hungarian Academy of Sciences (MTA SZAKI)
(http://www.sztaki.hu/?en)

e-inclusion campaign
(http://einclusion.hu/)

Electronic Government Center
(http://www.ekk.gov.hu/)

Hun- CERT
(http://www.cert.hu/)

Hungarian awareness building programs
(http://www.biztonsagosinternet.hu/)
(www.internethotline.hu)
(www.baratsagosinternet.hu)

Information on Hungarian Cybercrime Law
(http://www.coe.int/cybercrime)

Ministry of Defence
(http://www.hm.gov.hu/ministry)

Ministry of Economy and Transport
(http://en.gkm.gov.hu)

Ministry of Justice and Law Enforcement
(http://irm.gov.hu/?lang=en)

National Council for Communications and Information Technology (http://en.nhit.hu/start)

National Information Infrastructure Development Institute (NIIF) (http://www.niif.hu/en)

Prime Ministers Office
(http://www.meh.hu/english)

The Theodore Puskas Foundation
(http://www.neti.hu/pta/en/index)

## India

Indian Computer Emergency Response Team (CERT-In)
(http://www.cert-in.org.in)

Ministry of Communications and Information Technology
(http://www.moc.gov.in)

Ministry of Communications and Information Technology – Department of Information Technology (DIT)
(http://mit.gov.in/.)

National Association of Software and Service Companies
(www.nasscom.org)

National Informatics Centre
(http://home.nic.in/)

National Taskforce on IT and Software Development
(http://it-taskforce.nic.in/)

Standardisation, Testing, and Quality Certification (STQC) Directorate
(http://www.stqc.nic.in/)

## Italy

Association of Italian Experts for Critical Infrastructures
(http://www.infrastrutturecritiche.it)

CERT Difesa
(http://www.difesa.it/SMD/Staff/Reparti/II-reparto/CERT/default.htm)

CERT-IT
(http://idea.sec.dsi.unimi.it/activities.en.html)

GARR-CERT
(http://www.cert.garr.it/index-en.html)

GovCERT.it
(http://www.cnipa.gov.it/site/it-it/Attivit%C3%A0/Servizi_per_la_PA/Govcert.it/)

Italian State Police
(http://www.poliziadistato.it/pds/index.html)

Ministry for Innovation and Technologies
(http://www.innovazione.gov.it)

Ministry of Communication
(http://www.comunicazioni.it)

National Center for Informatics in the Public Administration (CNIPA)
(http://www.cnipa.gov.it.)

University of Milan Computer and Network Security Lab
(http://security.dsi.unimi.it)

## Japan

@police
(http://www.cyberpolice.go.jp/english/index.html)

APCERT
(http://www.apcert.org/)

JPCERT
(http://www.jpcert.or.jp/english)

Ministry of Economy, Trade and Industry
(http://www.meti.go.jp/english/index.html)

Ministry of Internal Affairs and Communications
(http://www.soumu.go.jp/english/index.html)

National Incident Response Team (NIRT)
(http://www.nisc.go.jp/en/shoukai/nirt/)

National Information Security Center
(http://www.nisc.go.jp/eng/index.html)

National Police Agency
(http://www.npa.go.jp/english/index.htm)

Prime Minister of Japan and Cabinet Office
(http://www.kantei.go.jp/foreign/index-e.html)

Telecom Information Sharing and Analysis Center Japan (Telecom-ISAC Japan)
(https://www.telecom-isac.jp/)

## Republic of Korea

e- Korea Vision 2006
(http://www.ipc.go.kr/ipceng/policy/vision_ground.jsp?num=1.)

Electronics and Telecommunications Research Institute (ETRI) (http://www.etri.re.kr/eng/)

Informatization Promotion Committee
(http://www.ipc.go.kr)

Internet Crime Investigation Center (ICIC)
(http://www.icic.sppo.go.kr)

Korea Communications Commission (KCC)
(http://www.kcc.go.kr)

Korean Information Security Agency (KISA)
(http://www.kisa.or.kr)

Korea Information Security Industry Association (KISIA)
(http://www.kisia.or.kr/new.)

Korea Internet Security Centre
(http://www.krcert.or.kr/index.jsp)

Korea IT Security Evaluation Center (KISEC)
(http://www.kisa.or.kr/kisae/kisec/jsp/kisec_6010.jsp)

KrCERT/CC
(http://www.krcert.or.kr)

Ministry of Government Legislation
(http://www.klaw.go.kr/)

Ministry of Public Administration and Security (MOPAS)
(http://www.mopas.go.kr)

Ministry of Science and Technology
(http://www.most.go.kr.)

National Cyber Security Center (NCSC)
(http://www.ncsc.go.kr)

National Information Security Alliance (NISA)
(http://www.nisa.or.kr/)

National Security Research Institute (NSRI)
(http://www.nsri.re.kr/kor/index.html.)

Prime Minister's Office
(http://pm.go.kr)

## Malaysia

E-Secure Malaysia
(http://www.esecuremalaysia.org.my)

Malaysia Communications and Multimedia Commission (MCMC) (http://www.mcmc.gov.my)

Malaysian Administrative Modernization and Management Planning Unit (MAMPU)
(http://www.mampu.gov.my)

Malaysian Computer Emergency Response Team (MyCERT) (http://www.mycert.org.my)

Ministry of Science, Technology and Innovation (MOSTI)
(http://www.mosti.gov.my/MostePortal/website/index.jsp)

National ICT Security & Emergency Response Centre (NISER) (http://www.niser.org.my)

## The Netherlands

Digibewust programme ("Digital Awareness")
(http://www.digibewust.nl)

Dutch Ministry of Economic Affairs (EA)
(http://www.ez.nl/)

Dutch National Coordinator Counterterrorism (NTCb)
(http://www.nctb.nl)

General Intelligence and Security Service (AIVD)
(https://www.aivd.nl/)

GOVCERT.NL
(http://www.govcert.nl)

Ministry of Defence
(http://www.mindef.nl/en/)

Ministry of Health, Welfare, and Sport (VWS)
(http://www.minvws.nl)

Ministry of the Interior and Kingdom Relations
(http://www.minbzk.nl)

Ministry of Transport, Public Works, and Water Management (V&W)
(http://www.verkeerenwaterstaat.nl)

National Advisory Centre Critical Infrastructures (NAVI)
(http://www.navi-online.nl)

National Continuity Consultation Platform Telecommunications (NCO-T)
(http://www.ez.nl/content.jsp?objectid=150712&rid=150996)

Netherlands Organisation for Applied Scientific Research (TNO) (http://www.tno.nl)

Platform Electronic Commerce in the Netherlands (ECP.NL) (http://www.ecp.nl)

SME malware alert service
(http://www.waarschuwingsdienst.nl)

Waarschuwingsdienst.nl
(http://www.waarschuwingsdienst.nl)

## New Zealand

AusCERT
(http://www.auscert.org.au)

Centre for Critical Infrastructure Protection (CCIP)
(http://www.ccip.govt.nz/)

Domestic and External Security Group (DESG) and Officials Committee for Domestic and External Security Co-ordination (ODESC)
(http://www.dpmc.govt.nz/dess/index.htm)

e-Government Programme
(http://www.e.govt.nz/)

Government Communications Security Bureau (GCSB)
(http://www.gcsb.govt.nz/)

Interdepartmental Committee on Security (ICS)

New Zealand Computer Society's Special Interest Group on Security (NZCS Sig-Sec)
(http://www.nzcs.org.nz/SITE_Default/special_interest_groups/SITE_Information_Systems_SIG/default.asp)

New Zealand Security Association (NZSA)
(http://www.security.org.nz/)

Security Policy and Guidance Website
(http://www.security.govt.nz/)

Standards New Zealand (SNZ)
(http://www.standards.co.nz/default.htm)

## Norway

Directorate for Civil Protection and Emergency Planning
(http://www.dsb.no/)

National Information Security Co-ordination Council (KIS)
(http://www.nsm.stat.no/kis/)

National Security Authority (NSM)
(http://www.nsm.stat.no/)

Nettvett
(http://www.nettvett.no/)

Norwegian Center for Information Security (NorSIS)
(http://www.norsis.no)

Norwegian Post and Telecommunications Authority (NPT)
(http://www.npt.no)

UNINETT CERT
(http://cert.uninett.no/)

## Poland

ARAKIS-gov
(http://arakis.cert.pl/en/index.html)

CERT Polska
(http://www.cert.pl/index3.html?id=24)

Ministry of Interior and Administration
(http://www.mswia.gov.pl/portal/en/3/63/)

Pionier CERT
(http://cert.pionier.gov.pl./)

Polish Competence Center for eGovernment and eEducation
(http://www.egov.edu.pl.)

Polish Penal Code
(http://www.cybercrimelaw.net/laws/countries/poland.html)

Research and Academic Computer Network in Poland
(http://www.nask.pl/run/n/home/)

## Russia

Electronic Russia
(http://www.e-rus.ru)

Federal Agency of Government Communications and Information
(http://www.agentura.ru/dossier/russia/fapsi/)

Federal Security Service (FSB)
(http://www.fsb.ru)

Information Security Doctrine of the Russian Federation
(http://www.medialaw.ru/e_pages/laws/project/d2-4.htm)

Institute of the Information Society
(http://www.iis.ru/en/index.html)

PRIOR
(http://prior.russia-gateway.ru/en/)

Russian Association for Networks and Services
(http://www.rans.ru/eng)

Russian Computer Security Incident Response Team
(RU-CERT). (http://www.cert.ru)

Russian Institute for Public Networks
(http://www.ripn.net:8080)

Russian Security Council
(http://www.kremlin.ru/eng/articles/institut04.shtml)

## Singapore

Governmentware 2007
(http://www.governmentware07.com/home.htm)

Infocomm Development Authority of Singapore
(http://www.ida.gov.sg)

Information Technology Standards Committee (ITSC)
(http://www.itsc.org.sg/)

Singapore Computer Emergency Response Team (SingCERT) (http://www.singcert.org.sg)

Singapore Police Force
(http://www.spf.gov.sg./)

## Spain

Antivirus Early-Warning Center (CATA)
(http://alerta-antivirus.inteco.es/portada/index.php)

Central e-government
(www.administracion.es)

CERT-CNN
(https://www.ccn-cert.cni.es)

Information Society and Telecommunications Analysis Center (http://www.enter.es)

Ministry for Public Administration
(http://www.csi.map.es)

Ministry for Public Administration  TECNIMAP
(http://www.tecnimap.es/Tecnimap/)

Ministry of the Interior
(http://www.mir.es/)

Ministry of Industry, Tourism, and Trade
(http://www.mityc.es)

Ministry of Industry, Tourism, and Trade General Directorate for the Development of the Information Society (DGDSI)
(http://www.mityc.es/DGDSI)

Ministry of Industry, Tourism, and Trade General Directorate of Telecommunications and Information Technologies (DGTTI) (http://www.mityc.es/Telecomunicaciones)

Red.es Office
(http://www.red.es)

Spanish Electronics, Information Technology, and Telecommunications Industries Association
(http://www.aetic.es)

Spanish National Research Network (RedIRIS)
(http://www.rediris.es/index.en.html)

## Sweden

Center for Asymmetric Threat Studies (CATS)
(http://www.fhs.se/en/Research/Centers-and-Research-Programmes/CATS/)

Confederation of Swedish Enterprise
(http://www.svensktnaringsliv.se/)

Swedish Armed Forces
(http://www2.mil.se/)

Swedish Defense Materiel Administration (FMV)
(http://www.fmv.se/)

Swedish Defense Research Agency (FOI)
(http://www.foi.se/FOI/templates/startpage____96.aspx)

The Swedish Emergency Management Agency (SEMA)
(http://www.krisberedskapsmyndigheten.se/)

Swedish Information Processing Society (DFS)
(http://www.dfs.se/)

Swedish IT Incident Centre (SITIC)
(http://www.sitic.se/)

Swedish National Defense College
(http://www.fhs.se/sv/)

Swedish National Defense Radio Establishment (FRA)
(http://www.fra.se/)

Swedish National Police Board (NPB)
(http://www.polisen.se/inter/nodeid=10230&pageversion=1.html)

Swedish Security Service
(http://www.securityservice.se/)

## Switzerland

CLUSIS
(http://www.clusis.ch)

Coordination Unit for Cybercrime Control (CYCO)
(http://www.cybercrime.ch/)

Federal Department of Defence, Civil Protection, and Sports (DDPS)
(http://www.vbs.admin.ch/)

Federal Office for Civil Protection
(http://www.bevoelkerungsschutz.admin.ch/)

Federal Office of Communications (OFCOM)
(http://www.bakom.ch/)

Federal Office of Information Technology, Systems, and Telecommunication (FOITT)
(http://www.efd.admin.ch/)

Federal Office for National Economic Supply (NES)
(http://www.bwl.admin.ch/)

Federal Strategy Unit for Information Technology (FSUIT)
(http://www.isb.admin.ch/)

InfoSurance Association
(http://www.infosurance.ch)

MELANI
(http://www.melani.admin.ch)

SONIA
(http://www.isb.admin.ch/themen/sicherheit/00152/00176/index.html)

## United Kingdom

Centre for the Protection of National Infrastructure
(http://www.cpni.gov.uk)

Central Sponsor for Information Assurance (CSIA)
(http://www.cabinetoffice.gov.uk/csia/)

Civil Contingencies Secretariat (CCS)
(www.ukresilience.info/ccs.aspx)

Combined Security Incident Response Team (CSIRTUK)
(http://www.cpni.gov.uk/Products/advisories.aspx)

Confederation of British Industry.
(http://www.cbi.org.uk)

GetSafeOnline
(http://www.getsafeonline.org/.)

GovCertUK
(http://www.govcertuk.gov.uk)

Home Office
(http://www.homeoffice.gov.uk)

Information Assurance Advisory Council
(http://www.iaac.org.uk/)

Institute of Information Security Professionals
(https://www.instisp.org)

Internet Watch Foundation
(http://www.iwf.org.uk)

National Counter Terrorism Security Office (NaCTSO)
(www.nactso.gov.uk)

Security Service (MI5)
(http://www.mi5.gov.uk)

The British Computer Society
(http://www.bcs.org)

The National Computing Centre
(http://www.ncc.co.uk)

Warning Advice and Reporting Points (WARPs)
(http://www.warp.gov.uk/)

## United States

Computer Emergency Response Team
(www.cert.org/)

Critical Infrastructure Partnership Advisory Council
(http://www.dhs.gov/xprevprot/committees/editorial_0843.shtm)

Department of Defense
(http://www.defenselink.mil/)

Department of Homeland Security (DHS)
(http://www.dhs.gov/index.shtm)

Department of Justice (DOJ)
(http://www.usdoj.gov/)

Department of State
(http://www.state.gov/)

DOJ Computer Crime and Intellectual Property Section
(http://www.usdoj.gov/criminal/cybercrime/index.html)

Energy Information Sharing and Analysis Center
(http://www.esisac.com/)

Federal Bureau of Investigation
(http://www.fbi.gov/)

Financial Services Information Sharing and Analysis Centre (FS-ISAC)
(http://www.fsisac.com/)

Government Accountability Office (GAO)
(http://www.gao.gov/)

House of Representatives' Committee on Homeland Security (http://homeland.house.gov/)

Information Technology Information Sharing and Analysis Center (IT-ISAC)
(https://www.it-isac.org)

InfraGard
(http://www.infragard.net/)

Institute for Information Infrastructure Protection (I3P)
(http://www.thei3p.org/)

ISAC Council
(http://www.isaccouncil.org)

National Communications System
(http://www.ncs.gov/)

National Cyber Security Alliance (NCSA)
(http://www.staysafeonline.info/)

National Cyber Security Division (NCSD)
(http://www.dhs.gov/xabout/structure/editorial_0839.shtm)

National Infrastructure Advisory Council (NIAC)
(http://www.dhs.gov/xprevprot/committees/editorial_0353.shtm)

Office of Cybersecurity and Communications (CS&C)
(http://www.dhs.gov/xabout/structure/gc_1185202475883.shtm)

Office of Emergency Communications (OEC)
(http://www.dhs.gov/xabout/structure/gc_1189774174005.shtm)

Office of Infrastructure Protection (OIP)
(http://www.dhs.gov/xabout/structure/gc_1185203138955.shtm)

OnGuardOnline.gov
(http://onguardonline.gov/index.html)

Partnership for Critical Infrastructure Security (PCIS)
(http://www.pcis.org)

Senate Homeland Security and Government Affairs Committee (http://hsgac.senate.gov/public/)

US-CERT
(http://www.uscert.gov)

# European Union (EU)

Community Research and Development Information Service (CORDIS) (http://cordis.europa.eu/en/home.html)

Critical Information Infrastructure Research Coordination (CI2RCO) (http://www.ci2rco.org)

ENISA Build on Synergies – Achieve Impact (http://www.enisa.europa.eu/doc/pdf/management_board/decisions/enisa_wp_2008.pdf)

ENISA Inventory of CERT Activities in Europe (http://www.enisa.europa.eu/cert_inventory/downloads/Enisa_CERT_inventory.pdf)

ENISA Who is Who Directory on Network and Information Security (http://www.enisa.europa.eu/doc/pdf/deliverables/wiw_v2_2006.pdf)

European Network and Information Security Agency (ENISA) (http://www.enisa.europa.eu/index.htm)

European Security Research Advisory Board (ESRAB) (http://ec.europa.eu/enterprise/security/articles/article_2006-04-06_en.htm)

European Security Research and Innovation Forum (ESRIF) (http://www.esrif.eu)

Europe`s Information Society Thematic Portal (http://ec.europa.eu/information_society/index_en.htm)

Full text of the Treaty of Lisbon (2007) (http://europa.eu/lisbon_treaty/full_text/index_en.htm)

Information Society and Media Directorate General (http://ec.europa.eu/dgs/information_society/index_en.htm)

## Group of Eight (G8)

G8 Information Centre (http://www.g8.utoronto.ca)

G8 Paris Conference on Dialogue between the Public Authorities and Private Sector on Security and Trust in Cyberspace (http://www.g8.utoronto.ca/crime/paris2000.htm)

Okinawa Charter on Global Information Society (http://www.g7.utoronto.ca/summit/2000okinawa/gis.htm)

## North Atlantic Treaty Organization (NATO)

Civil Emergency Planning (http://www.nato.int/issues/cep/index.html)

Index of organizations involved in Civil Emergency Planning (http://www.nato.int/issues/cep/role.html)

NATO Summit Bucharest (http://www.summitbucharest.ro)

## Organization for Economic Cooperation and Development (OECD)

Organization for Economic Cooperation and Development; Directorate for Science, Technology and Industry. (http://www.oecd.org/department/0,3355,en_2649_33703_1_1_1_1_1,00.html)

Organization for Economic Cooperation and Development; Policy Brief – The Future of the Internet Economy (http://www.oecd.org/dataoecd/20/41/40789235.pdf)

## United Nations (UN)

International Telecommunication Union (ITU)
(http://www.itu.int/home/index.html)

United Nations
(http://www.un.org)

United Nations Information and Communication Technologies Task Force (http://www.unicttaskforce.org)

## The World Bank Group

Global Information and Communication Technologies
(http://info.worldbank.org/ict/index.cfm.)

InfoDev-Security.net
(http://www.infodev-security.net/)

Information for Development (infoDev) Program
(http://www.infodev.org/en/index.html)

World Bank Group
(http://www.worldbank.org/)

# A4 List of Experts

## Australia

- **Alex Webling**, Attorney-General's Department, Australian government (2006 + 2008)
- **Patrick Drake-Brockman**, Attorney-General's Department, Australian government (2006)
- **Adam Cobb**, Director Stratwise Strategic Intelligence (2004)
- **Ivan Timbs**, National Office for the Information Economy (NOIE) (2002)

## Austria

- **Otto Hellwig**, Technische Universität Graz (2004 + 2006 + 2008)
- **Thomas Pankratz**, Austrian Federal Ministry of Defense, Bureau for Security Policy (2004 + 2006)
- **Gerald Torst**, Stabsstelle IKT-Strategie des Bundes, Federal Chancellery of the Republic (2004 + 2006)
- **Nieves Kautny**, University of Vienna (2006)
- **Ralph Schöllhammer**, University of Vienna (2006)

## Brazil

- **Mariana Balboni**, Brazilian Internet Steering Committee (2008)
- **Regina Maria De Felice Souza**, Agência Nacional de Telecomunicações – Presidency (2008)
- **João Henrique de A. Franco**, CPqD Telecom & IT Solutions (2008)
- **Sérgio Luis Ribeiro**, CPqD Telecom & IT Solutions (2008)

## Canada

- **Claudia Zuccolo,** Public Safety Canada (2006 + 2008)
- **Marta Khan**, Public Safety Canada (2006 + 2008)
- **Michel De Jong,** Public Safety Canada (2006 + 2008)
- **Suki Wong**, Public Safety Canada (2006 + 2008)
- **Janet Bax**, Public Safety and Emergency Preparedness Canada (PSEPC) (2006)
- **Phil Beahen**, Public Safety and Emergency Preparedness Canada (PSEPC) (2006)
- **Robert Corley**, Public Safety and Emergency Preparedness Canada (PSEPC) (2006)
- **Peter Hill**, Public Safety and Emergency Preparedness Canada (PSEPC) (2006)
- **Andrew McAllister,** Public Safety and Emergency Preparedness Canada (PSEPC) (2006)
- **Craig Oldham**, Public Safety and Emergency Preparedness Canada (PSEPC) (2006)
- **Julie Spallin**, Public Safety and Emergency Preparedness Canada (PSEPC) (2006)
- **Louise Forgues**, Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) (2004)
- **Jacques L. Grenier**, Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) (2002)
- **Shannon Hiegel**, Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) (2004)
- **Colin Knight**, Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) (2002)
- **Dan Lambert**, Solicitor General (2004)
- **Paul Pagotto**, Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) (2004)

## Estonia

- **Thomas Viira**, Estonian Informatics Center (2008)
- **Jaak Tepandi**, Institute of Informatics, Tallinn University of Technology (2008)

## Finland

- **Veli-Pekka Kuparinen**, National Emergency Supply Agency (NESA) (2004 + 2006 + 2008)
- **Ilkka Kananen**, National Emergency Supply Agency (NESA) (2004 + 2006 + 2008)
- **Hannu Sivonen**, National Emergency Supply Agency (NESA) (2006 + 2008)
- **Mika Purhonen**, National Emergency Supply Agency (NESA) (2004)
- **Markku Haranne**, Ministry of the Interior, Rescue Services Unit (2004)

## France

- **Stanislas de Maupeou**, SGDN - DCSSI - Sous-direction opérations Chef du CERTA (2008)
- **Isabelle Valentini**, Secretary-General for National Defense (SGDN) (2006)

## Germany

- **Susanne Jantsch**, Consultant (2002 + 2004 + 2006 + 2008)
- **Monika John-Koch**, Federal Office of Civil Protection and Disaster Assistance (BBK) (2008)
- **Dirk Reinermann**, Federal Office for Information Security (BSI) (2004)
- **Stefan Ritter**, Federal Office for Information Security (BSI) (2004)
- **Thomas Beer**, Industrieanlagen-Betriebsgesellschaft (IABG) (2004)
- **Willi Stein**, Federal Office for Information Security (BSI),   (2004)

- **Christine Scharz-Hemmert**, Industrieanlagen-Betriebsgesellschaft (IABG) (2002)
- **Ralf Bendrath**, Political Scientist (2002)
- **Jörn Brömmelhörster**, Consultant (2002)

## Hungary

- **Bence Birkás**, CERT-Hungary (2008)
- **Ferenc Suba**, CERT-Hungary (2008)
- **Lajos Muha**, Dennis Gabor College, Budapest (2008)
- **Barbara Locher**, Ministry of Economics and Transport (2008)
- **Peter Csokany**, National Communication Authority (2008)
- **Csaba Sandor**, Electronic Government Center (2008)

## India

- **Subimal Bhattacharjee**, Argus Integrated Systems (2006)
- **Luthra & Luthra** Law Offices (2006)

## Italy

- **Roberto Setola**, Complex Systems and Security Laboratory, Università Campus Bio-Medico (2004 + 2006 + 2008)
- **Tommaso Palumbo**, Postal and Communication Police (2006 + 2008)
- **Paolo Donzelli,** Prime Minister's Office - Dept. for Innovation and Technologies (2006)
- **Sandro Bologna**, Italian National Agency for New Technologies, Energy and the Environment (ENEA) (2004)
- **Giovanna Dondossola,** CESI (2004)

## Japan

- **Mika Shimizu,** East-West Centre (2006 + 2008)
- **Tomoko Makino**, Ministry of Internal Affairs and Communications (MIC) (2008)
- **Tohru Nakao,** Ministry of Internal Affairs and Communications (MIC) (2008)
- **Yoshihiro Sato,** National Information Security Center (NISC) (2008)
- **Toshihiko Suguri,** National Information Security Center (NISC) (2008)
- **Japanese experts** from the Ministry of Internal Affairs and Communication (MIC) (2006)
- **Ministry of Foreign Affairs** (MOFA) (2006)
- **National Police Agency** (NPA) (2006)
- **Cabinet Secretariat**, and the Ministry of Economy, Trade and Industry (METI) (2006)

## Republic of Korea

- **Heung Youl Youm**, Professor at the Department of Information Security Engineering of Soonchunhyang University (2008)
- **Seok-Koo Yoon**, Director National Cyber Security Center (NCSC) (2006)

## Netherlands

- **Eric Luiijf,** TNO Defense, Security and Safety (2002 + 2004 + 2006 + 2008)
- **Williët Brouwer**, Programme Manager Critical Infrastructure Protection, Ministry of the Interior (2008)
- **André Griffioen**, Deputy Programme Manager Critical Infrastructure Protection, Ministry of the Interior (2008)
- **Ronald de Bruin**, KWINT, ECP.nl (2002 + 2004)

## New Zealand

- **Mike Harmon**, Centre for Critical Infrastructure Protection (CCIP) (2004 + 2006)
- **Richard Byfield**, Centre for Critical Infrastructure Protection (CCIP) (2006)

## Norway

- **Stein Henriksen,** Norwegian National Security Authority (2002 + 2004 + 2006 + 2008)
- **Håkon Styri,** Norwegian Post and Telecommunications Authority (2008)
- **Einar Oftedal**, Norwegian National Security Authority (2008)
- **Lene Bogen Kaland**, Norwegian National Security Authority and National Information Security Co-ordination Council (2008)
- **Laila Berge**, Ministry of Justice and the Police (2006)
- **Dagfinn Buset**, Ministry of Justice and the Police (2006)
- **Roger Steen**, Directorate for Civil Protection and Emergency Planning (DSB) (2002 + 2004)
- **Kjetil Sørli**, Directorate for Civil Protection and Emergency Planning (DSB) (2004)
- **Cort Archer Dreyer,** Ministry of Trade and Industry (2002)
- **Havard Fridheim,** Norwegian Defence Research Establishment (FFI) (2002)
- **Arthur Gjengstö**, Secretary to the Norwegian Commission on the Vulnerability of Society (2002)

## Poland

- **Tomasz Prząda**, Polish Internal Security Agency (2008)
- **Michał Młotek**, Polish Ministry of Interior and Administration (2008)
- **Krzysztof Silicki**, NASK / CERT Polska (2008)
- **Mirosław Maj**, NASK / CERT Polska (2008)

## Russia

- **Anatoly Streltsov**, professor at the Institute of Information Security, Lomonosov Moscow State University (2006 + 2008)
- **Martin Wählisch**, Humbolt University Berlin (2006)

## Singapore

- **Experts form the Ministry of Home Affair** (MHA) (2006)

## Spain

- **Experts from the Directorate of the Centre for the Protection of National Infrastructure** (CNPIC) (2008)

## Sweden

- **Linda Englund**, Swedish Emergency Management Agency (SEMA) (2006 + 2008)
- **Jan Lundberg**, Swedish Emergency Management Agency (SEMA) (2002 + 2004 + 2006 + 2008)
- **Lars Nicander**, Swedish National Defence College (2004)
- **Henrik Christiansson**, Swedish Defence Research Agency (FOI) (2004)
- **Georg Fischer**, Swedish Defence Research Agency (FOI) (2004)
- **Sara Siri**, Swedish Emergency Management Agency (SEMA) (2004)
- **Peter Stern**, Swedish Emergency Management Agency (SEMA) (2002)
- **Peter Wallström**, Cell Network (2002)
- **Peter Westrin**, FOI, Swedish Defence Research Agency (2002)
- **Manuel W. Wik**, Swedish National Defence College (2002)

## Switzerland

- **Experts from the Federal office for Civil Protection** (FOCP) (2008) the Reporting and Analysis Center for Information Assurance (MELANI) (2008) the Federal Office for National Economic Supply (NES) (2008)
- **Ruedi Rytz,** Federal Strategy Unit for Information Technology (ISB) (2002 + 2004 + 2006)
- **Anton Lagger,** Federal Office for National Economic Supply (2004 + 2006)
- **Marc Henauer,** Federal Office of Police/DAP (2004 + 2006)
- **Michel Dufour,** Dufour Consulting (2002 + 2004 + 2006)
- **Gérald Vernez,** General Staff of the Swiss Armed Forces (2006)
- **Riccardo Sibilia,** armasuisse (2006)
- **Oliver Vaterlaus,** AWK Group (2006)
- **André Schmid,** InfoSurance Foundation (2004)
- **Kurt Haering,** Director Foundation InfoSurance (2002)
- **Ueli Haudenschild,** Federal Office for National Economic Supply (2002)
- **Thomas Köppel,** Former Official of the Federal Office of Police (2002)

## United Kingdom

- **Experts from the Centre for the Protection of National Infrastructures** (CPNI) (2008)
- **John Neil Park,** the National Infrastructure Security Coordination Centre (NISCC) (2004 + 2006)
- **Ted Barry,** National Infrastructure Security Coordination Centre (NISCC) (2004)
- **Stephen Cummings,** National Infrastructure Security Coordination Centre (NISCC) (2004)

## United States

- **Scott C. Algeier**, Executive Director IT-ISAC (2002 + 2006 + 2008)
- **Erica B. Russel**, Deputy Coordinator for International Critical Infrastructure Protection Policy, Department of State (2006)
- **John A. McCarthy**, Critical Infrastructure Protection Project, George Mason University School of Law (2004)
- **Emily Frye**, Critical Infrastructure Protection Project, George Mason University School of Law (2004)

## European Union (EU)

- **Marcelo Masera**, European Commission, Institute for the Protection and Security of the Citizen Joint Research Centre (2006 + 2008)
- **Martin Wählisch**, Humboldt University Berlin (2006 +2008)
- **Ronald De Bruin**, European Network and Information Security Agency (ENISA) (2006)

## Group of Eight (G8)

- **Harry Hoverd**, Home Office, United Kingdom (2006)

## North Atlantic Treaty Organization (NATO)

- **Denisa-Elena Ionete**, Civil Emergency Planning, NATO Headquarters (2008)
- **Evert G. J. Somer**, NATO Headquarters (2006)
- **Silla A. Jonsdottier**, NATO Headquarters (2004)

## Organization for Economic Cooperation and Development (OECD)

- **Anne Carblanc**, Organization for Economic Cooperation and Development (OECD) (2006 + 2008)
- **Peter Lübkert,** Organization for Economic Cooperation and Development (OECD) (2006)
- **Laurent Bernat,** Organization for Economic Cooperation and Development (OECD) (2006)

## United Nations (UN)

- **Experts from the International Telecommunication Union** (ITU) (2008)
- **Robert Shaw,** International Telecommunication Union (ITU) (2006)
- **Christine Sund,** International Telecommunication Union (ITU) (2006)

CSS
ETH Zurich

**The Center for Security Studies** at ETH Zurich was founded in 1986 and specializes in the fields of international relations and security policy. The Center coordinates and develops the Crisis and Risk Network (CRN), a Swiss-Swedish initiative for international dialog on risks and vulnerabilities that is aimed at enhancing knowledge of the complex causes, interactions, probabilities, and costs of risks in modern societies.

**The CIIP Handbook** focuses on national governmental efforts to protect critical information infrastructure and provides an overview of CII protection practices in a range of countries and international organizations.