




Critical Infrastructure Resilience in Ukraine: Energy, Transportation, and Communication

Report**Author(s):**

[Aebi, Simon](#) ; [Hauri, Andrin](#) ; [Kamberaj, Jurgena](#) 

Publication date:

2024-03

Permanent link:

<https://doi.org/10.3929/ethz-b-000662463>

Rights / license:

[In Copyright - Non-Commercial Use Permitted](#)

Originally published in:

CSS Risk and Resilience Reports

RISK AND RESILIENCE REPORT

Critical Infrastructure Resilience in Ukraine: Energy, Transportation, and Communication

Simon Aebi, Andrin Hauri, Jurgena Kamberaj

Zürich, March 2024
Center for Security Studies (CSS), ETH Zürich

Available online at: css.ethz.ch/en/publications/other-reports.html

Authors: Simon Aebi, Andrin Hauri, Jurgena Kamberaj

ETH-CSS project management: Andrin Hauri, Co-Head of the Risk and Resilience Team;
Oliver Thränert, Head of Think Tank

Editor: Andrin Hauri

Client: Federal Office for Civil Protection (FOCP)

FOCP project supervision: Stefan Brem, Head of Civil Protection Development

Layout and graphics: Miriam Dahinden-Ganzoni

Disclaimer: All views and opinions presented in this report are solely those of the authors.

© 2024 Center for Security Studies (CSS), ETH Zürich

DOI: 10.3929/ethz-b-000662463

Content

1	Introduction	5
1.1	Context	5
1.2	Objective	5
1.3	Method and Structure	5
1.4	Limitations	5
2	Critical Infrastructure Protection and Resilience	6
2.1	Defining Critical Infrastructure	6
2.2	Critical Infrastructure Protection and Resilience	7
3	Critical Infrastructure Protection in Ukraine	8
3.1	2014–2022	9
3.2	2022–2023	9
3.3	Damage Assessments and Estimations	11
4	Case Studies	13
4.1	Energy	14
4.2	Transportation	20
4.3	Information and Communication	25
5	Resilience Approaches and Lessons Learned	30
6	Concluding Remarks	33
7	Bibliography	34

Executive Summary

The Russian invasion of Ukraine in February 2022 and the subsequent targeted attacks on critical infrastructure (CI) have put the country and its population under immense pressure. However, Russian interference with Ukrainian CI did not begin in 2022 but goes back at least as far as 2014 and the events surrounding the annexation of Crimea. In the aftermath of 2014, various political and legislative processes related to the protection of CI were initiated or accelerated in Ukraine, culminating, for example, in the first comprehensive legislation on the protection of CI, which came into force in November 2021. The full-scale invasion in February 2022 further increased the pressure on Ukraine, with kinetic and cyber-attacks affecting CI across sectors and causing an estimated 150 billion USD in infrastructure damages and 225 billion USD in infrastructure losses by June 2023 alone, according to the Kyiv School of Economics. Despite the enormous pressure, Ukraine has so far managed to maintain the operation of its CIs to such an extent that they can continue to provide essential services, albeit in many cases at a reduced level. International assistance and reconstruction efforts have been pivotal to these efforts and should be seen as a key pillar of Ukraine's resilience, but various other characteristics, factors, and domestic actions have also helped to ensure the functioning of critical systems and services.

This CSS Risk and Resilience Report was commissioned by the Swiss Federal Office for Civil Protection (FOCP) to examine what information has been published to date on the impact and resilience efforts of Ukrainian CI following the Russian invasion and what preliminary lessons can be learned about the protection and resilience of CI in a war scenario.

The report was compiled mainly based on desktop research using secondary sources and grey literature, including media contributions. It is divided into four parts. It starts with an introduction defining CI and its role and protection in an armed conflict, followed by an overview of relevant Ukrainian legislation on CI and the impact of war on such infrastructures. In the third part, three case studies on the CI sectors of energy, transportation, and communication highlight the damage incurred and the characteristics and actions that enabled their continued operation from February 2022 to October 2023. The last part summarizes overall lessons from the three case studies that are applicable to CI resilience in general.

The analysis of the three the case studies on energy, transportation, and communication through the lens of the recently adopted EU Directive 2022/2557 on critical entities, which defines resilience as the ability to *prevent, protect against, respond to, resist, mitigate, absorb, accommodate, and recover* from incidents, identifies characteristics, factors, and actions that have increased

the resilience of Ukrainian CI. These can be summarized as follows:

- Historically grown redundancies can boost resilience.
- International assistance bridges gaps and fosters (early) reconstruction.
- Well-prepared state emergency measures guarantee minimal services.
- Business continuity management secures operations.
- Private-public coordination and cooperation assures an effective response.
- Decentralization and diversification reduce vulnerability.
- Continued digitalization increases efficiency.
- Adequate legislation facilitates preparedness.
- Military authorities are crucial for critical infrastructure protection.

1 Introduction

1.1 Context

Russia's invasion of Ukraine in February 2022 led to the intentional targeting of Ukrainian infrastructure to gain a military advantage by disrupting essential functions of Ukraine's society and economy. The war and the resulting atrocities have put the Ukrainian population under immense pressure, with deliberate attacks on infrastructures, particularly critical infrastructure (CI), playing a key role. Ukrainian society has proven to be resilient in the face of an exceedingly tiring situation. While the CI that enable prosperity and development have been used as leverage against Ukraine, its resilience is also a factor contributing to the overall resilience of the country. A better understanding of how Ukraine's CI is impacted and how the services are or are not maintained can support policy-makers, government agencies, and CI operators outside of Ukraine in drawing lessons for their own preparedness and operation of national CI in times of adversity.

1.2 Objective

This CSS Risk and Resilience Report was commissioned by the Swiss Federal Office for Civil Protection (FOCP) to examine what information has been published to date on the impact and resilience efforts of Ukrainian CI following the Russian invasion. By compiling and integrating currently publicly available assessments on Ukrainian CI, the report aims to provide an overview of what they reveal in terms of the protection and resilience of CI to ensure the functioning of the state, economy, and society in times of war. Building on these insights and combining them with further analysis by the authors, the report seeks to improve and deepen the understanding of how Ukraine has managed to sustain a certain level of CI functioning and derive lessons for CI protection and resilience approaches.

1.3 Method and Structure

This report was compiled based on desktop research using secondary sources and grey literature, including media contributions. Sources written in Ukrainian were translated using the machine translation systems DeepL and Google Translate.¹ Two Ukrainian experts on the energy sector and CI protection in Ukraine were interviewed in August and September 2023. The authors of this report decided to keep the experts interviewed anonymous to encourage a candid discussion. The authors would like to thank the experts for their contributions.

The report is divided into four parts, starting with an introduction defining CI and its role and protection in an armed conflict. The second part provides an overview of the relevant Ukrainian legislation on CI and the impact of war on these infrastructures. The third part consists of three case studies on the CI sectors energy, transportation, and communication, highlighting the damage incurred and the characteristics and actions that enabled their continued operation from February 2022 to October 2023. The case studies are based on the Swiss, EU, and NATO understanding of CI and its protection. In the fourth part, overall lessons are derived from the three case studies that are generally applicable to the resilience of CI and conclude the report.

1.4 Limitations

The research and analysis for this report are subject to several limitations. First, the war in Ukraine is still ongoing and its course may change with time. Certain information is not yet known or publicly available. Given the lack of or incomplete data, it is still too early to draw definitive conclusions. This is also reflected in the relatively limited number of rigorous academic analyses and publications available at present. Second, the literature reviewed for this report (including media contributions, government reports, and non-governmental publications) was mainly published in English and stems from Western or Ukrainian sources. The sources and information used may therefore be biased by a favorable Western perspective. The report does not claim to be exhaustive with regard to relevant sources. The Russo-Ukrainian conflict demonstrates how information in the context of war can be manipulated, restricted, or not even communicated for reasons of national or operational security or anticipated negative repercussions. Hence, the accuracy of the data must be understood in the context of the sources' political agenda and the cultural landscape. Third, the case studies and the lessons derived focus on the three CI sectors energy, transportation, and communications. Other CI sectors were only peripherally examined and analyzed for this report. Moreover, the cyberspace is much discussed in the context of the Russian invasion of Ukraine and is the subject of numerous analyses. Although the cyberspace and its relevant overlaps with the three case studies are addressed at various points in this report, it is not the focus, as its sheer size would require a separate report. Fourth, the international military and non-military assistance that Ukraine receives increases and sustains the country's defense and security efforts. Consequently, Ukraine's own protection efforts are distorted by this assistance – or it can be seen as one pillar of CI protection, more specifically the endogenous ability to mobilize international support in times of crisis or the exogenous effect of geopolitics.

2 Critical Infrastructure Protection and Resilience

In the early 20th century, wars among nation-states became increasingly reliant on the total of a country's capacities to support the war efforts (i.e., total war). While it was crucial to protect one's vital capacities, it became clear that they could be exploited on the adversary's side to obstruct their economic and social capacities and, consequently, their military capabilities.² Following the technical advancements that enhanced air operations, US strategists, during World War II, worked out concepts of "Strategic Bombing" to target an adversary's population and hit vital links within the industry or infrastructure systems. By doing so, they hoped to disrupt an opponent's entire military efforts to the point of defeat. These strains of thinking offer an explanation of why particular infrastructures and systems are considered vital and have increasingly been treated as a security problem in policymaking.³ During and especially after the Cold War, the protection of a nation and its population shifted away from conventional armed conflicts and nuclear threats to a broader hazard spectrum, including technological accidents or energy supply shortages. This development led to the understanding that various hazards, including natural ones, can impact infrastructure and endanger people.⁴ As a result, the securitization of infrastructure has evolved from a military-strategic issue to considering systems' vulnerabilities and exposures to a range of hazards and threats.⁵ This evolution shaped the understanding that no matter the potential source of disruption, certain infrastructures are essential for the functioning of the state, economy, and society, making them "critical".⁶

2.1 Defining Critical Infrastructure

Over time, different definitions of vital systems and CI have emerged and changed. The current definition of Critical National Infrastructure by the United Kingdom's National Protective Security Authority captures the different aspects and fits the broader European understanding of CI:⁷ "National Infrastructure are those facilities, systems, sites, information, people, networks, and processes, necessary for a country to function and upon which daily life depends. It also includes some functions, sites and organizations which are not critical to the maintenance of essential services, but which need protection due to the potential danger to the public (civil nuclear and chemical sites for example)."⁸

This definition also matches Switzerland's Federal Office for Civil Protection (FOCP) understanding of CI, specifying them as the services and supply systems essential to the economy and the livelihood of the population.⁹ The FOCP has defined the sectors Energy, Finances, Information and Communication, Public Administration, Public Health, Public Safety, Transport, Food and Water, and Waste Disposal as critical. Furthermore, FOCP's methodological approach and assessments identify 27 sub-sectors within these main sectors, designating systems and their operations/operators as part of CI.¹⁰ In essence, these infrastructures are crucial to society and its welfare. The interruption or unavailability of their services can pressure a society in the short- or long-term and fuel crises.¹¹ Strong interdependences also characterize today's CI. For example, communication infrastructure is dependent on the energy infrastructure for its operation and vice versa. These interdependencies can be physical, geographical, or logical in nature. An adverse incident in one system of infrastructure can trigger ripple or cascading effects throughout this system of systems.¹² Alongside the increasing interdependencies, additional trends such as globalization, urbanization, and cyberization can further amplify the vulnerability and exposure of CI. While the cyberspace, which harbors most of the modern infrastructure, has put new threats onto the map, such as cyberattacks or IT outages, urbanization and the systems required to run large cities have created higher concentrations of CI in densely populated areas.¹³ In addition, the ownership and operation of CI can span from fully government-controlled over semi-private arrangements to privately operated CI, whereas in Western countries the majority of CI are operated by the private sector (in certain instances under a government mandate), requiring public-private-partnerships and collaboration to be at the core of any CI governance efforts.¹⁴ While many western European countries are already adapting definitions and policies around CI, Ukraine enacted its first piece of legislation on CI in November 2021. Designed in line with the European understating of CI, the Ukrainian law defines CI as:¹⁵ "a set of critical infrastructure facilities", whereas CI facilities are "infrastructure facilities, systems, their parts and their aggregate, which are important for the economy, national security and defense, the disruption of which may harm vital national interest". Furthermore, the law defines the criteria that classify objects as CI and categorizes 17 sectors of vital functions and services that are of interest for national security (Article 8).

The recent geopolitical changes and shifts in the security landscape have led the EU to replace its 2008 Directive on CI and issue a new directive at the end of 2022, which now refers to Critical Entities rather than CI.¹⁶ "Critical entities, as providers of essential services, play an indispensable role in the maintenance of vital societal functions or economic activities in the internal mar-

ket in an increasingly interdependent Union economy.” The European Commission also stresses that CI and cyber can no longer be viewed separately and therefore repeatedly refers to its revised Directive 2018/2555 on cybersecurity, in which it describes the inherent nature of cyber across the domains of CI.¹⁷

The presented definitions underline the critical nature of these systems for a functioning state, economy, and society. With criticality comes the need to sustain or improve the stability of one’s systems and the assessment of potential sources of disruption and vulnerability.

2.2 Critical Infrastructure Protection and Resilience

Critical infrastructure protection (CIP) is the concept and process of adequately protecting CI from natural hazards, technological and man-made accidents, and deliberate attacks (e.g., sabotage, terrorist attacks, or armed conflict).¹⁸ Over the course of the 20th century, in parallel and influenced by the increasing incorporation of vital systems or infrastructures as objects of protection and strategic importance in military doctrine, the vulnerabilities of governments and societies became increasingly visible and needed to be addressed. In the 1950s, the US government started to map vulnerabilities spatially to understand where an impact on infrastructure could occur and how it would affect the population. These assessments were heavily based on population dynamic studies to understand how a (nuclear) attack would impact urban life, including the assets and infrastructure that enable it. As a result, an extensive list of elements was drawn up that would be crucial for civil defense and the safety of people, industries, and freedom of action.¹⁹ By listing and mapping these elements, vulnerabilities became more visible and underlined the emerging notion that not just deliberate attacks could disrupt the functioning of infrastructure but a broad range of hazards and threats. While it was broadly understood that infrastructure has to be protected against intentional threats, the transferability of US civil defense efforts to those of emergency management domains and vice versa became evident throughout the 1960s and 1970s. Strategic planners concluded that an all-hazards approach to protect infrastructure would also support the preparedness against conflict-related attacks.²⁰ With the end of the Cold War, the focus on protecting people and infrastructure gradually shifted from a conventional military or nuclear threat towards disasters and emergencies in general. The term CIP emerged in the 1990s and was introduced by the Clinton administration by appointing the Presidential Commission on Critical Infrastructure Protection. This commission mainly dealt with the increasing vulnerabilities stemming from the linkage between information systems and technical infrastructures.

Nevertheless, the meaning of CIP was truly amplified by 9/11 and its aftermath, raising the Western concerns of potential sabotage and terrorist attacks against infrastructure throughout the USA and Europe.²¹ While these types of events have relatively low probabilities of occurrence but high consequences, they are still difficult to predict and forecast. In addition, the range of possible hazards and sources of threats is inconclusive and may also extend to not yet identified or quantified risks. Consequently, CI stakeholders had to address this security problem differently.²² Since governments and CI operators could not anticipate every scenario or identify every threat (hazard-specific view), it made more sense to understand the vulnerabilities within the CI systems and reduce them in a systematic way. This approach should allow authorities and operators to strengthen the overall system and be better prepared to deal with any disruption through an all-hazards approach.²³ This all-hazards approach opened the door to expand CIP to CI resilience. The term resilience has been defined and studied in several fields and for different purposes. A general understanding stems from the engineering sciences, describing a system’s ability and speed to return to its initial state in case of perturbation.²⁴ For disaster and crisis management, the term had to reach into the social and social-ecological sphere that accounts for social actors and human systems. In this sense, resilience is understood as a system’s ability to absorb disruptions, cope with crises, maintain core functionality, and the capacity to adapt, improve, and transform.²⁵

Therefore, integrating resilience into CI and CIP has taken place gradually. The aforementioned EU Directive from 2022 states in Article 2: “Critical entities should be in a position to reinforce their ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from incidents that have the potential to disrupt the provision of essential services.”²⁶ The Directive puts strong emphasis on the entities that provide essential services which are crucial to “[the] maintenance of vital societal functions, economic activities, public health and safety, or the environment”. It expands the sectors considered critical, thereby repelling the 2008 Directive which focused mainly on the assets of CI operations in the energy and transportation sector.²⁷ A supplement to the 2022 Directive, published in 2023, provides further clarity on *essential services*, providing a non-exhaustive list of such services to be maintained by the entities.²⁸ These new policies reiterate that resilience depends, among other factors, on CI operators and their physical and non-physical assets to ensure the essential services and that the different sectors of CI are highly interconnected. It urges EU Member States to review and strengthen their national CI resilience, considering the national and international interdependencies. This underlines the shift from a pure CI assets protection approach

towards the objective of overall resilience. The interpretation of making CI resilient against various hazards and threats is incorporated in the Organization for Economic Cooperation and Development's (OECD) perception of how to govern CI and under the United Nations Office for Disaster Risk Reduction's (UNDRR) Sendai Framework efforts, putting special emphasis on cybersecurity.²⁹ Likewise, the updated Swiss National Strategy for Critical Infrastructure Protection from 2023 highlights the importance of cross-sectional resilience of the entire CI system to deal with emergency and crisis situations.³⁰ In Ukraine's 2021 law on CI, resilience is defined as "the state of critical infrastructure that ensures its ability to function normally, adapt to constantly changing conditions, withstand and quickly recover from threats of any kind."³¹ Here, resilience results from an ongoing CIP process, likely shaped by Ukraine's regulatory and organizational efforts over the past decades and influenced by emerging threats, challenges, and experiences, such as the hybrid threats from Russia. According to NATO, resilience in the face of hybrid threats and armed conflict inherently arises from Article 3 of the NATO Treaty and is to be understood as societal and national resilience. Societal resilience, which is interlinked with civil preparedness, supports national resilience and security against any attack. Therefore, NATO countries should strengthen their resilience capacities in seven baseline areas that inherently incorporate CI resilience. The baseline areas defined at the 2016 Warsaw Summit are: "continuity of government, energy supplies, uncontrolled movement of people, food and water resources, mass casualties and disruptive health crisis, civil communication systems, and transport systems."³²

3 Critical Infrastructure Protection in Ukraine

On 24 February 2022, Russian forces started the invasion of Ukraine after months of amassing troops and equipment along the Ukrainian border. With the declared aim of "demilitarizing and denazifying" Ukraine and protecting Russians in Ukraine, Vladimir Putin announced a special military operation.³³ Following the initial air strikes, ground forces quickly advanced and seized control over larger areas of Ukraine, reaching the outskirts of Kyiv within a few days.³⁴ Failing to swiftly take the capital and remove the government of President Volodymyr Zelenskiy, Russian troops withdrew from the Kyiv area to launch the next offensive in April 2022. This time, they focused their efforts on eastern and southern Ukraine, where the majority of the fighting has taken place ever since.³⁵ Despite Russian attempts to capture the full extent of the Donbas in March 2023 and the Ukrainian counter-offensive, grounds have not shifted significantly, leading to increasing fortification and entrenchment of the front lines in eastern Ukraine.

Over the first eight months, a growing pattern of deliberate targeting of CI by Russian forces emerged, reaching an initial peak in October 2022. In the beginning, the attacks were mainly aimed at infrastructure that directly supported the war effort (e.g., fuel supply or communication) and – to some degrees unexpectedly – at the Zaporizhzhia Nuclear Power Plant.³⁶ The longer the war lasted, however, the more evident the deliberate targeting of CI became, as demonstrated by the attacks on energy infrastructure from October 2022 onwards. Russia has deployed kinetic weapons and cyber means (including the use of Russian non-state actors) to carry out these operations.³⁷ In line with Russian military doctrine, the Ukrainian population was put under increasing pressure as the winter months approached.³⁸

This blend of conventional and irregular warfare, deployed across the full spectrum of conflict escalation and in parallel, would support the as yet ill-defined concept of hybrid warfare, where the exposure and vulnerability of CI become an attractive target in such conflict environments.³⁹

The events inside and outside Ukraine, such as the sabotage of the Nord Stream 2 underwater pipeline in September 2022, initiated discussions around CIP and resilience once again. For example, the EU called on its Member States to strengthen their resilience, underlined by the Council recommendation of 8 December 2022.⁴⁰ The EU and NATO have launched a Critical Infrastructure Resilience Task Force to foster collaboration (e.g., using Ukraine as a scenario for tabletop exercises), increase situational awareness, and develop resilience principles.⁴¹ However, Russian efforts to destabilize and undermine infrastructure in Ukraine did not begin with the 2022 inva-

sion. Placing these events within a historical context is crucial for understanding Ukraine's state of preparedness and the resilience of its critical infrastructure.

3.1 2014–2022

Russian interference with Ukrainian CI began as early as 2014 with the Euromaidan and subsequent events, such as the annexation of Crimea and Russian expansion of influence and control into the Donbas region.⁴² The disruption or seizure of CI as part of these Russian efforts has already put some stress on Ukrainian CI systems.⁴³ There is compelling evidence that Russia targeted CI in Ukraine to test and refine its cyber warfare capabilities against a weaker state, as was the case in the 2008 Georgian War.⁴⁴ The most significant attack occurred in December 2015, when a group called Sandworm targeted the Ukrainian power grid. This incident impacted three power distribution centers, leaving over 230,000 consumers without power for up to six hours.⁴⁵ Cyberattacks on CI and public authorities continued in 2016 and culminated in 2017 with the NotPetya ransomware attack, which predominantly affected Ukrainian government, energy, and financial institutions.⁴⁶ Furthermore, campaigns in the digital, media, and information domains repeatedly attempted to discredit the Ukrainian government by spreading false information and mistrust.⁴⁷ These experiences allowed authorities and organizations to implement early measures to strengthen Ukraine's stance against threats from Russia, which later proved to be one of the sources of the country's resilience in the face of the full-scale war.⁴⁸

3.1.1 Policy Reforms

Between the events of 2014/15 and the full-scale invasion in February 2022, different policy reforms have been announced or adopted in Ukraine. Some of them were specifically aimed at CIP and resilience, while others supported CIP efforts but primarily promoted Ukraine's Euro-Atlantic aspirations and integration. The current Ukrainian CIP and resilience system and legislation are rooted in efforts initiated in 2011 by the National Institute for Strategic Studies to create an interagency expert working group to address this issue. Until then, CI and CIP were not included in Ukrainian legislation. The next steps required coordination since the overall Ukrainian protection and crisis system consisted of several agencies acting in different silos (e.g., civil protection, cyber, terrorism). The institute began educating political leaders, institutions, and authorities involved with CI through reports, conferences, or tabletop exercises, with increasing support from NATO.⁴⁹ Following the events in 2014/15, the topic gained increasing attention, which led to the Green Book on the issue of Critical Infrastructure Protection in Ukraine in

October 2015 and to tangible decisions by parliament and the government.⁵⁰ The path to CIP legislation was further supported by other policy reforms and decisions in the field of security such as the National Security Strategy of Ukraine and the Cyber Security Strategy of Ukraine.

A concept for CIP approved by the government in 2017 foresaw a cross-sectional and -departmental CIP state system intended to define roles and responsibilities as well as organizational structures.⁵¹ In parallel, Ukraine adopted its first law On Basic Principles of Cybersecurity of Ukraine in 2017.⁵² Although the Law of Ukraine on Critical Infrastructure entered into force in November 2021 and was put into effect on 15 June 2022, a first draft of the law from 2019 allowed government agencies and CI leadership to familiarize themselves with CIP beforehand.⁵³ This fact becomes evident when considering that the protection of CI and its resilience is also mentioned in other policy documents, such as the 2020 National Security Strategy of Ukraine, the 2021 Foreign Policy Strategy of Ukraine, and the 2021 Concept on the National Resilience System.⁵⁴ In addition to the specific CIP and cybersecurity reform efforts, Ukraine initiated a decentralization reform in 2014 to shift administrative and fiscal powers from the central government to amalgamated territorial communities (ATC), which consist of merged local municipalities and enable more self-governance in areas such as education or healthcare. It addressed the historically centralized Soviet system with the aim of promoting greater transparency and accountability at the local level. The fiscal decentralization allowed ATCs to dispose of a higher share of tax revenues, make tax collection more efficient, and support local decision-making and investment decisions, e.g., in infrastructure.⁵⁵

3.2 2022–2023

With the start of the invasion, the tools and targets for attacks on CI expanded. What has been cyber-heavy in the run-up to the invasion was now combined with kinetic strikes by the Russian armed forces across different sectors and domains of CI.⁵⁶

A few hours before the physical invasion by military troops, cyberattacks disrupted Ukrainian broadband capacities by targeting Viasat's satellite modems throughout the country and overloading the Viasat KA-SAT's network. This left thousands of households without broadband access and hampered the communications capabilities of the military and CI facilities.⁵⁷

With the invasion, the air traffic infrastructure was targeted first. Not only military airfields were attacked, but also civilian aviation infrastructure such as Boryspil International Airport in Kyiv and Kherson International Airport. As a result, civil air traffic has been completely shut down to this day. Second, following vari-

ous Russian naval maneuvers in the Black Sea, the Sea of Azov, and the Kerch Strait, which led to protests by the Ukrainian authorities, Ukraine's commercial access to the sea was completely blocked. In addition to the sea-based traffic routes, transportation systems on land were also attacked or at least affected due to collateral damage. This includes roads, railways, and bridges. Although the backup control center of the state-run railway company Ukrzaliznytsia, the largest employer in Ukraine and responsible for over 20,000 km of rail network, was hit by a missile on 25 February 2022, the rail network itself was less affected than other transportation infrastructure. Russia was to a certain extent dependent on the railway for its military logistics. The railways, therefore, quickly became the backbone of the Ukrainian transportation sector, as they kept services running and allowed the movement of people and goods as well as humanitarian and military logistics.

Furthermore, civil, commercial, and military logistics heavily depend on road transportation, making it a worthwhile target. Not only Russia is targeting critical nodes in the road network, but Ukraine is also forced to attack transportation infrastructure, such as roads and railways, in the occupied territories to disrupt Russian war logistics (e.g., by targeting the Kerch Strait Bridge).⁵⁸

With the onset of the war in Ukraine, a major industrialized country became the target of an inter-state armed conflict, with its industries being severely affected. Drone and missile attacks targeted agricultural facilities, chemical sites, oil and gas infrastructure, and power plants and have taken a heavy toll on the country's economy but are also likely to have devastating effects on the environment. The extent of environmental damage cannot yet be conclusively quantified. Still, the war will result in billions of dollars in direct and indirect environmental damages and impact on human health through the possible loss of ecosystems, biodiversity, and agricultural production capacity.⁵⁹ Heavy industries, such as mining or steel production, appear to be a preferred target, with the consequence that considerable amounts of toxic and harmful substances are released and contaminate large areas in the event of damage or mismanagement. While response measures for environmental catastrophes exist in peacetimes, they are difficult to implement during war.⁶⁰ Moreover, the observed attacks on facilities of the agroindustry led to an estimated 40 per cent reduction in the usage of agricultural land. As an example, the destruction of the Kakhovka dam in June 2023 resulted in floods damaging housing, infrastructure, and agricultural fields on both sides of the Dnieper River and polluted the water downstream.⁶¹

The environmental toll, a labor shortage due to military drafting, war-related population movements, and the disruption caused by blocked seaports led to a considerable decline in exports. With Ukraine being among the top global agricultural producers and exporters of sun-

flower oil, corn, wheat, rapeseed, and barley, the impact on global food supply chains has been alarming.⁶² The environmental consequences of the war in Ukraine will affect the country and society for decades to come, including the harm from mines and unexploded ordnance, further aggravating human and environmental security.

The Russian aggression also affected the healthcare system. As of April 2022, the World Health Organization verified over 100 attacks on health infrastructures that put public healthcare and personnel at risk.⁶³ By the end of 2022, investigations indicate that 218 hospitals and clinics have been damaged or destroyed, mainly in the Kyiv area and along the front line in the East. Additional healthcare assets such as ambulances, pharmacies, blood centers, and dental centers have also been affected.⁶⁴

Another critical system that has been adversely affected by the war is the education system. While education is crucial for the development and well-being of children, educational institutions, especially in frontline or Russian-occupied regions, have been shelled and bombed. In some instances, schools had to be converted into shelters for the local population.⁶⁵

The CI sector most reported on in Western media was the energy infrastructure. As of November 2022, the Dutch think tank PAX has verified energy-related incidents in 17 Ukrainian regions, with a particular concentration in the regions Zaporizhzhia, Donetsk, Kharkiv, Dnipropetrovsk, Kyiv, and Mykolaiv.⁶⁶ These incidences include attacks on or unintentional damages to power production facilities (nuclear power plants, hydrological and thermal power plants), energy storage, and power and heating distribution systems.⁶⁷ Observations suggest that, in addition to putting pressure on Ukrainian society, economy, and military efforts, the energy infrastructure also played a role in determining the time frame for the invasion. Pre-war efforts to synchronize Ukraine's integrated power system (IPS) with the European Network of Transmission System Operators for Electricity (ENTSO-E) led the state-owned transmission system operator Ukrenergo to sign an agreement to interconnect with the European power system in 2017. On the day of the invasion, a scheduled test of the Ukrainian power system took place. The test included a three-day self-reliance test (i.e., island mode) of the power system during which the electricity needs of the country were met solely by domestic generation without being connected to any other power grid. The successful outcome of this test was a precondition to start the synchronization with ENTSO-E, which eventually occurred through an emergency synchronization in March 2022 (see also Section 4.1.2).⁶⁸ Thus, Russia began its invasion as Ukraine was decoupled from both the Russian and continental European power grids. However, it can be assumed that at the beginning of the invasion, Russia was not concerned with destroying Ukraine's energy infra-

structure, but rather using it to hamper Ukrainian military and defense capabilities.

Nevertheless, on 15 June 2022, the Ukrainian Minister of Energy announced that approximately 614,000 consumers were without electricity and 179,000 consumers without gas.⁶⁹ In September and October, Russia began targeted attacks on the Ukrainian energy sector, so that by the end of 2022, an estimated 40 per cent of the country's energy production and distribution infrastructure had been damaged.⁷⁰ With winter approaching, Russia aimed at the population's well-being by disrupting cities' combined power and heating plants. The attacks on energy infrastructure had cascading effects on other CI sectors, including government, healthcare, transportation, communication, and industrial activities. For example, when Russian missiles hit substations in Lviv, train services were temporarily disrupted, and the health of people cut off from power deteriorated significantly.⁷¹

The first months of the invasion exposed certain military protection gaps in Ukrainian CI. However, over time, a multi-layered air defense system was gradually set up with the support of Western military assistance. The boosting of air defense allowed Ukraine to better protect vulnerable CI, increasing successful missile and drone interceptions from 40–50 per cent observed on 10 and 11 October 2022 to 75–80 per cent of cruise missiles in December 2022.⁷² However, the available air defense systems must protect not only civilians and civilian infrastructure, but also military forces and maneuvers.⁷³ In parallel and complementing the kinetic attacks on Ukrainian infrastructure, Russian cyberattacks persisted throughout the invasion. In April 2022, Microsoft's Digital Security Unit reported that Russian military intelligence conducted destructive cyberattacks on the Ukrainian government hours before the attack started. Other CI, such as IT services, the energy sector, and financial organizations, were also targeted.⁷⁴

At the end of 2022, the First Deputy Minister of Internal Affairs stated that 702 CI objects had been damaged or destroyed since the beginning of the invasion.⁷⁵ Russia's targeted attacks on infrastructure in Ukraine have been criticized as a fight against the population and therefore a war crime. Russian leadership does not deny the precision strikes against infrastructure, but claims that only infrastructure of military origin or those supporting Ukrainian military efforts are hit, and therefore the attacks will continue.⁷⁶

3.2.1 Policy Reforms (cont.)

Despite the Russian invasion, the Ukrainian government continuously enacted, adapted, and introduced policies and regulations to secure essential operations and respond to the immediate challenges inflicted by the war. Among the first policy actions taken by Ukraine, was the

declaration of martial law, which remains in effect to-day.⁷⁷ Martial law inevitably leads to an increased degree of centralization of various aspects of administration and public services. However, stronger local governance, induced by the decentralization reform in 2014, is assumed to play a crucial role in Ukraine's resilience by increasing capabilities and capacities for local decision-making, enhancing flexible collaborations, and bolstering robust networks.⁷⁸ Resilience was reflected in increased preparedness, greater reliability of public services during times of distress, and a higher degree of autonomy over amalgamated territorial communities (ATC) resources.⁷⁹ The OECD stresses the importance of continuing the momentum of the decentralization reform and recommends strengthening regional and local involvement in planning, funding, and executing governmental and public services.⁸⁰ With regard to CIP, the State Service for the Protection of Critical Infrastructure and Ensuring the National Resilience System of Ukraine was established on 12 July 2022. This step is rooted in the previously mentioned 2021 law on CIP and is intended to ensure that the policies on CIP are implemented.⁸¹ The new state service aims to coordinate CIP and resilience as a dynamic and changing concept that requires continuous adaptation due to changes in the security environment.

3.3 Damage Assessments and Estimations

Alongside military and non-military support efforts, many countries have already signalled firm commitments to postwar reconstruction efforts in Ukraine. These commitments require ongoing damage and loss assessments to determine the extent of reconstruction needs, generate a foundation for the financial and operational early recovery, and set the ambitions for Ukraine's long-term reconstruction. These assessments also provide insights into CI and critical systems and allow for inferences based on the reported information.

The most notable and comprehensive damage assessment to date is the Ukraine Rapid Damage and Needs Assessment: February 2022 – February 2023, published jointly by the World Bank, the Government of Ukraine, the EU, and the UN, covering the first 12 months of the war. It estimates the direct damage to buildings and infrastructure at 135 billion USD, mainly concentrated in the regions along the front line, such as Donetsk, Zaporizhzhia, or Luhansk. Recovery and reconstruction needs are estimated to have already surpassed 400 billion USD by February 2023, concentrated in the social sector (e.g., housing, social protection) and CI (e.g., energy and transportation).⁸² In addition, the World Bank and the UN Development Program (UNDP) are specifically addressing the energy sector, with the Ukraine Energy Damage As-

assessment laying the groundwork for the potential reconstruction of the energy infrastructure by incorporating a green energy transition.⁸³ The assessments claim that about 45 per cent of all transformers have been damaged or destroyed in the Ukrainian-controlled area. Power generation capacity has been halved compared to pre-invasion levels, including an over 60 per cent decrease in thermal power generation.⁸⁴ A task force from the International Energy Charter has begun with monthly assessments of the Ukrainian energy sector and infrastructure.⁸⁵ However, many damage assessments and reports refer to the estimates on infrastructure damages by the Kyiv School of Economics (KSE). With support from the Ukrainian government, KSE runs a platform called “Damaged in Ua”, including the project “Russia Will Pay”, which aggregates physical infrastructure damage from various sources, including citizen reports.⁸⁶ As of June 2023, KSE estimates that total direct damage (at replacement costs) to Ukrainian infrastructure has surpassed 150 billion USD (see Table 1).⁸⁷

As one of the few assessments, KSE also attempts to quantify the impact of the war on railway and road infrastructure. In contrast to civil aviation and the manageable number of maritime transportation infrastructure, reporting on the extensive land transportation networks with thousands of kilometers of (rail)roads is challenging. The institute estimates damages in transportation at 36.6 billion USD and losses at 23.2 billion USD as of June 2023. These estimates include damage to 19 civilian airports and airfields, blockage or occupation of seaports, 507 km of disrupted railway lines in Ukrainian-controlled areas, over 25,000 km of damaged public roads, and more than 340 incapacitated bridges.⁸⁸

The interim report of the International Telecommunication Union offers a comprehensive summary of the impact of the war on the telecommunication and ICT sectors. It states that by August 2022, infrastructure damage (including fixed and mobile telecommunication, television, radio, satellite, and IT industry) has occurred in at least 10 of the 24 regions. In areas with active fighting, total damage to fixed and mobile telecommunication infrastructure is expected.⁸⁹

Other institutions and researchers have produced detailed and informative reports on single (critical) sectors that assess damages more precisely than just monetary damages, losses, and needs quantifications. One example are the reports of PAX on energy, fossil fuel, agriculture, and environmental impacts.⁹⁰ Physicians for Human Rights provide an assessment of the healthcare domain.⁹¹ The Human Impact Assessment of UNDP offers an extensive insight into the socio-economic effects of the war, for example on living standards, health, education, livelihoods, food security, social inclusion, and gender equality.⁹² The report helps in understanding the human harm caused by CI impairments, especially energy dependencies. It states that 7.1 million Ukrainians have been pushed into poverty, and 17.6 million need humanitarian assistance. It recognizes that circumstances vary across the country and highlights coping mechanisms of the Ukrainian people one year after the beginning of the invasion.

Many regions are inaccessible to experts due to the ongoing war, and there are only a few reports from the field. The report from the Estonian International Center for Defence and Security on lessons for civil defence from the first months of war constitutes an exception

Table 1 KSE total estimate of infrastructure damages as of June 2023

Property type	Total estimate of infrastructure damages in billion USD	Total estimate of infrastructure losses in billion USD
Residential buildings	55.9	16.4
Infrastructure	36.6	23.2
Assets of enterprises, industry	11.4	51.5
Education	9.7	2.1
Agriculture and land resources	8.7	40.3
Energy sector	8.8	27.2
Forestry fund	4.5	-
Transport vehicles	3.1	0.3
Healthcare	2.8	2.7
Communal services and utilities	2.7	3.5
Trade	2.6	33.9
Culture, sport, tourism	2.4	10.8
Administrative buildings	0.5	0.04
Digital infrastructure	0.5	1.4
Social sector	0.2	7.1
Financial sector	0.04	4.3
Total	150.5	224.6

and provides some insights from the ground.⁹³ In this context, the rapid damage assessments by the World Bank et al. conclude that the response time of the Ukrainian civil protection and emergency system, which was already lagging behind before the war, has increased, stretching its resources to the maximum.⁹⁴ An important expansion of this system was achieved in April 2023, when Ukraine joined the EU Civil Protection Mechanism (UCPM).⁹⁵ Remote sensing, data mining, and open-source intelligence efforts have promoted the geospatial analysis, reporting, and presentation of the military situation with the support of GIS tools.⁹⁶ These tools and sources are also used to analyze and document attacks on and damages to civilians, CI, and the environment.⁹⁷ Examples for this are the damage assessments of the United Nations Satellite Centre (UNOSAT), or the platform Ecodozor of the Geneva-based NGO Zoï that is supported by the Organization for Security and Co-operation in Europe (OSCE) and the UN Environment Programme (UNEP), and attempts to geolocate infrastructure damages and their environmental impacts.⁹⁸ As part of the Eyes on Russia project, the Centre for Information Resilience in cooperation with the open-source portal Bellingcat and their portal Civilian Harm in Ukraine offer maps and a mapping database that allow to track attacks against CI and civilian infrastructure.⁹⁹

3.3.1 Reconstruction Efforts and Funding

One of Ukraine's lifelines in overcoming the challenges of the war is international support, including both military and non-military assistance. A continuously updated overview of military, financial, and humanitarian aid is provided by the Ukrainian Support Tracker from the Kiel Institute for World Economy, focusing on the contributions from The Group of Seven (G7) and EU Member States to Ukraine.¹⁰⁰ Amidst these ongoing stabilization efforts, the topic of recovery and reconstruction of Ukraine gained political traction. Rebuilding Ukraine has become a priority for the USA and EU Member States, as there are economic, governance, and security interests at stake.¹⁰¹ This priority has led to two conferences. First, the Lugano Conference in Switzerland in July 2022 created a political framework that provides for the continuation of Ukraine's reform efforts to enable the country to lead its own "building-back-better" approaches.¹⁰² It was followed by the Ukraine Recovery Conference 2023 in London. The aim of this conference was to discuss how private sector investments can support the reconstruction process and to raise 60 billion USD for this purpose.¹⁰³ In parallel, several institutions such as the EU, the OECD, and the US-German-Marshall Fund advocate for the reconstruction of Ukraine, while plans and frameworks are being drawn up.¹⁰⁴ At the same time, Ukraine is actively analyzing the damages and planning its recovery.¹⁰⁵

4 Case Studies

The following case studies investigate how Ukrainian CI ensured their functionality in the face of the Russian aggression and consequently demonstrated resilience. The aim is to identify prerequisites, system characteristics, or actions that establish, enhance, or maintain CIP and resilience and have broader applicability and transferability within the domain of CI.

The three analyzed sectors are Energy, Transportation, and Information and Communication. These three sectors are also considered CI in Switzerland, align with the EU's understanding of essential services and critical entities, and constitute baseline requirements for NATO's concept of national resilience.¹⁰⁶ To identify and assess CI resilience, the case studies highlight elements that can be attributed to the proposed CI resilience measures of the EU. With reference to the EU Directive 2022/2557, resilience is identified in the following three case studies as the ability of CI systems to *prevent, protect against, respond to, resist, mitigate, absorb, accommodate, and recover* from incidents, or a combination thereof. In addition to tangible measures taken by all relevant actors, ability also includes characteristics and factors that enable a system to be resilient and ensure the essential services. This should contribute to a more holistic understanding of the overall resilience of the Ukrainian CI system and not focus exclusively on physical assets. For critical entities, two further aspects are defined in Article 13 of the EU Directive: "*to ensure adequate employee security management*" and "[to] *raise awareness about the [mentioned] measures*".¹⁰⁷

In this context, a necessary clarification on the subject of cyber must be made. Cyberattacks and cyber defense and resilience are important in most CI sectors, as expected from the previously mentioned definitions that explain the inherent existence of cyber in all modern CI sectors. In this report, however, the topic of cyber is mainly, albeit briefly, touched upon in the case study on Information and Communication, as information and communication technology is the fundamental infrastructure that enables cyber resilience. The report does not focus on the technicalities of cyber resilience.

4.1 Energy

4.1.1 Defining the Sector

According to the FOCP, the CI sector Energy consists of petroleum, natural gas, and electricity, as well as district and process heating.¹⁰⁸ The supply chains of petroleum, gas, and electricity consist of all the facilities and activities necessary for uninterrupted delivery to consumers, typically including production, transmission, storage, distribution, and trading. Petroleum and natural gas serve the industry and the population mainly as energy sources, for example, in chemical processes, as fuel, or for heating and cooking. Petroleum is also used by industry as a raw material, for example, to produce plastics. Electricity is the most critical energy source for the economy and the population, as it is a prerequisite for the functioning of, for example, most business processes, communication technologies, and other CI. The Swiss National Strategy for Critical Infrastructure Protection of 2023 assigns very high criticality to electricity and petroleum supply and high criticality to natural gas supply.¹⁰⁹ Regarding critical entities in the energy sector, the EU additionally considers district cooling and hydrogen, but otherwise covers the same energy sources as well as facilities and activities (production, transmission, etc.) as Switzerland.¹¹⁰ In its 2023 Final Assessment Report, the EU-NATO Task Force on the Resilience of Critical Infrastructure highlights the dependence of modern economies and societies on an uninterrupted supply of energy from a mix of sources and the difficulty of protecting diverse and widespread energy infrastructure.¹¹¹ A resilient energy supply is one of the seven baseline resilience requirements of NATO and is defined as “ensuring a continued supply of energy and having backup plans to manage disruptions.”¹¹² Ukrainian legislation on CI also identifies energy supply as a vital sector, explicitly including thermal energy.¹¹³

4.1.2 Baseline and Developments since the Beginning of the Invasion

Before the Russian invasion in February 2022, Ukraine had a well-developed energy industry and extensive energy supply infrastructure. The sector accounted for about 17 per cent of GDP and was a crucial source of the country's economic growth and modernization.¹¹⁴ The country has abundant gas, petroleum, and coal deposits, mainly in the Dnipro-Donetsk region in the east, the Carpathian region in the west, and the Black Sea and the Sea of Azov region in the south.¹¹⁵ Despite a century-long history of hydrocarbon production, its potential has not yet been fully realized, leaving Ukraine import-dependent even before the invasion. The country has also been an important transit country for petroleum and gas from the East to Europe with corresponding pipeline infrastructure. Ukraine's en-

ergy mix is diversified. In 2021, natural gas was the main source of energy (30 per cent), followed by coal (28 per cent), nuclear (23 per cent), petroleum (13 per cent), hydropower (3 per cent), and other renewables (<3 per cent).¹¹⁶ 100 per cent of the population had access to electricity, and about 95 per cent to clean cooking fuels.¹¹⁷

The Ukrainian petroleum industry includes six refineries and one gas and oil processing plant with a combined design capacity of over 50 million tons per year, which is about four times the domestic demand for petroleum products.¹¹⁸ Due to a lack of profitability and modernization, only the Kremenchuk Oil Refinery in the central Poltava region, with an actual production capacity of about 7 million tons per year, and the Shebelynka Gas and Oil Processing Plant in the Kharkiv region, with a capacity of about 0.5 million tons per year were in operation before the invasion.¹¹⁹ The petroleum transportation system consists of over 4,700 km of pipelines, 92 per cent of which are older than 30 years, 51 pump stations, and 11 large tank farms with a total capacity of about 1 million cubic meters. In 2021, Ukraine covered 81 per cent of domestic oil demand through imports, mainly from Russia, Belarus, and EU Member States.

Before 2022, Ukraine produced about 20 billion cubic meters (bcm) of natural gas per year or about 55 million cubic meters (mcm) per day, equivalent to approximately 70 per cent of domestic demand.¹²⁰ Ukraine has one of Europe's best-developed gas transmission networks, with a total length of 38,600 km, designed to transport gas from Russia and Belarus to Western and Central European countries.¹²¹ The domestic gas distribution network measures another 290,000 km.¹²² Ukraine has Europe's largest storage facilities, with a capacity of around 31 bcm per year at 13 underground locations. In 2021, Ukraine covered 33 per cent of domestic gas demand through imports.

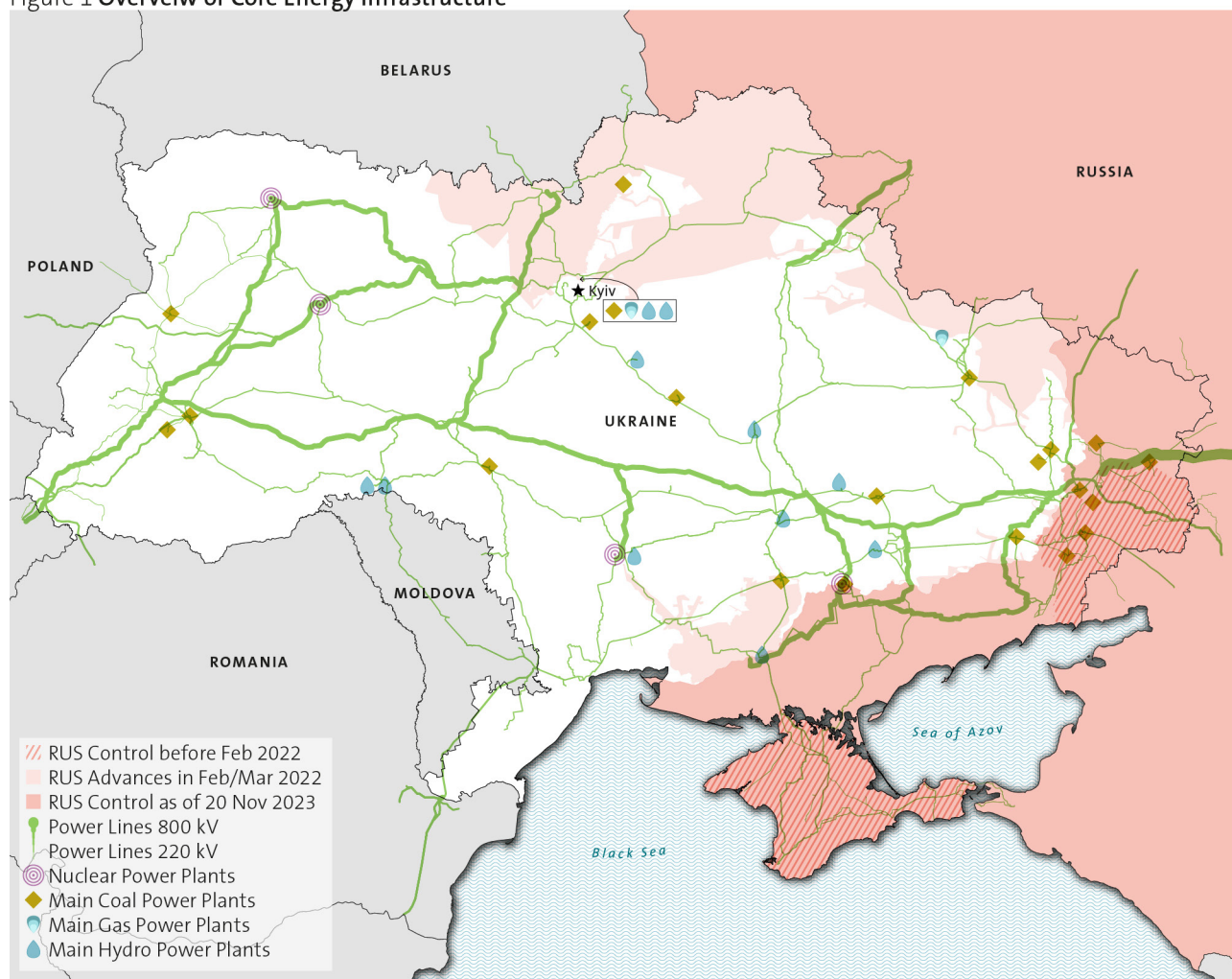
Further Reading

Thomas S. Popik, **“Preserving Ukraine's Electric Grid During the Russian Invasion,”** *Journal of Critical Infrastructure Policy* 3:1 (2022).

Tony Lawrence, **“Critical Energy Infrastructure: Lessons from Russia's War against Ukraine,”** and Oleksandr Sukhodolia, **“Ukrainian Energy Sector under Military Attack: Lessons for Resilience,”** Tomas Jermalavičius (ed.), *War and Energy Security: Lessons for the Future* (Tallinn: International Centre for Defence and Security ICDS, 2023).

Iryna Nikolaieva, Wim Zwijnenburg, **“Risks and impacts from attacks on energy infrastructure in Ukraine,”** PAX, 2022.

Figure 1 Overview of Core Energy Infrastructure



Source data: ISW, World Resource Institute, OpenInfraMap

In 2021, Ukraine had 54.5 GW of installed electricity generation capacity.¹²³ The country has four operational nuclear power plants with a total of 15 reactors, 16 thermal power plants (mainly coal but also oil and gas to cover peak demand), 49 combined heat and power plants, 11 hydropower plants, and some wind and solar power plants. The four nuclear power plants used to meet more than half of Ukraine's electricity needs, relying on nuclear fuel from Russia.¹²⁴ In 2021/22, Ukraine signed contracts with a US company to build new reactors and supply all nuclear fuel for the country in the future. The core power transmission network consisting of 220 kV to 800 kV lines, most of which was designed and built during the Soviet era, has a total length of 22,000 km, while the entire distribution network measures more than one million km.¹²⁵ Until February 2022, it ran in parallel with the Russian network but also had interconnections with Poland, Slovakia, Hungary, Romania, and Moldova.¹²⁶ As noted in Chapter 3.2, a planned three-day test of the Ukrainian grid in island mode began in the early hours of 24 February 2022 as part of Ukraine's pre-war intentions to de-

synchronize from the Russian grid and synchronize with ENTSO-E in 2023. Once the Russian invasion began, emergency synchronization with ENTSO-E was completed in record time by mid-March 2022, allowing electricity imports from and exports to European countries.¹²⁷

The Russian invasion of Ukraine can so far be roughly divided into three phases in terms of attacks on critical energy infrastructure. The first phase lasted from the beginning of the invasion in February until September/October 2022. It was characterized by a certain restraint of the Russian side to target CI in the energy sector unrelated to Ukrainian warfighting capabilities. The Russian leadership seemingly still believed in a quick victory and tried to capture the energy infrastructure as intact as possible.¹²⁸ During this phase, Russia primarily attacked the Ukrainian petroleum sector to impede fuel supplies. However, other energy installations also suffered damage in the fighting. The second phase lasted from September/October 2022 until March 2023. After numerous setbacks by its military in the summer of 2022, Russia shifted its strategy toward maximum destruction of the Ukrainian

energy system using long-range munitions. By cutting off the population from energy and other vital services such as heating, the Kremlin hoped to demoralize Ukraine and force Kyiv to make concessions or even surrender. In the third phase, which lasted from March to the present (November 2023), Russia changed its strategy again and somewhat reduced the intensity of its attacks on the Ukrainian energy system. Nevertheless, energy installations continue to be attacked with long-range munitions, damaged in battles, or deliberately destroyed by the Russian side, such as the Kakhovka Dam in June 2023.

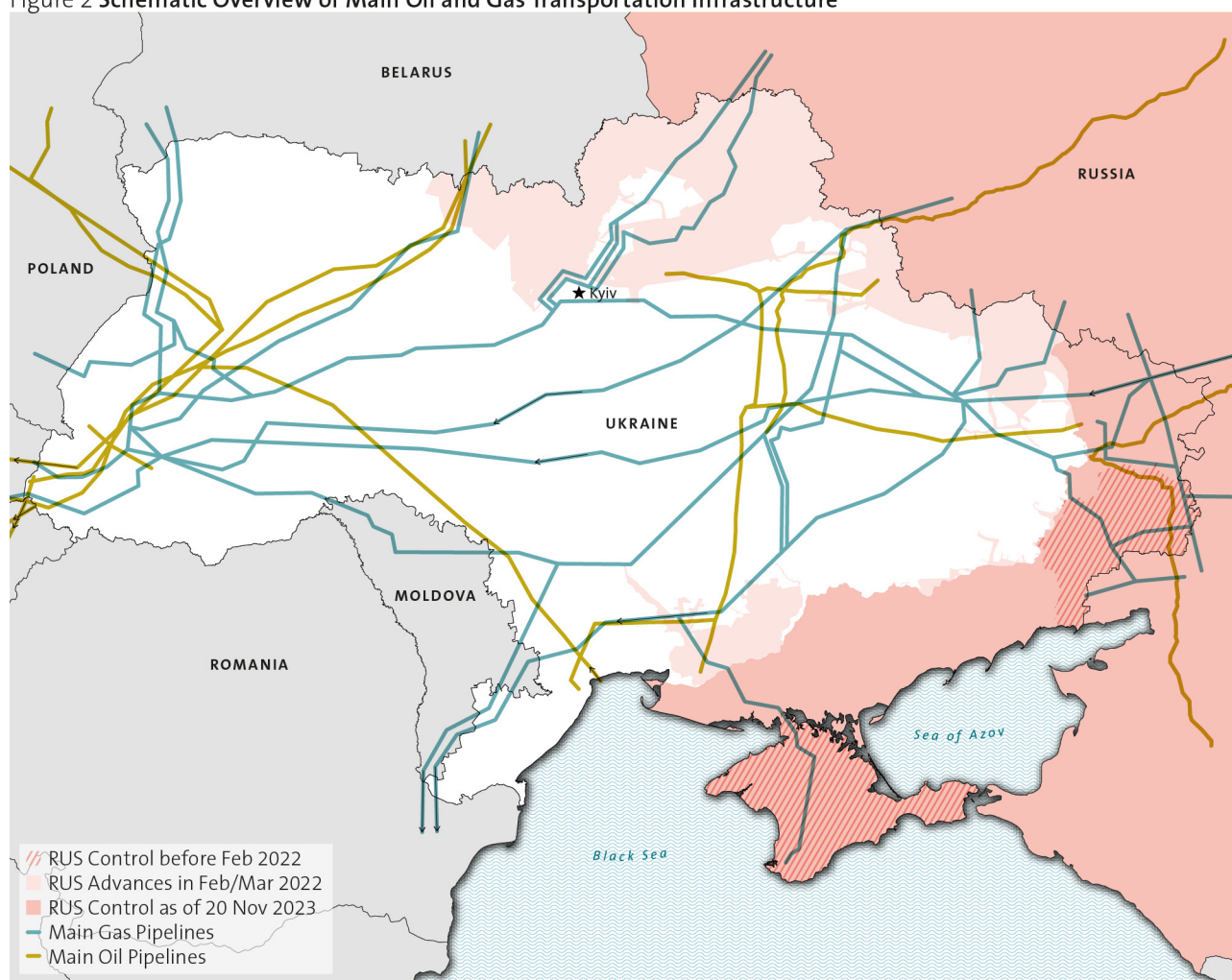
The petroleum industry was the first sector of Ukraine's energy supply that Russia attacked following its invasion, practically destroying it in the first phase until the summer of 2022. As early as 7 February 2022, Belarus stopped petroleum imports from Lithuania to Ukraine through its territory, straining the Ukrainian energy supply.¹²⁹ In the early weeks and months of the invasion, Russia concentrated its strikes on fuel depots at airports and oil terminals, as well as oil refineries.¹³⁰ Such attacks occurred in almost all regions of Ukraine, including Kyiv, Lviv, and Odesa. By September 2022, more than 28 big and small oil depots were destroyed or significantly damaged.¹³¹ The Kremenchuk Oil Refinery and adjacent fuel depots were attacked with missiles several times, causing the plant to cease operation in April 2022. The Shebelynka Gas and Oil Processing Plant suspended operations on 26 February due to Russian shelling and was irreversibly damaged by missiles in June 2022. Another large but non-operational oil refinery in Lysychansk in the Luhansk region was occupied by Russian forces in July 2022. As a result, Ukraine has been forced to suspend oil refining operations since summer 2022, and the entire petroleum industry has been severely crippled, leaving the country almost entirely dependent on imports.¹³² As import logistics proved challenging, e.g., due to the incompatibility of Ukrainian and Polish rail gauges (see Chapter 4.2), and capacity was therefore limited, fuel shortages occurred in the summer of 2022.¹³³ They had significant cascading consequences for the economy and the functioning of other CI, e.g., petroleum is a backup fuel for many power plants in Ukraine. During the second and third phases, Russia continued its attacks on the remaining oil infrastructure, targeting additional petroleum depots, transmission facilities, and shutdown refineries, including a newly constructed one in the Kharkiv region in June 2023.¹³⁴

The Ukrainian natural gas sector has also been under attack from Russia since the first phase, but it has proven more resilient than the petroleum industry. By September 2022, more than 150 gas production sites had to cease operations due to the hostilities, and around 15 per cent of Ukraine's natural gas reserves were occupied by Russian forces, reducing daily production by about 11 per cent to ~49 mcm/day.¹³⁵ One underground storage facility in the East had to cease operation due to nearby

fighting, and another was damaged, reducing available storage capacity by 0.73 bcm per year. About 200 km of gas transmission and 7,000 km of gas distribution pipelines have been damaged or destroyed. Many other gas infrastructures were damaged or had to suspend operations during this phase, such as more than 5,000 gas distribution control units. Between May and August 2022, the Russian gas transit to Europe through Ukraine decreased by approximately a third of the contracted volume due to interference by groups allied with Russia in occupied territories.¹³⁶ In the first weeks of the second phase, Ukraine was able to restart several gas infrastructure facilities, which increased gas production by about 0.5 mcm/day, after retaking some territories during the summer and autumn of 2022.¹³⁷ In November 2022, however, Russia stepped up its attacks on gas production and distribution facilities. Despite considerable repair efforts of system operators, about 600,000 households, or 5 per cent of all consumers, were without gas supply at the end of January 2023. In the same month, Moldova allowed companies to use virtual gas reverse flow, opening the possibility of importing natural gas from additional sources to Ukraine. In the third phase, regular attacks on Ukrainian gas infrastructure continued to hamper repair work and cause new damages.

In the first phase, the Ukrainian power sector suffered from deliberate, but mostly only disruptive attacks on generation capacities as well as their occupation by Russian forces. In contrast, the second and third phases were characterized by the targeted destruction of large parts of the power infrastructure. On the first day of the invasion, the Russian military occupied the Kakhovka Hydropower Plant and shut it down in September 2022. The Zaporizhzhia Nuclear Power Plant, the largest in Europe, was occupied in early March and shut down in September 2022.¹³⁸ Numerous other power plants were shelled and damaged, and several of them were occupied by September 2022. Towards the end of the first phase, around 5 per cent of the installed power generating capacity had been destroyed, 35 per cent was occupied, and more than 700,000 consumers had no access to electricity. The second phase started with extensive kinetic attacks on 11 September and 10 October 2022 against numerous power plants, high voltage lines, and substations far from the front lines. After the latter attack, an estimated 30 per cent of the Ukrainian power infrastructure was destroyed, resulting in daily short-term electricity outages for millions of people.¹³⁹ Attacks continued over the following months, with a particularly devastating strike on 15 November, compromising the electricity supply in 17 regions and forcing the transmission system operator to introduce rolling blackouts. The attack on 23 November split the Ukrainian power generation system into three separate islands and cut supply to two-thirds of all consumers.¹⁴⁰ It took ten hours to reconnect the three operating islands

Figure 2 Schematic Overview of Main Oil and Gas Transportation Infrastructure



Source data: ISW, The Oxford Institute for Energy Studies, Global Energy Monitor

and about a week for 80 per cent of affected consumers to regain access to power. By December 2022, all thermal and large hydroelectric power plants in Ukraine had either been damaged or destroyed. A month later, an estimated 50 per cent of the country's power infrastructure had been damaged, and Ukraine started to import electricity from the EU.¹⁴¹ Russia accompanied its attacks with countless attempted cyberattacks on the Ukrainian energy sector and a disinformation campaign, claiming, for example, that the rolling blackouts were a consequence of electricity exports to Europe and not the destruction of infrastructure.¹⁴² Toward the end of the second phase, Russian attacks began to lose some of their effectiveness thanks to better air defenses, continuous repair efforts, and warmer weather. Nevertheless, Russia continued its strikes against power plants, high-voltage lines, and substations unabated in the third phase. For example, a massive attack on 30 May 2023, desynchronized the Ukrainian power system, temporarily cutting off electricity to 2 million consumers.¹⁴³ A week later, Russian troops blew up the Kakhovka Dam, flooding 129 substations, two thermal power plants,

and 17 oil and gas infrastructure facilities downstream. At the time of writing, it remains to be seen whether Russia will step up its attacks on the Ukrainian energy system again in the winter of 2023/24.

4.1.3 Resilience Measures

Ukraine benefits from a remarkably robust energy system, much of it designed and built during the Cold War with World War III in mind, that helps *prevent incidents*.¹⁴⁴ The sheer size and wide geographic distribution of the energy infrastructure, as well as different transport routes, give the system a certain inherent resilience to disruptions and kinetic attacks. In addition, the infrastructure has certain redundancies, for example, in the power supply.¹⁴⁵ The national power grid of Ukraine was created after the end of the Cold War by merging several large regional grids, each with its own control centers and personnel.¹⁴⁶ As a result, the country has extra capacities and options to prevent a nationwide blackout by operating independent power islands, at least temporarily. At

the beginning of the invasion, Ukraine also had a significant surplus of power generation capacity, so the destruction of individual infrastructure elements did not immediately lead to a supply shortage.¹⁴⁷ The energy network of Ukraine is also highly interconnected with surrounding countries. This allows exports at times of overproduction, for example, in the electricity sector after the emergency synchronization with ENTSO-E in March 2022. In addition, Ukraine is an important transit country for Russian gas to Europe, which created some restraint on the Russian side to destroy respective infrastructure, at least in the early days of the invasion.¹⁴⁸ Both, export and transit continue to generate vital revenue for Ukraine. The strong interconnection also creates the possibility of imports in times of production shortfalls, improving the resilience of the power grid, for example. Ukraine's diversified energy mix reduces dependence on single energy sources and includes an increasing number of renewables, which played an important role in maintaining local power supply during the rolling blackouts in the winter of 2022/23.¹⁴⁹ Where there were strong import dependencies on Russia, Ukraine has been actively working to reduce them since the events of 2014/15, for example, in the gas sector or for the supply of nuclear fuels.¹⁵⁰ The events of 2014/15 also led to an increased focus on the issue of energy supply security at the political level in Ukraine, even before the invasion. For instance, a crisis management group was established under the Prime Minister's Office soon after to improve emergency preparedness in the gas and electricity sectors, develop contingency scenarios, and conduct stress tests.¹⁵¹ The Ministry of Energy worked closely with the power industry, developing options to keep the grid operational under different conflict scenarios. As mentioned in Section 3.1.1., Ukraine enacted a comprehensive CI law in December 2021 that includes the energy sector and provides tools and measures to prevent disruptions, such as certain obligations for CI operators.¹⁵² When the coordinated strikes on power and gas supplies began in earnest in September 2022, a coordination headquarters was established to bring together relevant ministries and the industry to prepare emergency measures and respond quickly to new destruction.¹⁵³ In addition to kinetic attacks, Ukraine has also learned from the experience of cyberattacks against energy infrastructure in the aftermath of the 2014/15 events. Two Security Operational Centers hosted by the industry, one for the electricity sector and one for the gas and oil sector, coordinate activities between the energy companies' cybersecurity teams and their counterparts on the government side.¹⁵⁴ This cooperation successfully prevented or averted most cyberattacks since the beginning of the invasion.

The measures taken by Ukraine before the invasion to ensure *adequate physical protection* of critical energy infrastructure proved insufficient, as they were in-

tended to defend against acts of sabotage and terrorist attacks at most.¹⁵⁵ The petroleum supply infrastructure of Ukraine proved particularly vulnerable in the face of the full-scale military assault due to the lack of underground storage facilities and well-protected refineries. In the power sector, substations, switching stations, and high-voltage transmission lines were also easy targets since they are above ground, unhardened, and usually not surrounded by other structures.¹⁵⁶ As a countermeasure, Ukrainian repair crews began to protect open-air transmission equipment with additional walls after the targeted attacks began.¹⁵⁷ In anticipation of another wave of kinetic attacks on energy infrastructures in the upcoming winter 2023/24, Ukraine took additional measures to harden or improve the physical protection where possible, for example with sandbags against debris and nearby detonations, metal cages against drone attacks, and concrete coffins against direct impacts.¹⁵⁸ At the outset of the invasion, the task of physical protection of CI resided with law enforcement agencies and was mainly performed by the state security police and private security services. This quickly proved insufficient, whereupon Ukraine began to strengthen the protection of CI with regular military units. Thus, it became apparent that CIP must be an integral part of defense planning by military authorities in peacetime.

Since February 2022, Ukraine has successfully implemented numerous measures to *respond to, resist, and mitigate* the consequences of incidents in the energy sector. The wartime expertise gained by thousands of energy workers since 2014/15 provided a solid foundation for these efforts and has been actively used by energy companies to optimize preparedness and train their colleagues across the country.¹⁵⁹ Industry stockpiled spare parts before the invasion to repair damaged energy infrastructure, and larger companies developed backup control centers with alternative communication channels in safer areas.¹⁶⁰ At the beginning of the invasion, they implemented pre-planned evacuation plans for their operational staff and families to these locations. All energy companies established specially trained repair crews, the number of which rapidly increased after the initial experiences in regions with intense fighting. These efforts were aided by the fact that Ukraine has a comparatively large number of engineers, due in part to the country's Soviet past.¹⁶¹ Additional personnel were brought out of retirement. Corporate crisis units closely coordinated the activities of these intervention teams with the military, law enforcement, and other government agencies. In addition, the companies helped each other out with materials, equipment, and personnel. In many cases, this joint effort and close coordination allowed for the rapid restoration of damaged infrastructure. However, Ukraine gradually ran out of spare parts, especially after Russia focused its attacks on energy infrastructure from the second phase

onward. By November 2022, more than 12,000 needed spare parts and equipment were in short supply, many with Soviet-era specifications that were hard to obtain.¹⁶² Despite the stockpiling by the energy companies, international support in supplying Ukraine with specialized equipment and spare parts became increasingly important. Since the first months of the invasion, the EU has been supplying such goods as humanitarian aid to Ukraine.¹⁶³ At the beginning of the second phase in October 2022, Ukraine requested and received further such emergency assistance via the NATO Crisis Response System and the UCPM. A dedicated coordination body, the International Energy Advisory Council, was established on 1 November 2022 for better coordination of international assistance to Ukraine.¹⁶⁴ International assistance was also central to bridging and mitigating energy supply shortfalls due to Russian attacks. When Ukraine was running low on fuel in the summer of 2022, EU Member States helped increase import capacities, for example, through truck entry permits and simplified customs clearance procedures, imports via Danube ports, or tanker slots in European ports (see Section 4.2.2). Various countries also helped with fuel or coal deliveries. Attacks on logistics were discouraged by a network of small petroleum storage facilities and direct deliveries to gas stations. When the power supply situation was particularly critical in the winter of 2022/23, imports from EU countries helped stabilize the Ukrainian grid.¹⁶⁵ Ukrainian companies importing electricity have been exempted by decree from scheduled outages until the end of April 2023 to ease the burden on domestic power generation. Demand-side measures introduced in the electricity sector included saving campaigns, consumption restrictions, and rolling blackouts. Electricity suppliers, authorities, and the media urged consumers to reduce consumption at peak times.¹⁶⁶ A government program allowed every Ukrainian citizen to replace five standard light bulbs with five LED light bulbs for free.¹⁶⁷ Outdoor advertising and streetlights were switched off, working from home and the purchase of generators were promoted, and trolleybuses and trams were replaced with buses with combustion engines. After rolling blackouts eventually had to be introduced, consumers could consult publicly available schedules from their local energy company to see when they would have power at home.¹⁶⁸ Companies curtailed production, adjusted operating hours accordingly, and, where possible, used alternative energy sources during hours without power. Generators and batteries play a crucial role in ensuring vital services for the Ukrainian population when the power supply fails. By the end of December 2022, nearly 1,500 bank branches and numerous gas stations across the country were equipped with a generator and could provide services during a power outage.¹⁶⁹ The telecommunications sector equipped some 5,000 mobile base stations with generators and replaced old lead bat-

teries in more than 22,000 other stations with new high-performance batteries that provide emergency power for at least three days.¹⁷⁰ A decree suspended tariffs and VAT for generators and other components until May 2023, and the volume of fuel that can be stored without a special permit was raised to 2,000 liters. In many cities, local authorities offered subsidies to residents to purchase generators that reduced the list price by up to 75 per cent. Other alternative energy sources are also examined or are already in use. For example, the acquisition of mobile gas-fired power stations with capacities of 30–50 MW each is planned for the emergency supply of CI. Renewable energy sources such as solar and wind power are used as backup power for distribution, pumping, or compressor stations in the gas sector, especially in remote locations.¹⁷¹ As a further means, the Ukrainian authorities had set up so-called Points of Invincibility throughout the country since November 2022.¹⁷² These are mobile or stationary rooms for up to 500 people, equipped with a generator and offering basic services such as electricity, mobile communications and internet, heat, and water free of charge around the clock. By the end of 2022, 11,500 such points had been set up.

As Russia's invasion of Ukraine is still ongoing, the country is currently not in a position to *recover from incidents* in the energy sector in the long term. For short-term recovery, such as repairs, restorations, etc., Ukraine depends on international support. In addition to assistance on a bilateral basis and through established mechanisms such as the UCPM, at least two other dedicated initiatives have been set up, namely, the International Energy Advisory Council mentioned above and the Ukraine Support Task Force. The latter was established by the Energy Community, a regional organization focused on Eastern Europe and the Black Sea, to coordinate the delivery of specialized energy equipment donated to Ukraine by private companies.¹⁷³

Short-term recovery in Ukraine does not strictly mean rebuilding the same facilities but focuses on restoring energy supply. This may involve switching to infrastructure that can run on alternative or even multiple energy sources, such as installing new boilers fueled by biomass or electricity in addition to natural gas.¹⁷⁴ Another measure to increase resilience in the energy sector is decentralization, moving away from centralized large Soviet-era infrastructures to many small ones. In the heating sector, for example, large systems linked to large combined heat and power plants are being replaced by several smaller, geographically distributed boilers or individual heating systems in buildings. In the area of power generation, a longer-term goal is to build local, small-scale microgrids and capacities that integrate standalone or combined renewable and storage technologies and help strengthen the resilience of the overall power supply system.¹⁷⁵

Thanks to a solid foundation, utmost commitment, adaptability, and resourcefulness of all stakeholders, as well as international support, Ukraine has so far managed to stabilize the country's energy supply at a lower level. In the process, the energy system withstood impacts for which it was never designed. This is an unprecedented feat, given the Russian attack with all available means. However, it remains to be seen for how much longer this will be possible, especially should international support begin to wane.

4.2 Transportation

4.2.1 Defining the Sector

The FOCP groups railways, water transportation, air transportation, and roads into the CI section of transportation.¹⁷⁶ In Switzerland, the road infrastructure includes motorways (national, cantonal, main, and secondary roads), tunnels and bridges. Water transportation comprises land-based infrastructure such as ports to handle shipments, inland waterway navigation referring to lakes and river networks such as the Rhine, and navigation on the high seas. Air transportation includes passenger and freight transport by air, distinguishing between civil, commercial, private, and military air traffic. In addition, this sub-sector is also concerned with ground-based infrastructure such as airports and air traffic management and control. Lastly, the rail transportation sector includes passenger and freight transport on the rail network. As with the energy sector, the current Swiss National Strategy for Critical Infrastructure Protection acknowledges the elevated criticality of the transportation sector, as it is strongly interconnected with other CI sectors, such as energy and communication. In the case of Ukraine, for example, half of the railway system is electrified and depends on a consistent energy supply. Similarly, road vehicles rely on a steady supply of fuel. Furthermore, a functioning and efficient transport and traffic system is seen as a fundamental prerequisite for a modern economy that depends on the mobility of goods and people.¹⁷⁷ The EU shares the same understanding of the transportation sector and strongly emphasizes service providers (i.e., the entities) and their assets to ensure the services.¹⁷⁸ In NATO's understanding, the 2023 Final Assessment Report of the EU-NATO Task Force on the Resilience of Critical Infrastructure points out that while diverse routing options can tackle limited redundancies in the transportation systems, certain pivotal nodes (e.g., major airports, primary railway hubs, etc.) remain irreplaceable, especially in defense aspects. Nevertheless, the resilience of the logisti-

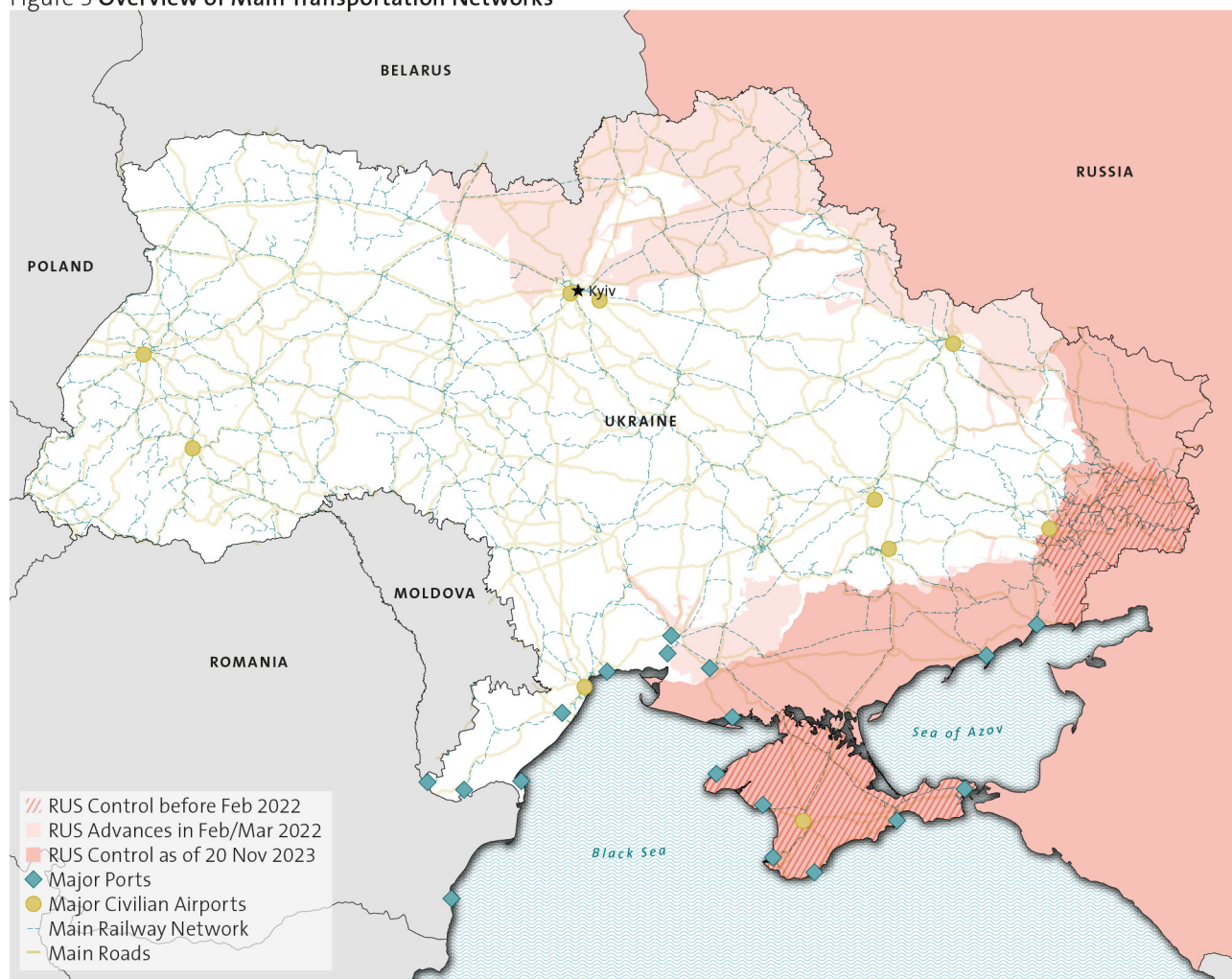
Further Reading

Romina Bandura / Janina Staguhn / Benjamin Jensen, **"Modernizing Ukraine's Transport and Logistics Infrastructure,"** *Center for Strategic & International Studies*, 2022.

Mari Eccles, **"Prepare for takeoff...soon: Kyiv airport readies for post-war flights,"** *POLITICO*, 18.10.2023.

Sarah Topol, **"Ukraine's 15,000-Mile Lifeline,"** *The New York Times Magazine*, 07.11.2023

Figure 3 Overview of Main Transportation Networks



Source data: ISW, Geofabrik, OpenStreetMap contributors

cal network depends not solely on its central nodes, but also on a system that is equipped with diverse routes and can accommodate civil and commercial transportation even in times of crisis.¹⁷⁹ In line with the European understanding of the importance of transportation, the Ukrainian Cabinet of Ministers enacted Resolution Nr. 1109 in 2020, defining Transportation and Postal Services, specifically air, roads, railways, sea and river ways, and postal services as a critical sector, which later found its way into the country's CIP legislation.¹⁸⁰

4.2.2 Baseline and Developments since the Beginning of the Invasion

Transportation is one of the key sectors of the Ukrainian economy.¹⁸¹ The transport infrastructure includes a widespread railway network, a rather outdated road system, sea and river ports, airports and an extensive air service, including freight and customs terminals. Together with warehousing, postal and courier services, the transport sector accounted for 6.5 per cent of the country's GDP in

2021.¹⁸² The Ministry of Infrastructure has been entrusted as the primary authority overseeing the protection and enhancement of this infrastructure. Furthermore, as outlined in Article 53 of the Presidential Decree Nr. 392/2020, ambitions to modernize the transport infrastructure – including via public-private collaborations and transparent privatization – have been marked as pivotal strategies to enhance the country's national security.¹⁸³

First, Ukraine has one of Europe's most extensive railway networks, with a length of over 20,952 km almost half of which is electrified.¹⁸⁴ Its gauge width of 1.520 mm is a longstanding challenge as it is incompatible with the gauge width of 1435 mm used in most EU countries.¹⁸⁵ The pre-war capacity of border crossings by rail was about 80 million tons per year, which was only 50 per cent of what it could be due to inefficiencies created by transferring goods to European standard railcars.¹⁸⁶ A network of almost 1,500 railway stations exists in Ukraine, overseen and managed by the state-owned company Ukrzaliznytsia.¹⁸⁷ This enterprise is organized as a single monopolistic company, controlling railway infra-

structure and services and providing 82 per cent of freight and 50 per cent of passenger transport across all transportation modes in Ukraine.¹⁸⁸ The railways density in Ukraine, at 496.27 km per million inhabitants, exceeds the European average of 429.97 km per million inhabitants and connects major cities and border crossings with neighboring countries. Ukrzaliznytsia's transportation capacities before the war were used primarily to transport metal, coal, iron ore, construction materials, and passengers. With 266,000 employees, Ukrzaliznytsia is Ukraine's largest employer.¹⁸⁹ The organization is still deeply rooted in its Soviet heritage, providing fixed salaries and additional benefits that range from medical facilities to educational institutions for its staff.¹⁹⁰

Second, Ukraine also features extensive infrastructure for water transportation. Out of the 18 Ukrainian seaports, 13 are located on the continental territory of Ukraine along the shores of the Black Sea, the Sea of Azov, and the Danube River. All ports are state-owned and fall under the Ukrainian Sea Ports Authority (USPA) jurisdiction. Established in 2013, USPA processed more than half of the country's exports before the war and handled 90 per cent of Ukrainian grain and oilseeds exports. These exports are of crucial importance for the country's economy.¹⁹¹ The remaining five ports of Kerch, Yalta, Sevastopol, Feodosia, and Yevpatoria are located in the territory of Crimea, which has been occupied by Russia since 2014.¹⁹² Ukraine has several navigable rivers, including the Danube, the Dnipro, the Southern Bug, and the Dniester, with a total of 10 river ports that are state or privately owned.¹⁹³ Of these rivers, the Danube is the most used for shipping. It connects Ukraine by sea with nine European countries, including the port of Constanta in Romania. Ukraine's state-owned Danube ports Izmil, Reni, and Ust-Danube are located on the lower part of the river, which forms a border with Romania before it flows into the Black Sea. Before the invasion, these ports handled up to 4 per cent of Ukrainian exports, equivalent to approximately six million tons of cargo under the administration of USAP.¹⁹⁴

Third, air transport comprises the transportation of passengers and cargo by aircraft. Before the invasion, the Ukrainian air transport sector comprised 19 airfields for civilian purposes, 21 passenger airlines, and 19 airlines carrying mail and cargo. Governed by the Ministry of Infrastructure (state policy on infrastructure) and the State Aviation Administration of Ukraine (i.e., authority for civil aviation), this industry served 16.2 million passengers in 2021.¹⁹⁵ Ukraine inherited a substantial aircraft manufacturing industry from its past as part of the USSR, exemplified by the Antonov Company, a prominent Ukrainian aircraft and manufacturing company.¹⁹⁶ An approximation to the EU air transportation market and liberalization has occurred in recent years, attracting investments.¹⁹⁷ However, the events in 2014/15 resulted in the loss of

control over what were then two of Ukraine's busiest airports, Simferopol and Donetsk. While Simferopol airport continued to operate under the occupation administration, Donetsk airport's facilities were heavily damaged in the intense fighting of 2014 and 2015, rendering it inoperable.¹⁹⁸

Lastly, Ukraine has a network of public roads spanning over 169,000 kilometers, including national, regional, and communal roads.¹⁹⁹ In terms of durability (39.2 per cent lacking adequate strength) and surface evenness (51.1 per cent affected), up to 90 per cent of general-purpose roads have not been repaired in the last 30 years.²⁰⁰ Consequently, a considerable portion of the infrastructure does not meet the standards of modern-day roads.²⁰¹ In 2021, 41 per cent of cargo (in tons) and 20 per cent of volume (in tons-kilometers) was transported by road, a large proportion of which is accounted for by so-called last mile-cargo that is transported over relatively short distances. Lorries are frequently used to deliver agricultural products to ports and to import high-value products (electronics, appliances, apparel, etc.) from the EU.²⁰²

As of 2023, there are about 28,500 road and railway bridges in Ukraine. The average age of many road bridges exceeds 60 years, and more than 30 per cent are deemed to be in a critical condition.²⁰³

When the invasion by Russia began in February 2022, the transportation infrastructure was affected across all sectors. The first infrastructures to be hit by missile attacks were airports and airfields. Consequently, authorities swiftly closed the civilian airspace of Ukraine.²⁰⁴ By June 2023, 19 out of 35 airfields were damaged, including 12 civilian and seven dual-purpose airfields (excluding military airfields). In addition to the complete shutdown of the aviation industry, four of the 13 ports, namely Berdyansk, Mariupol, Skadovsk and Kherston, were captured by Russia by October 2022 and operations were suspended, while access to the remaining main ports was blocked. This has a major impact on Ukrainian exports, as more than half of them are shipped by water.²⁰⁵ Ukraine was forced to adapt its agricultural export systems quickly. Instead of shipping agricultural goods via the now damaged, blocked or captured ports, a mix of rail, road, and river routes allows for at least a portion of the goods to be shipped through neighboring countries to the west.²⁰⁶ Coping with these supply chain interruptions was crucial for the country's economy and industrial functioning, since the storage capacities of farmers are exhausted and income losses are accumulating. This was similarly important for the global food supply. The operation of the Danube ports Reni and Izmil was once again hampered in the summer of 2023 by the seasonal shallowing of the Danube and Russian shelling of the port infrastructure.²⁰⁷ The rail and road infrastructures were not targeted in the first two weeks of the inva-

sion, as Russia considered them essential for its plans to occupy the country. Damage nevertheless occurred in the form of collateral damage from the ongoing fighting or if it was deemed beneficial for tactical reasons.²⁰⁸ Over time, however, the Ukrainian railway system faced increasing difficulties as Russia targeted substations, fuel reserves, and railway assets, such as the simultaneous attack on five railway stations in western Ukraine in April 2022.²⁰⁹ By June 2023, over 500 km of railway tracks, more than 53 railway stations and around 9,500 buildings and other structures relevant to operations had been damaged by the war in the areas controlled by Ukraine.²¹⁰ As many ports are blocked, Ukraine is increasingly using the rail network for exports, despite the inherent inefficiencies of this process due to the different track gauges.²¹¹ In this situation, road transportation has become an important substitute for many export and import activities. For the road sub-sector, however, a less detailed damage assessment could be carried out as part of this report. It is estimated that by Summer 2023, 25,400 km of roads and 344 bridges were damaged.²¹² At the same time, as part of its defense strategy, Ukraine targeted road infrastructure along key highways to prevent Russian forces from advancing.²¹³

KSE estimates the direct damages of transport infrastructure at 36.6 billion USD by June 2023 and a further 23.2 billion USD in indirect damage.²¹⁴ While the number of reported damages to air and water transportation infrastructure is more or less consistent, estimates of damages to rail and road infrastructure vary depending on the period and the report. The reason for this could lie in the assessment methods and used calculations, as well as the assumptions made on infrastructure in occupied territories and the ongoing maintenance and rebuilding.

4.2.3 Resilience Measures

As in the energy sector, the *prevention of incidents*, as well as ensuring adequate physical *protection* depends to a large extent on Ukraine's defense capabilities and ability to maintain control of CI elements such as transportation nodes.²¹⁵ However, certain factors give the Ukrainian transportation system an advantage in coping with the distress. For example, the extensive Ukrainian railway network allowed for flexible transportation of goods and people, enabling swift rerouting of trains in the event of attacks.²¹⁶ As only half of the rail network is electrified, diesel-powered trains continued operations on de-energized sections if substations were compromised.²¹⁷

In the air transportation sector, swift actions were taken in anticipation of the invasion by strategically relocating aircraft to safer locations. In some cases, operators also blocked runways, deactivated navigation systems, and drained fuel reserves.²¹⁸ Even though civil air traffic has shut down, service operators have implement-

ed measures to *accommodate* a smoother transition once operations can resume. For example, the airport Kyiv-Boryspil focuses during this phase of the war on staff retention. Ukraine's largest airport has committed to paying its employees two thirds of their regular salaries to prevent the loss of trained personnel. Although this approach ensures a certain degree of skilled staff, it imposes a considerable financial burden on the airport, translating to an expenditure of approximately 3.2 million EUR monthly.²¹⁹ While civil air transportation was factually incapacitated, seaports found measures to *mitigate* the impact on their services. As the Ukrainian seaports and routes in the Black Sea are virtually inoperable, a diversification in service provision to the river network and its peripheral infrastructure, the Danube ports, has been observed, although this is not considered a long-term solution. Especially the river ports of Izmail and Reni are productive, while Ust-Danube is lagging due to inadequate infrastructure, lack of necessary water depths, and missing railway connectivity from the main Ukrainian hubs.²²⁰ Today, these Danube ports have become a crucial economic link to Europe, shipping nearly one third of the country's agricultural exports and iron and steel. This diversification strategy has preserved revenue streams and avoided dependence on a single mode of transport for exports. However, it has also created competition for limited capacities, including for the necessary land connections to rail or road infrastructure, requiring more operational flexibility and capacity from the critical entities. One example is the relocation of pilots from Black seaports to the Danube ports.²²¹ The latter is being done even though the EU-NATO Task Force on the Resilience of Critical Infrastructure concluded that disruptions at these major seaports could have significant consequences.²²² This is mainly because there are limited alternatives available to compensate for the impeded flow of bulk goods, which can impact both civilian and military domains. However, the resilience of a logistics network is not solely reliant on its central nodes. Even if these nodes become non-operational, a system equipped with diverse routes can still function. To overcome this challenge, Ukraine utilized its peripheral infrastructure such as the Danube ports, transforming it into a significant export route. Several projects were initiated to improve the capacities of these river ports, including deepening the riverbed, constructing warehouse complexes, and expanding the Bystroe estuary.²²³ Furthermore, there are plans to privatize the port of Ust-Danube through a public sale, in line with the vision of the government to improve infrastructure through private collaboration.²²⁴ A further relaxation of the difficult situation in the export economy for agricultural goods was achieved in July 2022 through the Black Sea Grain Initiative, an agreement between Ukraine and Russia facilitated by Türkiye and the UN.²²⁵ It allowed the commercial export of food and fertilizers from the key Ukrainian ports of Odesa, Chornomorsk, and Yuzhny/Piv-

dennyi in the Black Sea. Up to 400 ships were able to leave these ports until October 2022.²²⁶ Following the suspension of the agreement by Russia in July 2023, Ukraine established a humanitarian corridor along the Romanian and Bulgarian coasts, allowing around 700,000 tons of grain to be exported in August 2023.²²⁷

The most notable observations regarding *responding to, resisting, and mitigating* the consequences of incidents come from the rail sector. With the airspace closed and the port infrastructure being utilized for exports, the railway system and its operating company Ukrzaliznytsia became Ukraine's lifeline. The company reacted quickly to the unfolding situation and bolstered the resilience of the railway system and the transportation sector as a whole. It facilitated the transportation of people from East to West and offered free-of-charge tickets to evacuees.²²⁸ The supply of humanitarian goods and military logistics was facilitated, while operational guidelines were adjusted so that trains ran more slowly to minimize the extent of possible damage.²²⁹ The historical organizational division of Ukrzaliznytsia into six independent regions proved to be beneficial, as this organizational structure and regional independence enabled a relatively simple transition from regular operation to crisis mode. The operation of passenger trains, the provision of humanitarian aid, and the rapid repair of destroyed or disrupted infrastructure, whenever and wherever required, demonstrated the high degree of modularity.²³⁰ Another crucial factor for the resilience of the railway lies in Ukrzaliznytsia's surplus of personnel, especially the surplus of engineers, machinists, and technical specialists who were already familiar with the internal structure and operations of the organization and could seamlessly transition into a range of roles, for example from repair work to regular maintenance. Although this overstaffing was criticized before the war, it enabled the company to repair and maintain damaged infrastructure promptly. Between January and August 2023, the company carried out extensive restoration work on the railway, renewing 854 km of tracks, an increase of 22 per cent compared to the same period in 2022, and re-establishing connectivity in recaptures territories.²³¹ Volunteers, many of whom with ties to Ukrzaliznytsia, provided additional support for this performance.²³² Intensive chains of communication were established at the operational level, using a Soviet-era closed-circuit system called Selector for leadership to communicate with its managers in the field, ensuring the flow of critical information in real-time and enabling decision-making.²³³ Ukrzaliznytsia has constantly moved its top management and operational hubs, at times even in a high-speed diesel train, to reduce their exposure.²³⁴ Moreover, the company harbors its own procurement services, e.g., laundry services, glass factory, and steel-rail manufacturing units.²³⁵ This capability permitted the company to produce spare parts, whilst reducing costs and depen-

dency on external suppliers.²³⁶ In accordance with the country's overall push to digitalize services, Ukrzaliznytsia also sees this as a step towards modernizing and optimizing its services. For example, an app has been introduced that offers an interactive digital map to guide citizens in train evacuations and points them to available shelters by collecting evacuation data.²³⁷ Overall, Ukrzaliznytsia maintained high efficiency, shown by its punctuality rate of 97 per cent for long-distance domestic trains as of 15 January 2023. Nevertheless, external and international aid has been crucial to boost railway operations. For example, with the support of the Red Cross Society's donation of generators, train stations were kept in operation.²³⁸ While responding to Ukrainian requests for spare parts for the railway system, investments were pledged, and various agreements were reached to support this transportation sub-sector. A significant step was the provision of a 50 million EUR loan to Ukrzaliznytsia by the European Bank for Reconstruction and Development (EBRD). This infusion of funds was instrumental in providing liquidity to ensure the seamless operation of the expansive Ukrainian rail network.²³⁹ On a bigger scale, Solidarity Lanes connecting the EU to Ukraine were created through international initiatives. Given the blocked seaports, the European Commission and EU Member States established essential corridors and alternative logistics routes using all modes of transport to facilitate the export of Ukrainian grain and other agricultural products, as well as the import of critical goods such as humanitarian aid, animal feed, and fertilizers.²⁴⁰

When it comes to bridges, an overlap exists between railways and public roads. Therefore, a commission tasked with assessing the condition of bridge structures was established to evaluate the transport and operational state of public road and railway bridges, with particular emphasis on larger, more complex structures subject to heavy traffic.²⁴¹ Moreover, emergency repair crews were dispatched to quickly mitigate damages and minimize disruptions, while alternative routes or detours to circumvent affected areas were implemented to ensure consistent traffic circulation. This included solutions, such as metal bridges provided by the Czech Republic and France to re-establish key transportation links promptly.²⁴²

Although ongoing repair and maintenance work is underway across all transportation sub-sectors, full *recovery* is difficult during an ongoing war. Genuine recovery efforts will require substantial investments. Nonetheless, initial efforts are made to begin the *recovery* process and prepare for the moment the situation allows for returning to normal operations. In the air transportation sector, the Ukrainian government intends to restore five airports to reach the pre-war passenger volume of 16.2 million passengers in 2021, as per official reports.²⁴³ Therefore, agreements are already negotiated to support the transition, for example, the EU's proposition to lower

the minimum airport slot usage rate for airlines coming to Ukraine during the first 16 weeks after services resume.²⁴⁴ For railway transportation, Prime Minister Denys Shmyhal announced that Ukraine would begin phased construction of railway tracks to European standards (1435 mm gauge), starting in the country's west.²⁴⁵ The primary concern of the government concerning roads is restoring infrastructure to facilitate heavy vehicular traffic, especially lorries.²⁴⁶

International cooperation and assistance are crucial for Ukrainian efforts towards *recovery*. In this regard, the Minister of Finance of Ukraine has recently signed an agreement with the EBRD to enhance the efficiency of transportation channels and improve transport accessibility across the region. The aim of such collaborations is to streamline logistics and thereby reduce the costs associated with transportation between Ukraine and the EU.²⁴⁷

The overall resilience performance of the transportation sector, and most notably of the railway sector, lies in what Kharrazi et al. define as key features of network resilience, namely diversity (e.g., using different modes of transporting people), modularity (e.g., railway regions independent of each other), and redundancy (e.g., diesel-powered trains to substitute electrified ones).²⁴⁸ In addition, the situation in Ukraine demonstrates the importance of having diversified logistical options. Although circumstances and challenges differ, the themes of resilience, flexibility, and the ability to leverage peripheral infrastructures are essential.

4.3 Information and Communication

4.3.1 Defining the Sector

The FOCP incorporates telecommunications, information technology (IT) services, the media, and postal services within the information and communication (IC) sector. First, it is specified that telecommunication refers to all the means necessary to electronically, magnetically, optically, or electromagnetically transmit information via fixed, mobile, wireless, or satellite infrastructure. This includes the internet, 5G connectivity, and telecommunication providers. Second, IT services are concerned with processing and storing data and information, ranging from software to hardware necessary in communications, business, and industry technology. Third, and strongly dependent on telecommunication to broadcast information is the media as an apparatus of mass communication that enables citizens to receive information and, therefore, supports decision-making in a democratic manner (e.g., media outlets, government announcements, or early warnings).²⁴⁹ Furthermore, the updated Swiss National Strategy for Critical Infrastructure Protection from 2023 recognizes the centrality of telecommunications as almost all CI operations depend on functioning telecommunication networks.²⁵⁰ The EU covers information and communication in the rather broad definition of digital infrastructure (and business-to-business ICT services), including internet providers and services, cloud computing and data centers, content delivery networks, and public electronic communication providers and services.²⁵¹ This is consistent with the sectoral analysis of the EU-NATO Task Force on the Resilience of Critical Infrastructure's final assessment report proclaiming digital infrastructure as the foundation of today's communications.²⁵² In addition, at the 2016 Warsaw Summit, NATO members defined one of their baseline resilience requirements as: "Resilient civil communications systems: ensur-

Further Reading

Nino Kubinidze et al., "Interim assessment on damages to telecommunication infrastructure and resilience of the ICT ecosystem in Ukraine," *International Telecommunication Union*, December 2022

Emma Schroeder / Sean Dack, "A parallel terrain: Public-private defense of the Ukrainian information environment," *Atlantic Council*, 2023.

Vera Bergengruen, "The Battle for Control Over Ukraine's Internet," *Time*, 18.10.2022.

ing that telecommunications and cyber networks can function even under crisis conditions, with sufficient back-up capacity. This also includes the need for reliable communications systems including 5G, robust options to restore these systems, priority access to national authorities in times of crisis, and the thorough assessments of all risks to communications systems.”²⁵³ In the case of Ukraine, the 2021 law on CI defines two areas that overlap with the previous categorizations: information services and electronic communications.²⁵⁴

As more recent definitions illustrate, cyber or digital infrastructure is the term, concept, and domain that replaces or at least complements the conventional information and telecommunication sphere. The previous definitions are still relevant because they enable the cyberspace and are technically and virtually present in almost every other CI, facilitating modern-day operations. Next to cyber and digital infrastructure, the information domain is another topic increasingly interlaced within this sphere. The efforts within this domain can include protecting information, securing information, and countering fake news.

It is generally understood that Russian cyber operations have thus far not generated the decisive impact some analysts expected, while Ukrainian cyber defense keeps up its guard.²⁵⁵ Several publications and reports document Ukraine’s cybersecurity impact, efforts, and resilience, which is omitted from this report (i.e., the technicalities of cyber- and information resilience).²⁵⁶ Instead, the following case study will focus on the resilience of the IC sector, i.e., highlighting efforts that ensure the service of telecommunications, IT services, and the media.

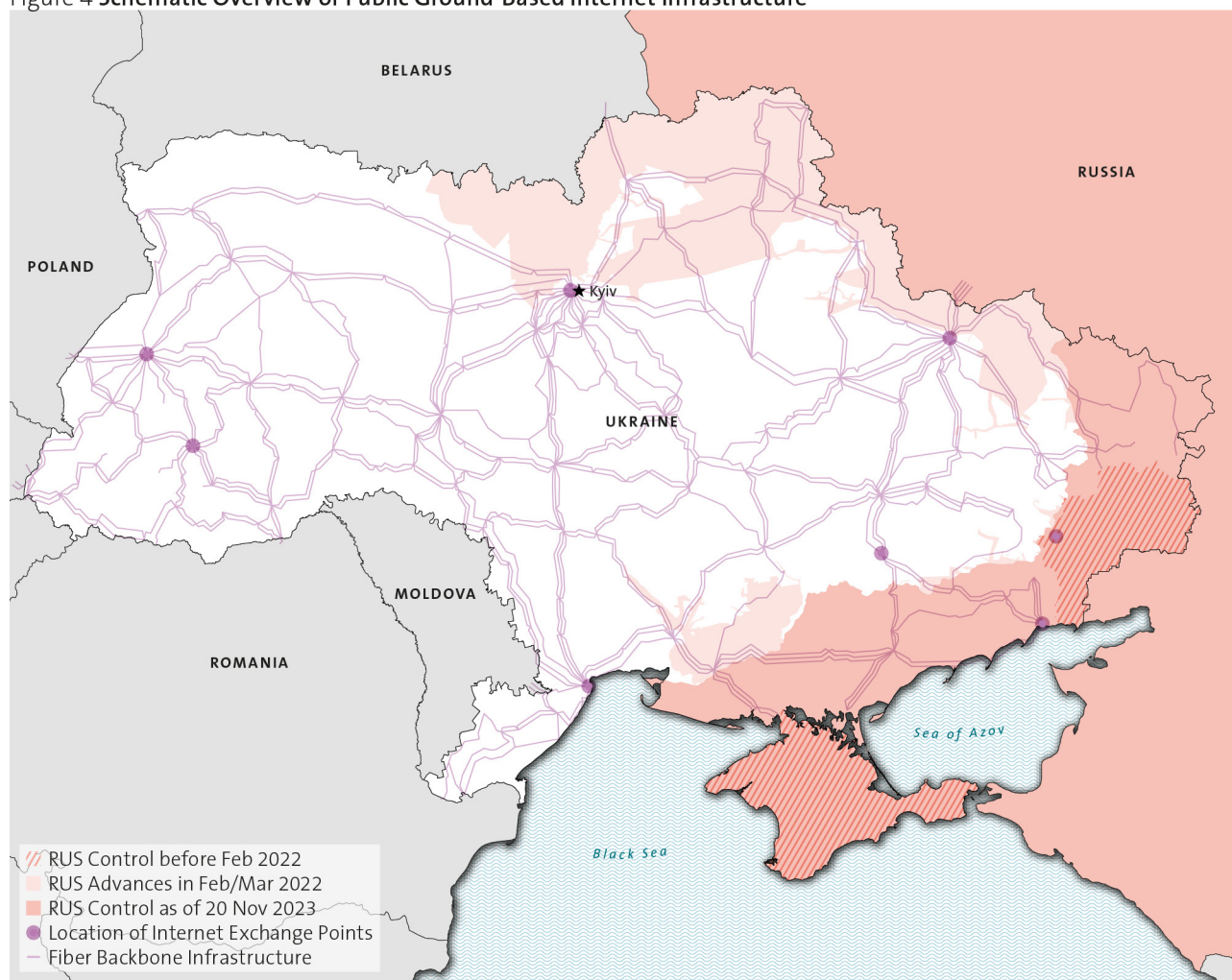
4.3.2 Baseline and Developments since the Beginning of the Invasion

Before the full-scale invasion, Ukraine possessed an increasingly developed telecommunication sector, a thriving IT industry, and a diverse media landscape. In certain instances with some gaps to European standards, such as internet coverage. The mobile and wireless market was and is dominated by a few large operators, i.e., Kyivstar, Vodafone Ukraine, and Lifecell, which claim over 95 per cent of the market share and provided a 91.6 per cent coverage of the population by at least 3G in 2021.²⁵⁷ The fixed broadband market is composed of two domains and provided 79.2 per cent of households access to the internet in 2020.²⁵⁸ First, the fixed internet service providers (ISP) consist of a few big players that claim roughly half of the market, while thousands of local and regional end-user network providers make up the rest of the market. This fragmentation stems from the historical roots of the early Soviet-era internet. Second, the network transportation infrastructure, such as fiber optic cables or internet exchange points, is concentrated on a few operators that

provide the backbone of the internet and serve mobile operators and TV channels for signal transmission (e.g., connecting different base stations or cell towers via fiber to enhance transmission speed and volume).²⁵⁹ The IT industry, making up 3.5 per cent of Ukraine’s GDP and accounting for over a third of service exports in 2021, counts over 2,000 companies (product- and service-oriented) and employs roughly 290,000 people.²⁶⁰ This IT ecosystem is not just one of the main export pillars, but also an enabler for Ukraine’s ambitious digitalization and e-governance efforts that have gained traction in recent years, e.g., with the continuous development of the e-governance application Diia.²⁶¹ The Ukrainian media environment was characterized by a greater diversity compared to other former Soviet nations. However, it has also been subject to political influence, including the presence of pro-Russian media outlets. Television is one of the most popular media platforms and the most popular TV channels are owned by a few magnates.²⁶²

Incidents against IC infrastructure had already occurred before the invasion, e.g., cyberattacks against Kyivstar’s mobile base stations. However, the advancing Russian forces and preceding air strikes deliberately targeted IC infrastructures with kinetic attacks.²⁶³ The reasons to attack IC in armed conflicts are diverse. First, modern military forces need IC. Interrupting the IC capabilities of a military, which often depend to a certain degree on public or private service providers, can disrupt or complicate Communication, Coordination, and Command & Control (4Cs) or the functioning of equipment.²⁶⁴ In addition, many processes of civil protection also depend on a functioning IC infrastructure. For example, multi-hazard early warning systems, such as Air Alarm or Kyiv Digital, incorporated military threats.²⁶⁵ Second, telecommunication and IC infrastructure are at the heart of other CI sectors like energy and transportation. They serve not only households and businesses, but also other CI services and government functions. Therefore, targeting IC infrastructure can be a means to disrupt other CI sectors or create cascading effects across the overall CI system. Third, cyberattacks occur through, within, or on IC infrastructure as they are an essential component of the cyber domain, e.g., networks or transmission installations. Consequently, any modern-day military operation also acts within the electromagnetic, cyber, and information domains, making IC a viable target. For example, at the beginning of the full-scale invasions, Russian hackers targeted Viasat’s KA-SAT satellite modems, leaving thousands of Ukrainians temporarily without broadband internet access. Similarly, the massive cyberattacks that targeted Ukrtelecom, a major Ukrainian telecommunication network provider, reduced connectivity by 13 per cent for 15 hours.²⁶⁶ While the Ukrainian cyberspace has proven relatively resilient, kinetic actions against ground-based physical infrastructure caused far-reaching damages. The World Bank esti-

Figure 4 Schematic Overview of Public Ground-Based Internet Infrastructure



Source data: [ISW](#), [ITU](#), [TeleGeography](#)

mated overall damages to IC infrastructure at 1.6 billion USD (including postal services) by the end of February 2023 and losses of the telecommunication sector at 1.55 billion USD.²⁶⁷ It is assumed that Russia has seized or completely destroyed Ukrainian IC infrastructure, such as TV and radio stations, mobile base stations, and fiber cables, in occupied territories. In the summer of 2022, roughly 20 per cent of mobile communication was suspended, leading to a significant decline in mobile coverage, while a simultaneous shift from fixed to mobile internet was recorded.²⁶⁸ In January 2023, an average of 25 per cent of mobile bases are considered to be disrupted, with a temporary maximum of 59 per cent of them out of service in November 2022.²⁶⁹ Furthermore, Ukraine's Special Communications Service estimated that over 60,000 kilometers of fiber cables have been destroyed or seized by the invaders.²⁷⁰ With the seizing of mobile and fixed communication infrastructure, Russia re-routed internet traffic through Russian internet exchange points and was able to block, restrict, or channel internet traffic and Ukrainian radio frequencies in the occupied territories.²⁷¹

Overall internet connectivity in Ukraine is estimated to have deteriorated by at least 16 per cent by October 2022, resulting in a total of over 19,000 hours of internet disruptions measured by the downtime and inaccessibility of IP addresses, while in occupied regions more than half of the IP addresses are no longer accessible.²⁷² Data centers which store government data have become valuable targets that require increased protection.²⁷³ The war has also impacted the IT industry, forcing over 70 per cent of IT companies to fully (17.5 per cent) or partially (53.3 per cent) relocate business within Ukraine or abroad. IT companies are further challenged by travel bans, migration activities, or possible conscription of employees.²⁷⁴ Equally devastating have been the impacts on media infrastructure in contested areas. On 1 March 2022, Kyiv's television tower got hit by two missiles, following Russian warnings to prevent the spread of misinformation. Within the first month of the invasion, at least 32 television channels, multiple radio stations, and several broadcasting antennas experienced similar attacks.²⁷⁵

Overall, Ukraine's IC sector can be considered resilient, as demonstrated by the facts that access to the internet and digital services remains relatively high in the post-2022 period, the continuous stability of internet exchange points, and the increase in connectivity. However, the sector was significantly affected by cascading effects of the attacks on energy infrastructure and the resulting outages.²⁷⁶

4.3.3 Resilience Measures

The Interim Assessment of the International Telecommunication Union (ITU) from December 2022 and the country profile 2022 provide a broad account of resilience and sustainability measures of the Ukrainian telecommunication and IT sectors.²⁷⁷ In addition, a holistic analysis of the digital ecosystem by Itzhak and Fer and a report on the information environment by the Atlantic Council's Digital Forensic Research Lab (DRFLab) have begun to report on resilience in the broader IC sector.²⁷⁸ The IT Ukraine Association offers insights for the country's IT industry, which has been the only industry able to increase its export volume in 2022 compared to 2021.²⁷⁹

Ukrainian IC resilience can be attributed to some inherent characteristics of the systems. As with energy and transportation, some IC systems were already designed to withstand a certain degree of stress. One example is the way the internet's end-user networks are structured, as the early Soviet approach led to a diversified shelf of internet providers on local and regional levels. Therefore, if one network is disrupted, the effect is limited.²⁸⁰ The hardening of the more extensive information infrastructure gained attention since the events of 2014, for example, due to the Cyber Security Strategy 2016 that got amended continuously to incorporate ongoing changes in the security landscape.²⁸¹ These observations have led IC operators to prepare specifically for an armed conflict.²⁸²

Concerning *preventing incidents* and ensuring *adequate physical protection*, the military plays an essential role by deploying its defense capabilities, such as air defense.²⁸³ Nevertheless, operators, such as Ukraine's third-largest mobile service provider Lifecell, have taken additional steps to reduce the likelihood of an incident about two months before the invasion by starting to organize its responsibilities in a state of war, increasing its cyber defense posture, and engaging in a close exchange of information with government and security organizations.²⁸⁴ To reduce exposure of Lifecell's operations, the company faced the difficult task of relocating offices and assets from its eastern locations to the country's West, and setting up network redundancies while maintaining services.²⁸⁵ In some instances, IC operators have proactively destroyed internet infrastructure, such as software of internet service providers, before it could be misused

or reconnected by the invading Russian forces.²⁸⁶ A change in data protection regulation allowed the government to store and process data in clouds provided by various tech companies such as Microsoft or Amazon, often offered as free humanitarian assistance.²⁸⁷ This increased government data protection against cyber and physical attacks on telecommunication and information infrastructure, such as data centers and servers, as many servers were located outside Ukraine.²⁸⁸ This step shows that international collaborations between different actors is necessary in the cyber and IC domains, or can at least strengthen digital resilience and increase the robustness.²⁸⁹

The invasion, however, made it necessary to *respond to, resist, and mitigate* the consequences of incidents within the IC domain. In 2004, the Ukrainian government defined contingency plans for the operational and technical management of telecommunications in case of emergency or under martial law. The procedure foresees the creation of the National Telecommunication Networks Operation Center to deal with communication challenges in crises or emergencies.²⁹⁰ However, given the immense stress on connectivity caused by the invasion, the Ukrainian Minister for Digital Transformation promptly approached SpaceX for its Starlink service to support and bolster the communication capabilities of the country. The call was answered swiftly, and the low-orbit satellite-based broadband internet provider shipped the first batch of Starlink terminals to Ukraine as a donation. The terminals that were delivered later were then paid for by allied governments or organizations.²⁹¹ Although satellite-based internet does not have the same capacity in terms of speed and volume as fiber-optic cables, it allows to bridge periods of connection loss or power outages. Starlink also serves as a temporary solution in liberated territories until the main IC infrastructure is repaired.²⁹² Although most communication takes place via modern infrastructure, older but reliable communication systems have also proved useful in some cases and sectors. One example is the closed communication system of the railway provider Ukrzaliznytsia mentioned in the previous chapter. The company's ex-Soviet high-frequency system proved to be a reliable and secure communications channel, providing a connection to almost 1,500 railway stations. The company has been reluctant to use Starlink, as its signals could be intercepted and allow the localization of leadership personnel.²⁹³

Before the invasion, IC operators adapted and refined their contingency plans and adjusted their operations to the circumstances. While maintenance crews put in many shifts to keep internet infrastructure running, hundreds of volunteers and private organizations shoulder a significant part in reconnecting fiber cables and restoring mobile base stations in their respective regions, sometimes by bringing their own equipment and spare parts. This cooperation goes so far that telecommunica-

tion operators request skilled volunteers to respond to alerts.²⁹⁴ Another aspect that IC operators had to quickly react to was the evolving refugee and migration flows and the relocation of business activities from east to west, which led to an unusual accumulation of people in certain areas, such as the western border areas, resulting in an increasing need for mobile connectivity. Mobile operators took various steps to ensure the accessibility and affordability of their services. First, they requested the responsible ministries to broaden the spectrum of allowed frequency bands to accommodate the increasing demand.²⁹⁵ Second, collaborations between operators emerged with the support of the government. In March 2022, the Ukrainian Ministry of Digital Transformation decided with the three major operators on the mobile market to activate free internal roaming throughout the country (voice, SMS, mobile internet), allowing connection to another provider if one service provider's network coverage failed. The networks are thus used jointly to ensure the vital service.²⁹⁶ Service providers have reduced costs of essential communication services and made efforts to restore and adjust network load and demand due to high traffic volumes and fluctuations in the early days of the war. This was achieved through an adaptable and restructured IC infrastructure, re-routing and distribution of traffic to different operators, reducing the speed of service of some consumers or applications to relieve bandwidths, and prioritizing the demands of certain consumers.²⁹⁷ To support Ukrainians who have sought refuge in other European countries, international roaming agreements have been implemented with European operators to lower costs, including the distribution of free SIM cards.²⁹⁸ The attempts of the government to create a business-friendly environment for CI operators further supports agreements and collaborations. For example, a relaxation of accounting and reporting standards for companies in the electronic communication industry during the war was introduced.²⁹⁹ In addition, telecommunication operators can obtain electricity for their infrastructures de facto free of charge until the end of martial law plus 60 days, i.e., for 1 kopeck or approximately 0.00026 USD per month.³⁰⁰ The power supply was the biggest concern for IC operation, as it was the reason for most of the IC outages. Mobile base stations were therefore equipped with diesel generators to sustain the power supply, especially in rural areas. At the same time, better batteries were acquired to replace damaged infrastructure or bridge disruptions of the energy supply. Old lead-acid batteries are continuously replaced by modern lithium-ion systems that last longer and can be recharged faster. For example, Kyivstar has installed 8,000 new batteries within its network, putting considerable pressure on the market for these goods.³⁰¹

Likewise, the IT industry and its companies facing power outages and resulting destabilizations of systems resorted to different measures, including acquiring

diesel generators, fuel, and batteries. Some companies also implemented notification systems that monitored energy supply and connectivity to timely switch to other service channels like Starlink or diversify their internet service providers.³⁰² IT companies also ensured that business continuity management (BCM) plans were in place and could be implemented quickly.³⁰³

In the media and news domain, a shift in news consumption and distribution from traditional sources to social media has been observed. The rise of the messenger app Telegram, which hosts the channels of the president, governors, and government officials is particularly striking.³⁰⁴ This development led TV and radio channels to expand to alternative platforms like YouTube.³⁰⁵ The television stations underwent further changes with the introduction of martial law, which calls for a uniform information policy.³⁰⁶ Television has become concentrated under the monopolizing force of the newly emerged United News, a conglomerate initiated by the four largest TV networks, to share the effort of 24-hour non-stop broadcasting, calling it the "national telethon". The aim is to speak as one voice to deliver information during the war. The approach of coordinating the TV broadcasting services is seen as one pillar of securing the media and information space, while pro-Russian channels were already banned before the invasion.³⁰⁷ The banning of pro-Russian channels in 2021 was perceived as a contribution to security. However, broadcasters outside the national telethon are struggling to implement government regulations and criticism is being voiced, questioning freedom of speech.³⁰⁸

With the war still ongoing, *recovering from incidents* is a difficult undertaking. Although repair crews and technicians work around the clock to fix damaged sections of physical IC infrastructure, some areas are inaccessible due to the occupation or ongoing fighting. Among the challenges reconstruction teams face are the restrictions imposed by martial law on the purchase and import of equipment, access to certain areas, or curfews.³⁰⁹ This forced telecommunication operators to become more efficient and adapt to the circumstances of war by organizing teams remotely, reinforcing teams with personnel from other cities, or scheduling deployment at a time when fighting was likely to be at its lowest.³¹⁰ In the search for spare parts, online platforms have been set up on which companies worldwide can voluntarily indicate which ICT spare parts they can offer. While repairs and restoration will only maintain the current system, the long-term focus is on *recovery* and depends heavily on adequate funding. While the international community has launched various initiatives, Ukrainian telecommunication companies have already pledged funding to recover and modernize the country's IC infrastructure, such as Kyivstar, which has pledged 600 million USD to rebuild digital services.³¹¹ Despite the significant impact of the war

on the country and its economy, the IC sector has kept on pushing innovation and maintained the countries basis for further digitalization. For example, the Ministry of Digital Transformation has accelerated its drive to digitize the citizens' interaction with the state through the Diia app since the beginning of the invasion, shifting to a 24/7 service and continuously introducing new services to expand state and public services and facilitate citizen interaction during wartime.³¹² Another example is the project IT Generation that is aimed at increasing the number of IT professionals.³¹³

As far as *ensuring adequate employee security is concerned*, a number of points were identified. Prior to the invasion, Lifecell specifically trained and prepared its personnel for armed conflict. While some employees have been or are still exposed to the dangers of hostilities, e.g., when maintaining or restoring physical infrastructure, many have relocated to safer areas or even outside Ukraine. With the lessons learned and implemented during the pandemic, working from home has become more effective and, above all, safer in times of war. The security departments of the companies support and advise employees and their families, particularly in high-risk zones, and provide financial remuneration, e.g., in the form of risk premiums.³¹⁴ IT companies have adapted offices to enable employees to live there, or they pay for relocation and co-working spaces.³¹⁵ Under martial law, men have not been permitted to leave the country, while the Minister of Digital Transformation urged the government to keep IT professionals in place and relieve them from possible drafting.³¹⁶ As a result, more than 85 per cent of the country's IT professionals defend the economy in various roles in the private and public sectors.³¹⁷

This case study on IC identifies a number of key factors for the resilience of this CI sector. First, public-private and private-sector partnerships and collaborations have improved preparedness and response during times of stress. Second, international assistance has played a vital role in ensuring functionality and protection. Third, the conflict in Ukraine has highlighted the benefits of offering public services virtually and accelerated digitalization. Fourth, employee training enhances resilience. Lastly, the IC sector relies heavily on a stable power supply and must therefore seek redundancies in order to at least bridge short-term power outages to ensure functionality.

5 Resilience Approaches and Lessons Learned

The preceding case studies provide an insight into three different CI sectors, presenting characteristics of the systems, the impact of Russian aggression against Ukraine on the infrastructure, and factors and measures that have bolstered the resilience of the system, including its CI entities and assets that provide the essential services. In an armed conflict, the protection and resilience of CI is a crucial element that contributes to the overall resilience of a society. Although the three selected CI sectors are different and face sector-specific challenges, general overarching lessons can be identified. The following overview serves as a compendium of lessons that are also relevant to risks other than armed conflict and can therefore inform CIP and resilience efforts in an all-hazards approach.

Historically grown redundancies can boost resilience

Maintaining the availability of historically grown redundancies in CI that have proven to be reliable over time increases resilience by enabling fallback levels for emergencies. All three CI sectors examined exhibit redundancies that are rooted in the historical or pre-war design of the systems, regardless of whether they were implemented intentionally or evolved as a result. For example, the extensive transit and distribution network in the energy sector made it possible to bypass local disturbances via alternative routes. The national power grid, which was established after the Cold War by merging regional grids, provided the country with excess capacities at the beginning of the invasion. The transportation and logistics sector was able to maintain its operations thanks to the rail network, which is still operated with diesel trains on around half of its extensive network, and even takes over the tasks of other ailing modes of transport. The distribution of end-user networks for internet access among thousands of providers limited the interruptions to the users of the affected networks. This independence of end-user networks can also be observed in the energy sector with its regional power grids, which are able to operate in island mode, or in the transport sector with the six railway regions, which are able to perform the entire range of operations independently. The interconnectedness of the Ukrainian system has also supported the protection of particular CI components. For example, Ukraine's unique position as an important transit country for gas and oil kept Russia from attacking those assets, at least initially.

International assistance bridges gaps and fosters (early) reconstruction

International assistance was and remains a crucial success factor for all of Ukraine's efforts. While the Ukrainian armed forces receive continuous assistance, the three case studies demonstrate how important external support is for the operation of CI as well. First, rapid engagement and dialogue that clearly defined what is needed enabled the country to unlock specific capabilities, such as Starlink to smoothen telecommunication outages. For Ukraine, it has therefore been essential to quickly promote and steer international support efforts by engaging in bi- or multilateral agreements and mechanisms (e.g., solidarity lanes, international roaming agreements, UCPM) and leveraging or instrumentalizing one's key positions (e.g., grain deal, which facilitated global food supply) to maximize assistance. These agreements enabled Ukraine to bridge emerging shortages in essential services, for example, by importing electricity via ENTSO-E. Second, the conclusion of agreements required commitments, exemplified by the reconstruction and expansion of the rail system according to EU standards. Entering into such agreements becomes more targeted if concepts of the recovery and reconstruction of damaged infrastructure are drawn up at an early stage. Immediate initiation of recovery and reconstruction efforts allows for more targeted funding and a well-ordered transition in the post-war period, demonstrated, for example, by the agreed slots for airlines once civil airspace is reopened.

Well-prepared state emergency measures guarantee minimal services

With the invasion, the Ukrainian government declared a state of war and martial law. Since then, various emergency measures have been implemented to maintain a certain level of essential services. These measures included adapted regulations for CI operators and their services. Examples include the expansion of usable frequency bands for telecommunication operators, the continued wage payments for railway workers, or the relaxation of regulations on how much fuel can be stored without a permit. In contrast, regulation became stricter in certain areas. For example, travel bans decreased the flexibility of IT companies, rolling blackouts and consumption restrictions in the energy sector limited consumption, and the prioritization of connectivity in the IC sector reduced access for certain actors. The aim of all these measures was to ensure the provision of essential services in all CI sectors, to keep the overall system running, and to strike a balance between military efforts, civil security, and societal well-being.

BCM secures operations

BCM surfaces in various forms and throughout different organizational levels of CI stakeholders, including the administration, authorities, and companies. First, human capital improved resilience in all three sectors examined. Prioritizing employee safety, retention, and well-being is paramount for strengthening human capital. This can be achieved through measures such as continued pay or crisis-oriented training. Such approaches have facilitated the creation of pools of specialists who are able to move seamlessly between different positions, increasing flexibility, and easing the transition back to normal operations. Examples for this include safety training for telecommunication staff, the reallocating of staff in the railway sector, and the retention of specialist staff in the aviation industry. In addition, the education system must ensure that there are enough qualified staff, for example through initiatives like IT Generation. The strong social cohesion created by the shared experience of war has also released additional potential in the form of volunteers and former employees brought out of retirement. These additional workers fill gaps and help to keep operations running with their expertise. Second, the efficiency of remote coordination, communication, and deployment of staff, as seen during the pandemic, underscores the value of lessons learned from previous crises. Third, reduced exposure saves lives and assets in an armed conflict. Examples for this include the relocation of physical and virtual assets such as airplanes or data centers away from the possible sources of danger, the implementation of evacuation plans in all three analyzed CI sectors, and the relocation of businesses, such as IT companies, and potential targets, such as company management or mobile energy supply. Fourth, the acquisition of spare parts becomes more challenging the longer a conflict lasts, as seen in the energy sector. The railway company Ukrzaliznytsia tries to meet this challenge by adapting its production facilities to produce its own spare parts. Here, too, voluntary engagement can play an important role in bridging gaps, as demonstrated by the volunteers who bring spare parts to repair power transmission lines, railways, or fiber cables. Lastly, as almost every modern business and operational activity requires energy, the impact of energy shortages and power outages has been mitigated by switching to diesel fuel, e.g., for the operation of telecommunication base stations or trains, or by replacing older batteries with more powerful ones. The energy sector itself has also focused on switching to more local and renewable energy sources, such as solar or wind power.

Private-public coordination and cooperation assures an effective response

A shared crisis not only creates social cohesion, but also solidarity and support between government and compa-

nies, which should be institutionalized before, during and after a crisis. As CI and essential services often intersect with those of private operators and public or government agencies, coordination and cooperation are fundamental to crisis management. Ukraine has strengthened this facet of CIP and resilience to secure essential services. First, industry agreements such as the government-backed initiative to share telecommunication networks between the big three providers or the cross-company coordination of resources (spare parts, staff, etc.) between energy suppliers have supported the response of the entire CI sector. Second, committees and bodies for close cooperation between industry, military, law enforcement, and government agencies installed before or during the invasion facilitated the efficient coordination of protection, repair, or restoration work. For example, energy providers coordinate their cyber defense efforts with government actors through private sector headquarters, and IC operators and the National Operation Center for Telecommunication work closely together in their cyber defense efforts.

Decentralization and diversification reduce vulnerability

Decentralization and diversification are heavily emphasized concepts for creating resilient systems. Both can be found in Ukraine. The energy sector was able to diversify into different energy sources and decentralize its supply structures from large central infrastructure elements to smaller generation capacities for local CI. The transportation sector case study has shown that when seaports are closed or damaged, the river network, peripheral river ports, and rail infrastructure offer an alternative for exporting goods. Decentralization and diversification can result from the historical design of a system, but they can also be the result of preparatory or response measures (e.g., sharing of networks by telecommunication providers) and reduce the vulnerability to disruption of essential services.

Continued digitalization increases efficiency

The continuous efforts of the Ukrainian government to advance digitalization have supported the overall resilience of society, the economy, and CI, for example through the rapid integration of missile alerts into the e-government apps for citizens. Digitalization made it possible to efficiently back up data abroad, implement shelter locations in the rail app, and operate online platforms to communicate globally which spare parts are needed. Moreover, the efficiency of remote coordination, communication, and deployment of employees is constantly increased by digital solutions. Overall, the country's digital ambitions hold the potential to modernize CI and thus directly and indirectly support the reconstruction and recovery efforts.

Adequate legislation facilitates preparedness

Although CI, its protection, and resilience have found their way into legislation only recently, the preceding development of CIP and the cross-cutting cyber strategies, coupled with lessons learned since 2014, have enabled more targeted legislation. Legislation defines responsibilities, informs and adapts stakeholders, and requires protective measures to be taken. This increases the preparedness of CI operations for emergencies. Moreover, non-CI-related legislation, such as the decentralization reform or the regulation allowing data to be stored abroad, has further increased the freedom of action, enabled investments in infrastructure, and improved the provision of resources at regional and local level. However, not only the legislation and its implementation, but also the activities that took place before the legislation was passed, such as consultations, table-top exercises, etc., forced stakeholders to address the issue of CIP and CI resilience even before the invasion.

Military authorities are crucial for CIP

In contrast to natural hazards or accidents, CI in an armed conflict cannot only be affected by indiscriminate damage, but can also become a targeted object of strategic, operational, or tactical importance. Such deliberate targeting, as seen in the energy infrastructure in Ukraine, requires equally sophisticated and specialized protection, both kinetic and cyber. Even though some Ukrainian energy infrastructures have been hardened, this does not replace primary defense against kinetic threats, e.g., air defense. CIP must be an integral part of defense planning by military authorities. Similarly, non-military efforts to protect CI must incorporate the military domain to create an all-hazards approach to CI resilience. Conducting table-top exercises involving different stakeholders has proven to be a viable option for engaging stakeholders, sharing knowledge, coordinating tasks, clarifying responsibilities, and discussing or simulating scenarios with different objectives and outcomes, as has been done in the energy sector.

6 Concluding Remarks

With the aim of understanding the impact of the Russian invasion on Ukrainian CI and drawing lessons for resilience, this report offers insights into how Ukrainian CI continues to provide essential services despite being deliberately compromised by the adversities of war. As the Ukrainian understanding of CIP and CI resilience are aligned with the Western view, the report offers insights into the value of the current understanding of CIP when confronted with the hazards of armed conflict.

First, the case of Ukraine demonstrates that it is essential to integrate CIP and CI resilience into overall national security and defense concepts to achieve an all-hazards approach. Second, the case studies presented emphasize the shift in the definition of CI from a solely physical basis to a system of physical and non-physical assets. The analyzed case studies offer the opportunity to examine the non-physical side in more detail and to understand the nature of CI and its resilience more holistically. While physical and non-physical CI assets have been destroyed or damaged, various components of the broader CI system, including interdependent elements, have attempted, and often succeeded in securing essential services. These components are institutional, social, historical, relational, network, and human in nature. Third, the Ukrainian CI system is characterized by diversity, modularity, and redundancy, and draws its resilience from various internal sources such as BCM, private-public collaborations and lessons learned from the pandemic, previous security challenges, as well as from the external dimension of international assistance.

At the time of writing, Ukraine is in its second winter of war. Although defense capabilities such as air defense have been ramped up with Western support, it remains to be seen how the already battered CI system will continue to cope and adapt to further attacks.

7 Bibliography

- 1 DeepL SE, *DeepL Translator*, deepl.com, nd.; Google, *Google Translate*, translate.google.com, nd.
- 2 Stephan J. Collier / Andrew Lakoff, "The vulnerability of vital systems," in: Miriam Dunn Cavelty / Kristian Sjøby Kristensen (eds.), *Securing 'the Homeland'* (London and New York: Routledge, 2008), pp. 17–39.
- 3 Stephan J. Collier / Andrew Lakoff, *The Government of Emergency: Vital Systems, Expertise, and the Politics of Security* (Princeton and Oxford: Princeton University Press, 2021), pp. 39–42.
- 4 Stephan J. Collier / Andrew Lakoff, "The vulnerability of vital systems," in: Miriam Dunn Cavelty / Kristian Sjøby Kristensen (eds.), *Securing 'the Homeland'* (London and New York: Routledge, 2008), pp. 17–39.
- 5 Andrew Lakoff / Stephen J. Collier, "Infrastructure and Event: The Political Technology of Preparedness," in: Bruce Braun / Sarah J. Whatmore (eds.), *Political Matter: Technoscience, Democracy, and Public Life* (Minneapolis: University of Minnesota Press, 2010), pp. 243–266.
- 6 Claudia Aradau, "Security That Matters: Critical Infrastructure and Objects of Protection," *Security Dialogue* 41:5 (2010), pp. 491–514.
- 7 Alessandro Lazari, *European Critical Infrastructure Protection* (Cham: Springer International Publishing, 2014), p. 4.
- 8 National Protective Security Authority, *Critical National Infrastructure*, npsa.gov.uk, 25.04.2023.
- 9 Federal Office for Civil Protection FOCP, *Critical infrastructure protection*, admin.ch, nd.
- 10 Federal Office for Civil Protection FOCP, *Critical Infrastructure*, admin.ch, nd.
- 11 Miriam Dunn Cavelty / Kristian Sjøby Kristensen, "Introduction: securing the homeland: critical infrastructure, risk, and (in)security," in: Miriam Dunn Cavelty / Kristian Sjøby Kristensen (eds.), *Securing 'the Homeland'* (London and New York: Routledge, 2008), pp. 1–14.
- 12 Steven M. Rinaldi / James p. Peerboom / Terrence K. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," *IEEE Control Systems Magazine* 21:6 (2001), pp. 11–25.
- 13 Martin Coward, "Network-Centric Violence, Critical Infrastructure and the Urbanization of Security," *Security Dialogue* 40:4/5 (2009), pp. 399–418.; Martin Ruder, "Cyber-Threats to Critical National Infrastructure: An Intelligence Challenge," *International Journal of Intelligence and Counterintelligence* 26:3 (2013), pp. 453–481.
- 14 OECD, *Good Governance for Critical Infrastructure Resilience* (Paris: OECD Publishing, 2019).
- 15 Verkhovna Rada of Ukraine, Проект Закону про критичну інфраструктуру, rada.gov.ua, 2021.
- 16 European Parliament / Council of the European Union, *Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC*, eur-lex.europa.eu.
- 17 European Parliament / Council of the European Union, *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)*, eur-lex.europa.eu.
- 18 Alessandro Lazari, *European Critical Infrastructure Protection* (Cham: Springer International Publishing, 2014).
- 19 Andrew Lakoff / Stephen J. Collier, "Infrastructure and Event: The Political Technology of Preparedness," in: Bruce Braun / Sarah J. Whatmore (eds.), *Political Matter: Technoscience, Democracy, and Public Life* (Minneapolis: University of Minnesota Press, 2010), pp. 243–266.
- 20 Ibid.
- 21 Ibid.
- 22 Miriam Dunn Cavelty / Kristian Sjøby Kristensen, "Introduction: securing the homeland: critical infrastructure, risk, and (in)security," in: Miriam Dunn Cavelty / Kristian Sjøby Kristensen (eds.), *Securing 'the Homeland'* (London and New York: Routledge, 2008), pp. 1–14.; Stephan J. Collier / Andrew Lakoff, "The vulnerability of vital systems," in: Miriam Dunn Cavelty / Kristian Sjøby Kristensen (eds.), *Securing 'the Homeland'* (London and New York: Routledge, 2008), pp. 17–39.
- 23 Christer Pursiainen, "Critical infrastructure resilience: A Nordic model in the making?," *International Journal of Disaster Risk Reduction* 27 (2018), p. 632–641.
- 24 Crawford S. Holling, "Engineering Resilience versus Ecological Resilience," in: Peter Schulz (ed.), *Engineering within Ecological Constraints* (Washington, DC: National Academy of Engineering, 1996), pp. 31–43.
- 25 Carl Folke, "Resilience: The emergence of a perspective for social–ecological systems analyses," *Global Environmental Change* 16:3 (2006), pp. 253–267.; Carl Folke et al., "Resilience and Sustainable Development: Building Adaptive Capacity in a World of Transformations," *AMBIO: A Journal of Human Environment* 31:5 (2002), pp. 437–440.; Markus Keck / Patrick Sakdapolrak, "What is Social Resilience? Lessons Learned and Ways Forward," *Erdkunde* 67:1 (2013), pp. 5–19.; Brian Walker et al., "Ecology and Society: Resilience, Adaptability and Transformability in Social–ecological Systems," *Ecology and Society* 9:2 (2004).
- 26 European Parliament / Council of the European Union, *Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC*, eur-lex.europa.eu.
- 27 European Commission / Directorate-General for Migration and Home Affairs, *Commission Staff Working Document Impact Assessment: Accompanying the document Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities*, eur-lex.europa.eu, 16.12.2020.
- 28 European Commission / Directorate-General for Migration and Home Affairs, *COMMISSION DELEGATED REGULATION (EU) of 25.07.2023 supplementing Directive (EU) 2022/2557 of the European Parliament and of the Council by establishing a list of essential services*, eur-lex.europa.eu, 2023.
- 29 OECD, *Good Governance for Critical Infrastructure Resilience* (Paris: OECD Publishing, 2019).; United Nations Office for Disaster Risk Reduction, *Making Critical Infrastructure Resilient* (Brussels: United Nations Office for Disaster Risk Reduction, 2020).
- 30 Federal Council, *Nationale Strategie zum Schutz kritischer Infrastrukturen Ganzheitlicher Ansatz zur Sicherstellung der Verfügbarkeit von essenziellen Gütern und Dienstleistungen*, fedlex.admin.ch, 2023.
- 31 Verkhovna Rada of Ukraine, Проект Закону про критичну інфраструктуру, rada.gov.ua, 2021.
- 32 NATO, *Resilience, civil preparedness and Article 3*, nato.int, 02.08.2023.; Edward H. Christie / Kristine Berzina, "NATO and Societal Resilience: All Hands on Deck in an Age of War," *German Marshall Fund of the United States*, 2022.
- 33 The Kremlin, *Address by the President of the Russian Federation*, en.kremlin.ru, 24.02.2022.
- 34 Paul D'Anieri, *Ukraine and Russia: From Civilized Divorce to Uncivil War* (Cambridge/New York: Cambridge University Press, 2023), pp. 272–307.; Silvia Aloisi / Frank Jack Daniel, "Timeline: The events leading up to Russia's invasion of Ukraine," *Reuters*, 01.03.2022.; Andrew Osborn / Polina Nikolskaya, "Russia's Putin authorises 'special military operation' against Ukraine," *Reuters*, 24.02.2022.; Harris et al., "As Russia prepared to invade Ukraine, U.S. struggled to convince Zelensky, allies of threat," in: *Washington Post*, 16.08.2023.
- 35 Andrew E. Kramer / Andrew Higgins, "The focus of fighting shifts to Ukraine's south," *The New York Times*, 15.08.2022.
- 36 Niklas Masuhr, "Die Invasion der Ukraine nach einem Jahr – Ein militärischer Rück- und Ausblick," *Länder-Analysen* 279 (2023), pp. 5–10.; Andrian Prokip, *The Russian Federation's Acts of Nuclear Terrorism Must Be Stopped*, wilsoncenter.org, 10.03.2022.; Will Vernon / Laura Gozzi, "Ukraine war: Sergei Surovikin removed as commander of Ukraine invasion force," *BBC News*, 11.01.2023.
- 37 Stéphane Duguin / Pavlina Pavlova, "The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict," *Think Thank European Parliament*, 04.09.2023, pp. 10–11.
- 38 Centre for Information Resilience, "Weaponising Winter: The strategic shift in Russia's attacks on Ukraine's energy infrastructure," *Centre for Information Resilience*, 2023.
- 39 Lennart Maschmeyer, "Assessing Hybrid War: Separating Fact from Fiction," *CSS Analyses in Security Policy* 332 (2023).; Frank Hoffmann, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Arlington, VA: Potomac Institute for Policy Studies, 2007).
- 40 Council of the European Union, *Council Recommendation of the European Union of 8 December 2022 on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure*, eur-lex.europa.eu, 08.12.2022.
- 41 NATO, *NATO and European Union launch task force on resilience of critical infrastructure*, nato.int, 16.03.2023.; NATO ENERGY SECURITY Center of Excellence, *Execution of the Table Top Exercise Coherent Resilience 2022 CEPS*, enseccoe.org, 27.10.2022.
- 42 Kateryna Zarembo / Sergiy Solodky, *The Evolution of Russian Hybrid Warfare: Ukraine*, cepa.org, 29.01.2021.; Dumitru Minzarari, "An Assessment of Russia's Way of War in the Wake of its Aggression in Ukraine," in: Pentti Forsström (ed.), *Russia's War on Ukraine: Strategic and Operational Designs and Implementation* (Helsinki: National Defence University Department of Warfare, 2023), pp. 10–20.

- 43 Shane Harris, "Hack Attack," *Foreign Policy*, 03.03.2014.; Michael Kofman et al., *Lessons from Russia's Operations in Crimea and Eastern Ukraine* (California: Rand Corporation, 2017).
- 44 Carol V. Evans, "Future Warfare: Weaponizing Critical Infrastructure," *Parameters* 50:2 (2020), pp. 3–42.
- 45 Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, 03.03.2003.; John Hultquist, *Sandworm Team and the Ukrainian Power Authority Attacks*, mandiant.com, 07.01.2016.; Michael Assante, *Confirmation of a Coordinated Attack on the Ukrainian Power Grid*, sans.org, 06.01.2016.
- 46 Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, 22.08.2018.
- 47 Charlie Smart, "How the Russian Media Spread False Claims About Ukrainian Nazis" *The New York Times*, 02.07.2022.
- 48 Mathieu Boulègue / Orysia Lutsevych / Anaïs Marin, "Civil society Under Russia's Threat: Building Resilience in Ukraine, Belarus and Moldova," *Chatham House: The Royal Institute of International Affairs*, November 2018, pp. 7–19.
- 49 Interview with Ukrainian representatives in autumn 2023.
- 50 Sergiy Kondratov et al., *Developing the Critical Infrastructure Protection System in Ukraine* (Kyiv: National Institute for Strategic Studie, 2017); Ihor Yefimenko / Andrii Sakovskyi / Yevhen Bilozorov, "Protection of critical infrastructure as a component of Ukraine's national security," *Law Journal of the National Academy of Internal Affairs* 13:2 (2023), pp. 74–85.
- 51 Oleksandr Sukhodolia, "Implementation of the Concept of Critical Infrastructure Protection in Ukraine: Achievements and Challenges," *Information & Security: An International Journal* 40:2 (2018), pp. 107–119.; Oleksandr Sukhodolia, "Ukraine," in: Alessandro Lazari / Robert Mikac (eds.), *The External Dimension of the European Union's Critical Infrastructure Protection Programme* (London: Routledge, 2022), pp. 133–149.
- 52 Verkhovna Rada of Ukraine, Про основні засади забезпечення кібербезпеки України, rada.gov.ua, 17.08.2017.
- 53 Oleksandr Sukhodolia, "Ukrainian Energy Sector under Military Attack: Lessons for Resilience," in: Tomas Jermalaivičius (ed.), *War and Energy Security: Lessons for The Future* (Tallinn: International Center for Defence and Security, 2023), p. 46.; Dimitry Dubov / Oleksandr Sukhodolia, Президент України підписав Закон України «Про критичну інфраструктуру», niss.gov.ua, 13.12.2021.
- 54 Hanna Shelest, *NATO's Resilience Concept and Ukraine*, prisma.ua, 29.12.2021.; President of Ukraine, УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №392/2020, president.gov.ua, 14.10.2020.; President of Ukraine, УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №448/2021, president.gov.ua, 30.07.2021.; President of Ukraine, УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №479/2021, president.gov.ua, 20.08.2021.
- 55 Valentyna Romanova, "Ukraine's resilience to Russia's military invasion in the context of the decentralisation reform," *Stefan Batory Foundation*, 2022.
- 56 Cătălin Peptan, "Considerations on some aggressions against critical infrastructure on the territory of Ukraine during the 'special military operation' conducted by the Russian Federation," *Annals of the 'Constantin Brancusi' University of Targu Jiu, Engineering Series* 1/2022 (2022), pp. 37–47.; Bogusław Pacek / Piotr Pacek, "Russia's devastating impact on critical infrastructure during the hybrid war in Ukraine," *Bezpieczeństwo* 2:51 (2023), p. 11–27.
- 57 Raphael Satter, "Satellite outage caused 'huge loss in communications' at war's outset -Ukrainian official," *Reuters*, 15.03.2022.
- 58 Seth G. Jones / Riley McCabe / Alexander Palmer, "Seizing the Initiative in Ukraine: Waging War in a Defense Dominant World," *Center for Strategic & International Studies*, 12.10.2023.
- 59 The Economist, "The war has devastated Ukraine's environment, too," *The Economist*, 12.01.2023.
- 60 PAX, *Environment and Conflict Alert Ukraine: A first glimpse of the toxic toll of Russia's invasion of Ukraine*, paxforpeace.nl, 09.03.2022.
- 61 Viktor Vyshnevskiy et al., "The destruction of the Kakhovka dam and its consequences," *Water International* 48:5 (2023), pp. 631–647.; UN RC/HC Ukraine / UNCT Ukraine, "Potential Long-Term Impact of the Destruction of the Kakhovka Dam," *United Nations Ukraine*, 09.06.2023.
- 62 Wim Zwijnenburg / Iryna Nikolaieva, "Attacks on Agro-Industrial Sites in Ukraine: Environment and Conflict Alert Ukraine," *PAX*, 2023.
- 63 World Health Organization, *WHO records 100th attack on health care in Ukraine*, who.int, 07.04.2022.; PAX, "Impact on healthcare from bombing and shelling in Ukraine," *PAX*, 31.03.2022.; Marta Dzhus / Iryna Golovach, "Impact of Ukrainian-Russian War on Health Care and Humanitarian Crisis," *Disaster Medicine and Public Health Preparedness* 17:e340 (2023), pp. 1–3.
- 64 Christian De Vos et., "Destruction and Devastation: One Year of Russia's Assault on Ukraine's Health Care System," *Physicians for Human Rights*, 21.02.2023.
- 65 Centre for Information Resilience, "Education: The effect of the invasion on Ukraine's education system – One year overview," 2023.
- 66 Iryna Nikolaievy / Wim Zwijnenburg, "Risks and impacts from attacks on energy infrastructure in Ukraine," *PAX*, 2022.
- 67 Iryna Nikolaievy / Wim Zwijnenburg / Christina Parandii, "Risks and Impacts from Attacks on Fossil Fuel Facilities in Ukraine," *PAX*, 2023.
- 68 USAID, *How did Ukraine synchronize with the EU's power system, and why is it important for the country's energy security*, energysecurityua.org, 16.03.2023.; Andrian Prokip, *Integration of Ukrainian Power System to ENTSO-E: challenges and opportunities*, ceenergynews.com, 25.03.2021.
- 69 Government of Ukraine, Робота енергосистеми України станом на 15 червня 2022 року, kmu.gov.ua, 15.06.2022.
- 70 Iryna Nikolaievy / Wim Zwijnenburg, "Risks and impacts from attacks on energy infrastructure in Ukraine," *PAX*, 2022.
- 71 Jane Arraf, "Russian Missiles Hit Power Stations in Lviv and Along Crucial Railways," *The New York Times*, 03.05.2022.; Jaco Cilliers, *Uncovering the reality of Ukraine's decimated energy infrastructure*, undp.org, 12.04.2023.
- 72 Ian Williams, "Putin's Missile War: Russia's Strike Campaign in Ukraine," *Center for Strategic & International Studies*, May 2023, pp. 20–21.
- 73 Niklas Masuhr, "Die Invasion der Ukraine nach einem Jahr – Ein militärischer Rück- und Ausblick," in: *Länder-Analysen* 279 (2023), pp. 5–10.
- 74 Microsoft Digital Security Unit, "An overview of Russia's cyberattack activity in Ukraine," *Microsoft Corporation*, 27.04.2022.
- 75 Ministry of Internal Affairs, В Україні з початку повномасштабного вторгнення РФ уражено понад 700 об'єктів критичної інфраструктури, - Євгеній Єнін, mvs.gov.ua, 28.12.2022.
- 76 Francesca Ebel, "Russian defense minister insists Ukraine infrastructure is military target," *The Washington Post*, 01.11.2022.
- 77 Verkhovna Rada of Ukraine, Про затвердження Указу Президента України "Про введення воєнного стану в Україні", rada.gov.ua, 24.02.2022.
- 78 Andrii Darkovich / Myroslava Savisko / Maryna Rabinovych, "Explaining Ukraine's Resilience to Russia's Invasion: The Role of Local Governance and Decentralization Reform," *PONARS Eurasia Policy Memo* 855, 2023.; Maryna Rabinovych et al., "Explaining Ukraine's resilience to Russia's invasion: The role of local governance," *Governance* (2023).
- 79 Valentyna Romanova, "Ukraine's resilience to Russia's military invasion in the context of the decentralisation reform," *Stefan Batory Foundation*, 2022.
- 80 OECD, "Rebuilding Ukraine by Reinforcing Regional and Municipal Governance," (Paris: OECD Publishing, 2022).
- 81 Verkhovna Rada of Ukraine, Про утворення Державної служби захисту критичної інфраструктури та забезпечення національної системи стійкості України, rada.gov.ua, 12.07.2022.
- 82 World Bank Group / Government of Ukraine / European Commission, *Ukraine Rapid Damage and Needs Assessment: February 2022 – February 2023 (English)* (Washington, D.C.: World Bank Group, 2023).
- 83 United Nations Development Programme and World Bank Group, "Ukraine Energy Damage Assessment," *United Nations Development Programme*, 05.04.2023.
- 84 United Nations Development Programme, "Towards a Green Transition of the Energy Sector in Ukraine," *United Nations Development Programme*, 20.06.2023.
- 85 Task Force International Energy Charter, "Ukrainian energy sector evaluation and damage assessment – XI (as of June 24, 2023)," *Energy Charter Secretariat*, 2023.
- 86 Damaged in Ua, Проєкт "Росія заплатить", damaged.in.ua, nd.
- 87 Kyiv School of Economics, "Report on damages and losses to infrastructure from the destruction caused by Russia's military aggression against Ukraine as of June 2023," *Damaged in Ua*, 2023.; Kyiv School of Economics, *The total amount of direct damage to Ukraine's infrastructure caused due to the war as of June 2023 exceeded \$150 billion*, kse.ua, 02.08.2023.
- 88 Kyiv School of Economics, "Report on damages and losses to infrastructure from the destruction caused by Russia's military aggression against Ukraine as of June 2023," *Damaged in Ua*, 2023, pp. 22–28.
- 89 Nino Kubinidze et al., "Interim assessment on damages to telecommunication infrastructure and resilience of the ICT ecosystem in Ukraine," *International Telecommunication Union*, December 2022.
- 90 Iryna Nikolaievy / Wim Zwijnenburg, "Risks and impacts from attacks on energy infrastructure in Ukraine," *PAX*, 2022.; Iryna Nikolaievy / Wim Zwijnenburg / Christina Parandii, "Risks and Impacts from Attacks on Fossil Fuel Facilities in Ukraine," *PAX*, 2023.; Wim Zwijnenburg / Iryna Nikolaieva, "Attacks on Agro-Industrial Sites in Ukraine: Environment and Conflict Alert Ukraine," *PAX*, 2023.
- 91 Christian De Vos et., "Destruction and Devastation: One Year of Russia's Assault on Ukraine's Health Care System," *Physicians for Human Rights*, 21.02.2023.

- 92 United Nations Development Programme, "Human Impact Assessment," *United Nations Development Programme*, 12.06.2023.
- 93 Ivo Juurvee, "Civil Defence in Ukraine: Preliminary Lessons From the First Months of War," *International Center for Defence and Security*, 2022.
- 94 World Bank Group / Government of Ukraine / European Commission, *Ukraine Rapid Damage and Needs Assessment, August 2022* (Washington, D.C.: World Bank Group, 2022), pp. 193–200.; World Bank Group / Government of Ukraine / European Commission, *Ukraine Rapid Damage and Needs Assessment: February 2022 – February 2023 (English)* (Washington, D.C.: World Bank Group, 2023) pp. 114–117.
- 95 European Commission, *Ukraine joins the EU Civil Protection Mechanism*, europea.eu, 20.04.2023.
- 96 Ihor V. Kholoshyn et al., "Assessment of military destruction in Ukraine and its consequences using remote sensing," *IOP Conf. Series: Earth and Environmental Science* 1254 (2023).
- 97 Yusupujian Aimaity et al., "War Related Building Damage Assessment in Kyiv, Ukraine, Using Sentinel-1 Radar and Sentinel-2 Optical Images," *Remote Sensing* 14:24 (2022).
- 98 UNOSAT, *UNOSAT Analyses*, unosat.org, nd.; Zoi Environment Network, *Ecodozor: environmental consequences and risks of the fighting in Ukraine*, ecodozor.org, nd.
- 99 Centre for Information Resilience, *Eyes on Russia*, eyesonrussia.org, nd.; Bellingcat, *Civilian Harm in Ukraine*, ukraine.bellingcat.com, nd.
- 100 Christoph Trebesch et al., "The Ukraine Support Tracker: Which countries help Ukraine and how?," *Kiel Institute for World Economy*, 2023.
- 101 Charles p. Ries / Howard J. Shatz, *Looking Beyond the War: Planning for Ukraine's Reconstruction*, rand.org, 2023.; Howard J. Shatz et al., *Reconstructing Ukraine: Creating a Freer, More Prosperous, and Secure Future* (Santa Monica: RAND Corporation, 2023).
- 102 Federal Department of Foreign Affairs FDFA, "Presentation of the Lugano Declaration as a political framework for reconstruction in Ukraine," eda.admin.ch, 05.07.2022.
- 103 Foreign, Commonwealth & Development Office, *Ukraine Recovery Conference 2023*, gov.uk, nd.
- 104 The Economist, "The EU has begun debating how to fund the reconstruction of Ukraine," *The Economist*, 16.01.2023.; OECD, *Rebuilding Ukraine by Reinforcing Regional and Municipal Governance* (Paris: OECD Publishing, 2022).; OECD, *OECD strengthens support for Ukraine with four-year Country Programme*, oecd.org, 07.06.2023.; Ronja Ganster et al., "Designing Ukraine's Recovery in the Spirit of the Marshall Plan," *The German Marshall Fund of the United States*, 2022.
- 105 The National Council for the Recovery of Ukraine from the Consequences of the War, "Draft Ukraine Recovery Plan: Materials of the 'Recovery and development of infrastructure' working group," *National Council for the Recovery of Ukraine from the War*, July 2022.; President of Ukraine, *Ukraine Recovery Plan*, recovery.gov.ua, nd.
- 106 Federal Office for Civil Protection FOCF, *Kritische Infrastrukturen*, admin.ch, nd.; European Commission / Directorate-General for Migration and Home Affairs, *COMMISSION DELEGATED REGULATION (EU) of 25.07.2023 supplementing Directive (EU) 2022/2557 of the European Parliament and of the Council by establishing a list of essential services*, eur-lex.europa.eu, 2023.; NATO, *Resilience, civil preparedness and Article 3*, nato.int, 02.08.2023.; Edward H. Christie / Kristine Berzina, "NATO and Societal Resilience: All Hands on Deck in an Age of War," *German Marshall Fund of the United States*, 2022.
- 107 European Parliament / Council of the European Union, *Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC*, eur-lex.europa.eu.
- 108 Federal Office for Civil Protection FOCF, *Kritische Infrastrukturen*, babs.admin.ch, nd.
- 109 Federal Council, *Nationale Strategie zum Schutz kritischer Infrastrukturen Ganzheitlicher Ansatz zur Sicherstellung der Verfügbarkeit von essenziellen Gütern und Dienstleistungen*, fedlex.admin.ch, 2023, p. 7.
- 110 European Parliament / Council of the European Union, *Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC*, eur-lex.europa.eu.; European Parliament / Council of the European Union, *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)*, eur-lex.europa.eu.
- 111 EU-NATO Task Force on the Resilience of Critical Infrastructure, "Final Assessment Report," NATO, 2023, p. 5f.
- 112 NATO, *Resilience, civil preparedness and Article 3*, nato.int, 02.08.2023.
- 113 Verkhovna Rada of Ukraine, Проект Закону про критичну інфраструктуру: Стаття 9. Сектори критичної інфраструктури, rada.gov.ua, 25.11.2021.
- 114 United Nations Development Programme and World Bank Group, "Ukraine Energy Damage Assessment," *United Nations Development Programme*, 05.04.2023, p. 4.
- 115 Iryna Nikolaiev / Wim Zwijnenburg / Christina Parandii, "Risks and Impacts from Attacks on Fossil Fuel Facilities in Ukraine," *PAX*, 2023, p. 4.
- 116 Our World in Data, *Share of Energy consumption by source, Ukraine*, ourworldindata.org, 2023.
- 117 Our World in Data, *Electricity access Ukraine*, ourworldindata.org, 29.05.2023.; Our World in Data, *Share of the population with access to clean fuels for cooking*, ourworldindata.org, 29.05.2023.
- 118 International Energy Agency IEA, "Ukraine Energy Profile," IEA, 2020, p. 21.
- 119 Iryna Nikolaiev / Wim Zwijnenburg / Christina Parandii, "Risks and Impacts from Attacks on Fossil Fuel Facilities in Ukraine," *PAX*, 2023, p. 4.
- 120 Ibid.
- 121 International Energy Agency IEA, "Ukraine Energy Profile," IEA, 2020, p. 20.
- 122 International Energy Charter, "Ukrainian energy sector evaluation and damage assessment – II," *International Energy Charter*, 2022, p. 10.
- 123 Iryna Nikolaiev / Wim Zwijnenburg, "Risks and impacts from attacks on energy infrastructure in Ukraine," *PAX*, 2022, p. 4f.
- 124 Tony Lawrence, "Critical Energy Infrastructure: Lessons from Russia's War against Ukraine," in Jermalavičius, Tomas (ed.), *War and Energy Security: Lessons for the Future* (Tallinn: International Centre for Defence and Security ICDS, 2023), p. 42.
- 125 International Energy Agency IEA, "Ukraine Energy Profile," IEA, 2020, p. 18.
- 126 Thomas S. Popik, "Preserving Ukraine's Electric Grid During the Russian Invasion," *Journal of Critical Infrastructure Policy* 3:1 (2022), p. 19.
- 127 Ibid, p. 21.
- 128 Iryna Nikolaiev / Wim Zwijnenburg / Christina Parandii, "Risks and Impacts from Attacks on Fossil Fuel Facilities in Ukraine," *PAX*, 2023, p. 43f.
- 129 Oleksandr Sukhodolia, "Ukrainian Energy Sector under Military Attack: Lessons for Resilience," in Jermalavičius, Tomas (ed.), *War and Energy Security: Lessons for the Future* (Tallinn: International Centre for Defence and Security ICDS, 2023), p. 48f.
- 130 Iryna Nikolaiev / Wim Zwijnenburg / Christina Parandii, "Risks and Impacts from Attacks on Fossil Fuel Facilities in Ukraine," *PAX*, 2023, p. 5f.
- 131 International Energy Charter, "Ukrainian energy sector evaluation and damage assessment – II," *International Energy Charter*, 2022, p. 12.
- 132 Iryna Nikolaiev / Wim Zwijnenburg / Christina Parandii, "Risks and Impacts from Attacks on Fossil Fuel Facilities in Ukraine," *PAX*, 2023, p. 11.
- 133 Thomas S. Popik, "Preserving Ukraine's Electric Grid During the Russian Invasion," *Journal of Critical Infrastructure Policy* 3:1 (2022), p. 30.
- 134 International Energy Charter, "Ukrainian energy sector evaluation and damage assessment – XI," *International Energy Charter*, 2023, p. 17f.; Iryna Nikolaiev / Wim Zwijnenburg / Christina Parandii, "Risks and Impacts from Attacks on Fossil Fuel Facilities in Ukraine," *PAX*, 2023, p. 7.
- 135 International Energy Charter, "Ukrainian energy sector evaluation and damage assessment – II," *International Energy Charter*, 2022, p. 9f.
- 136 Thomas S. Popik, "Preserving Ukraine's Electric Grid During the Russian Invasion," *Journal of Critical Infrastructure Policy* 3:1 (2022), p. 28.
- 137 International Energy Charter, "Ukrainian energy sector evaluation and damage assessment – VIII," *International Energy Charter*, 2023, p. 13–15.
- 138 International Energy Charter, "Ukrainian energy sector evaluation and damage assessment – II," *International Energy Charter*, 2022, p. 4f.; Thomas S. Popik, "Preserving Ukraine's Electric Grid During the Russian Invasion," *Journal of Critical Infrastructure Policy* 3:1 (2022), p. 23f.
- 139 Centre for Information Resilience, "Weaponising Winter: The strategic shift in Russia's attacks on Ukraine's energy infrastructure," *Centre for Information Resilience*, 2023, p. 9.
- 140 Slawomir Matuszak, *On the verge of blackout: Ukraine facing attacks on its electricity generation system*, osw.waw.pl, 18.01.2023.
- 141 International Energy Charter, "Ukrainian energy sector evaluation and damage assessment – VIII," *International Energy Charter*, 2023, p. 4.
- 142 Andrian Prokip, *Ukrainian Energy During the War and Between the Winters*, wilsoncenter.org, 16.05.2023.
- 143 International Energy Charter, "Ukrainian energy sector evaluation and damage assessment – XI," *International Energy Charter*, 2023, p. 4f.
- 144 Andrian Prokip, *Ukrainian Energy During the War and Between the Winters*, wilsoncenter.org, 16.05.2023.
- 145 Oleksandr Sukhodolia, "Ukrainian Energy Sector under Military Attack: Lessons for Resilience," in Tomas Jermalavičius (ed.), *War and Energy Security: Lessons for the Future* (Tallinn: International Centre for Defence and Security ICDS, 2023), p. 47f.
- 146 Ibid, p. 58.

- 147 Thomas S. Popik, "Preserving Ukraine's Electric Grid During the Russian Invasion," *Journal of Critical Infrastructure Policy* 3:1 (2022), p. 19f.
- 148 Ibid, p. 32–35.
- 149 Andrian Prokip, *Ukrainian Energy During the War and Between the Winters*, wilsoncenter.org, 16.05.2023.
- 150 Oleksandr Sukhodolia, "Ukrainian Energy Sector under Military Attack: Lessons for Resilience," in Tomas Jermalavičius (ed.), *War and Energy Security: Lessons for the Future* (Tallinn: International Centre for Defence and Security ICDS, 2023), p. 47; Ministry of Energy of Ukraine, *Preparations for the heating season enter final stage, says Prime Minister*, kmu.gov.ua, 12.09.2023.
- 151 International Energy Agency IEA, "Ukraine Energy Profile," IEA, 2020, p. 24.
- 152 Verkhovna Rada of Ukraine, Проект Закону про критичну інфраструктуру, rada.gov.ua, 25.11.2021; Oleksandr Sukhodolia, "Ukrainian Energy Sector under Military Attack: Lessons for Resilience," in Tomas Jermalavičius (ed.), *War and Energy Security: Lessons for the Future* (Tallinn: International Centre for Defence and Security ICDS, 2023), p. 56f.
- 153 Roman Sviridovich, Створюємо штаб по реагуванню на пошкодження енергетичної інфраструктури, - Зеленський, censor.net, 13.09.2022.
- 154 Oleksandr Sukhodolia, "Ukrainian Energy Sector under Military Attack: Lessons for Resilience," in Tomas Jermalavičius (ed.), *War and Energy Security: Lessons for the Future* (Tallinn: International Centre for Defence and Security ICDS, 2023), p. 55.
- 155 Ibid, p. 56f.
- 156 Tony Lawrence, "Critical Energy Infrastructure: Lessons from Russia's War against Ukraine," in Tomas Jermalavičius (ed.), *War and Energy Security: Lessons for the Future* (Tallinn: International Centre for Defence and Security ICDS, 2023), p. 43.
- 157 Sophie Lambroschini, "How Do Ukrainian Networks Resist? Sources and Limits of Critical Infrastructure Resilience," *PONARS Eurasia Policy Memo* 816 (2022).
- 158 Ivo Mijnsen, "Will Ukraine's energy infrastructure hold up against Russian missile attacks?", *nzz.ch*, 20.11.2023.; Roman Olearchyk, "Ukraine braced for attacks on its power grid as winter draws in," *Financial Times*, 02.11.2023.; Mathias Hammer, "Ukraine Races to Protect its Energy System from Russia," *Times*, 15.11.2023.
- 159 Ibid.
- 160 Oleksandr Sukhodolia, "Ukrainian Energy Sector under Military Attack: Lessons for Resilience," in Tomas Jermalavičius (ed.), *War and Energy Security: Lessons for the Future* (Tallinn: International Centre for Defence and Security ICDS, 2023), p. 52f.
- 161 Interview with Ukrainian representatives in autumn 2023.
- 162 Sophie Lambroschini, "How Do Ukrainian Networks Resist? Sources and Limits of Critical Infrastructure Resilience," *PONARS Eurasia Policy Memo* 816 (2022).
- 163 Oleksandr Sukhodolia, "Ukrainian Energy Sector under Military Attack: Lessons for Resilience," in Tomas Jermalavičius (ed.), *War and Energy Security: Lessons for the Future* (Tallinn: International Centre for Defence and Security ICDS, 2023), p. 55f.
- 164 Ministry of Energy Ukraine, *High-Level International Energy Advisory Council addressed the provision of additional assistance to the Ukrainian energy sector*, kmu.gov.ua, 16.11.2022.
- 165 Slawomir Matuszak, *On the verge of blackout: Ukraine facing attacks on its electricity generation system*, osw.waw.pl, 18.01.2023.
- 166 Oleksandr Sukhodolia, "Ukrainian Energy Sector under Military Attack: Lessons for Resilience," in Tomas Jermalavičius (ed.), *War and Energy Security: Lessons for the Future* (Tallinn: International Centre for Defence and Security ICDS, 2023), p. 52, 54.
- 167 Slawomir Matuszak, *On the verge of blackout: Ukraine facing attacks on its electricity generation system*, osw.waw.pl, 18.01.2023.
- 168 Centre for Information Resilience, "Weaponising Winter: The strategic shift in Russia's attacks on Ukraine's energy infrastructure," *Centre for Information Resilience*, 2023, p. 7.
- 169 Slawomir Matuszak, *On the verge of blackout: Ukraine facing attacks on its electricity generation system*, osw.waw.pl, 18.01.2023.
- 170 Justin Ling, "Batteries are Ukraine's Secret Weapon Against Russia," *Wired*, 23.02.2023.
- 171 Oleksandr Sukhodolia, "Ukrainian Energy Sector under Military Attack: Lessons for Resilience," in Tomas Jermalavičius (ed.), *War and Energy Security: Lessons for the Future* (Tallinn: International Centre for Defence and Security ICDS, 2023), p. 59.
- 172 Slawomir Matuszak, *On the verge of blackout: Ukraine facing attacks on its electricity generation system*, osw.waw.pl, 18.01.2023.
- 173 Iryna Nikolaievy / Wim Zwiijnenburg, "Risks and impacts from attacks on energy infrastructure in Ukraine," *PAX*, 2022, p. 15.
- 174 Oleksandr Sukhodolia, "Ukrainian Energy Sector under Military Attack: Lessons for Resilience," in Tomas Jermalavičius (ed.), *War and Energy Security: Lessons for the Future* (Tallinn: International Centre for Defence and Security ICDS, 2023), p. 53f.
- 175 Interview with Ukrainian representatives in autumn 2023; Oleksii Romanov, "Empowering Ukraine – Small distribution generation and reforming the energy system of Ukraine," *Zentrum Liberale Moderne*, 2023; for more information on microgrids, see for example: Ganna Kostenko / Artur Zaporozhets, "Enhancing of the Power System Resilience Through the Application of Micro Power System (microgrids) with Renewable Distributed Generation," *System Research in Energy* 3:74 (2023), pp. 25–38.
- 176 Federal Office for Civil Protection FOCP, *Kritische Infrastrukturen*, babs.admin.ch, nd.
- 177 Federal Council, *Nationale Strategie zum Schutz kritischer Infrastrukturen Ganzheitlicher Ansatz zur Sicherstellung der Verfügbarkeit von essenziellen Gütern und Dienstleistungen*, fedlex.admin.ch, 2023.
- 178 European Parliament / Council of the European Union, *Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC*, eur-lex.europa.eu.; European Commission / Directorate-General for Migration and Home Affairs, *COMMISSION DELEGATED REGULATION (EU) of 25.07.2023 supplementing Directive (EU) 2022/2557 of the European Parliament and of the Council by establishing a list of essential services*, eur-lex.europa.eu, 2023.
- 179 EU-NATO Task Force on the Resilience of Critical Infrastructure, "Final Assessment Report," NATO, 2023.; NATO, *Resilience, civil preparedness and Article 3*, nato.int, 02.08.2023.
- 180 Verkhovna Rada of Ukraine, Деякі питання об'єктів критичної інфраструктури, rada.gov.ua, 09.10.2020.; Verkhovna Rada of Ukraine, Проект Закону про критичну інфраструктуру: Стаття 9. Сектори критичної інфраструктури, rada.gov.ua, 25.11.2021.
- 181 Ministry of Infrastructure, *National Transport Strategy of Ukraine 2030*, mtu.gov.ua, 25.05.2018.
- 182 Iryna Kosse, "Rebuilding Ukraine's Infrastructure after the War," *The Vienna Institute for International Economic Studies*, 2023.
- 183 President of Ukraine, Стратегія національної безпеки України: БЕЗПЕКА ЛЮДИНИ - БЕЗПЕКА КРАЇНИ, rada.gov.ua, 14.09.2020.
- 184 Ministry of Infrastructure, *National Transport Strategy of Ukraine 2030*, mtu.gov.ua, 25.05.2018.; Volodymyr Bilotkach / Marc Ivaldi, "Rebuilding Ukrainian transport infrastructure," in: Yuriy Gorodnichenko et al. (eds.), *Rebuilding Ukraine: Principles and policies* (London and Paris: CERP Press, 2022), pp. 215–239.
- 185 Ministry for Restoration, *Ukrainian Railway Statistics*, mtu.gov.ua, 07.11.2023.
- 186 Stanislav Zinchenko, *Resilience lessons: How iron & steel industry of Ukraine cope with logistic challenges*, gmk.center, 27.04.2023.
- 187 Денис Кацило, "Неефективна «Укрзалізниця» перетворилася на машину з порятунку мільйонів українців. Як компанію переставили на воєнні рейки," *Forbes UA*, 04.04.2022.
- 188 Volodymyr Bilotkach / Marc Ivaldi, "Rebuilding Ukrainian transport infrastructure," in: Yuriy Gorodnichenko et al. (eds.), *Rebuilding Ukraine: Principles and policies* (London and Paris: CERP Press, 2022), pp. 215–239.
- 189 Ministry of Infrastructure, *National Transport Strategy of Ukraine 2030*, mtu.gov.ua, 25.05.2018.; Sarah A. Topol, "Ukraine's 15,000-Mile Lifeline," *The New York Times Magazine*, 15.11.2022.
- 190 Alan Chln, "How Ukraine's Trains Are Adapting to War," *Foreign Policy*, 27.08.2023.
- 191 USPA, ПРО ПІДПРИЄМСТВО, uspa.gov.ua, nd.; Verkhovna Rada of Ukraine, Про морські порти України, rada.gov.ua, 01.01.2022.; Monika Kiss, "Russia's war on Ukraine: Implications for transport," *European Parliamentary Research Service*, 2022.
- 192 USPA, *Register of Seaports of Ukraine*, uspa.gov.ua, nd.
- 193 Ukrainian Sea Ports Authority, *linkedin.com*, nd.
- 194 Yuriy Grigorenko, *The bottleneck: why Danube ports cannot save Ukrainian exports*, gmk.center, 12.07.2022.
- 195 Iryna Kosse, "Rebuilding Ukraine's Infrastructure after the War," *The Vienna Institute for International Economic Studies*, 2023.
- 196 Logistics Cluster, *Ukraine Aviation*, logcluster.org, nd.
- 197 Monika Kiss, "Russia's war on Ukraine: Implications for transport," *European Parliamentary Research Service*, 2022.
- 198 Volodymyr Bilotkach / Marc Ivaldi, "Rebuilding Ukrainian transport infrastructure," in: Yuriy Gorodnichenko et al. (eds.), *Rebuilding Ukraine: Principles and policies* (London and Paris: CERP Press, 2022), pp. 236–260.

- 199 Ministry for Communities, Territories and Infrastructure Development of Ukraine (Ministry of Infrastructure), Пріоритети діяльності Державного агентства автомобільних доріг України (Укравтодору) на 2021–2023 роки, mtu.gov.ua, 27.05.2021.; State Statistics Service of Ukraine, «Statistical Yearbook of Ukraine 2021», *State Statistics Service of Ukraine*, 2022.
- 200 Ministry of Restoration, Technical condition of general-purpose roads, mtu.gov.ua, 07.11.2023.
- 201 OECD, “Transport infrastructure trends and regional development,” in OECD (ed.), *Transport Bridging Divides* (Paris: OECD Publishing, 2020).
- 202 Iryna Kosse, “Rebuilding Ukraine’s Infrastructure after the War,” *The Vienna Institute for International Economic Studies*, 2023.
- 203 Ministry of Infrastructure, *Priorities of the State Highway Agency of Ukraine (Ukravtodor) for 2021–2023*, mtu.gov.ua, 07.11.2023.
- 204 Mari Eccles, “Prepare for takeoff...soon: Kyiv airport readies for post-war flights,” *POLITICO*, 18.10.2023.; International Transport Forum, “Transport Policy Responses to the War in Ukraine, No. 3,” *International Transport Forum*, 2022.
- 205 Romina Bandura / Janina Staguhn / Benjamin Jensen, “Modernizing Ukraine’s Transport and Logistics Infrastructure,” *Center for Strategic & International Studies*, 2022.; Pavel Polityuk, “Ukraine say its Black Sea grain corridor is working,” *Reuters*, 26.10.2023.; Dennis Koegeboehn, *Impacts of the Russia-Ukraine War on Ports and Transport*, tocevents-europe.com, nd.
- 206 Caitlin Welch et al., *Spotlight on Damage to Ukraine’s Agricultural Infrastructure since Russia’s Invasion*, csis.org, 15.06.2022.
- 207 United Nations Ukraine, *There has been almost one attack every other day hitting vital port and grain facilities in Ukraine*, ukraine.un.org, 13.09.2023.; Vadim Kolisnichenko, *Danube ports operation is limited due to the shelling and shelling of the Russian Federation*, gmcenter.org, 01.08.2023.
- 208 Sophie Lambroschini, “How Do Ukrainian Networks Resist? Sources and Limits of Critical Infrastructure Resilience,” *PONARS Eurasia Policy Memo* 816 (2022).
- 209 Lorenzo Tondo / Pjotr Sauer, “Russia bombs five railway stations in central and western Ukraine,” *The Guardian*, 25.04.2022.
- 210 Kyiv School of Economics, “Report on damages and losses to infrastructure from the destruction caused by Russia’s military aggression against Ukraine as of June 2023,” *Damaged in Ua*, 2023, pp. 22–28.
- 211 Romina Bandura / Janina Staguhn / Benjamin Jensen, “Modernizing Ukraine’s Transport and Logistics Infrastructure,” *Center for Strategic & International Studies*, 2022.
- 212 Kyiv School of Economics, “Report on damages and losses to infrastructure from the destruction caused by Russia’s military aggression against Ukraine as of June 2023,” *Damaged in Ua*, 2023, pp. 22–28.
- 213 Alex Horton / Anastacia Galouchka, “Defending Ukraine’s ‘highway of life’ – the last road out of Bakhmut,” in: *The Washington Post*, 12.03.2023.
- 214 Kyiv School of Economics, “Report on damages and losses to infrastructure from the destruction caused by Russia’s military aggression against Ukraine as of June 2023,” *Damaged in Ua*, 2023, pp. 22–28.
- 215 Florence Aubenas, “Ukraine’s rail battle: ‘Our tanks go in first, then our trains,’” *Le Monde*, 07.11.2023.
- 216 Sarah Topol, “Ukraine’s 15,000-Mile Lifeline,” *The New York Times Magazine*, 07.11.2023.
- 217 Alexander Kamyshin, *Twitter*, twitter.com, 06.11.2022.; Esther Geerts, “The plan B to keep trains running in Ukraine: diesel and ... steam locomotives?,” in: *RailTech*, 11.11.2022.
- 218 Mari Eccles, “Prepare for takeoff...soon: Kyiv airport readies for post-war flights,” *POLITICO*, 18.10.2023.; International Transport Forum, “Transport Policy Responses to the War in Ukraine, No. 3,” *International Transport Forum*, 2022.
- 219 VisitUkraine, *Boryspil Airport is already preparing to resume flights: what is known*, visitukraine.today, nd.; Mari Eccles, “Prepare for takeoff...soon: Kyiv airport readies for post-war flights,” *POLITICO*, 18.10.2023.; International Transport Forum, “Transport Policy Responses to the War in Ukraine, No. 3,” *International Transport Forum*, 2022.
- 220 Yuriy Grigorenko, *The bottleneck: why Danube ports cannot save Ukrainian exports*, gmcenter.org, 07.11.2023.
- 221 Ekaterina Bouckley / Nikolaos Aidinis Antonopoulos, “Ukraine grains exporters turn to Danube ports, heating competition with iron ore, steel shipments,” *S&P Global*, 2023.; Emma Graham-Harrison, “‘The war had come to us too’: how Ukraine’s Danube ports became vital hubs – and targets,” *The Guardian*, 09.11.2023.; Stanislav Zinchenko, *Resilience lessons: How iron & steel industry of Ukraine cope with logistic challenges*, gmcenter.org, 27.04.2023.
- 222 EU-NATO Task Force on the Resilience of Critical Infrastructure, “Final Assessment Report,” NATO, 2023, p. 6.
- 223 Stanislav Zinchenko, *Resilience lessons: How iron & steel industry of Ukraine cope with logistic challenges*, gmcenter.org, 07.11.2023.
- 224 Андрій Швадчак, *The day has come – Ukraine sells port*, ti-ukraine.org, 17.01.2023.
- 225 Caitlin Welch et al., *Spotlight on Damage to Ukraine’s Agricultural Infrastructure since Russia’s Invasion*, csis.org, 15.06.2022.
- 226 United Nations, *Black Sea Grain Initiative Joint Coordination Centre – Live data*, un.org, nd.
- 227 United Nations Secretary General, *Secretary-General’s press encounter on the Black Sea Initiative*, un.org, 17.07.2023.; Al Jazeera, “Russia sends first free grain to Africa since end of Black Sea deal,” aljazeera.com, 17.11.2023.; Norwegian Maritime Authority, *The Black Sea and the Sea of Azov*, sdir.no, 10.10.2023.
- 228 Sarah A. Topol, “Ukraine’s 15,000-Mile Lifeline,” *The New York Times Magazine*, 15.11.2022.; Lesya Kharachenko, *Kamyshin: Leading Ukraine’s Iron Diplomacy*, iwpr.net, 22.02.2023.; Ukrposhta, *Ukrposhta and Ukrzaliznytsia delivered 2 million parcels by rail mail*, ukrposhta.ua, 18.07.2022.; Centre for Transport Strategies, *Ukrzaliznytsia Boasts 97% Train Departure Punctuality Rate*, en.cfts.org.ua, 18.01.2023.
- 229 Денис Каціло, “Неефективна «Укрзалізниця» перетворилася на машину з порятунку мільйонів українців. Як компанію переставили на воєнні рейки,” *Forbes UA*, 04.04.2022.
- 230 Amrop, *Sustainable Success Stories: Interview with Jakub Karnowski, Ukrainian Railways*, amrop.com, nd.
- 231 World Bank Group / Government of Ukraine / European Commission, *Ukraine Rapid Damage and Needs Assessment: February 2022 – February 2023 (English)* (Washington, D.C.: World Bank Group, 2023.); Oleksiy Sorokin, “Ukrzaliznytsia can modernize by looking at how others did it,” *Kyiv Post*, 02.07.2019.; Amrop, *Sustainable Success Stories: Interview with Jakub Karnowski, Ukrainian Railways*, amrop.com, nd.; Ukrzaliznytsia, *Укрзалізниця нарощує обсяги оновлення та ремонту колійної інфраструктури*, uz.gov.ua, 25.09.2023.
- 232 TSN, *Укрзалізниця шукає волонтерів на вокзалах: що треба робити*, tsn.ua, 03.03.2022.; Sophie Lambroschini, “How Do Ukrainian Networks Resist? Sources and Limits of Critical Infrastructure Resilience,” *PONARS Eurasia Policy Memo* 816 (2022).
- 233 Денис Каціло, “Неефективна «Укрзалізниця» перетворилася на машину з порятунку мільйонів українців. Як компанію переставили на воєнні рейки,” *Forbes UA*, 04.04.2022.
- 234 Ibid.
- 235 Sarah Topol, “Ukraine’s 15,000-Mile Lifeline,” *The New York Times Magazine*, 07.11.2023.
- 236 Marco Raimondi, *Ukrainian Railways: ‘in-house production can also serve EU integration’*, railfreight.com, 07.08.2023.
- 237 Isobel Koshiw / Lisa O’Carroll, “Kyiv transport app is transformed into life-saving war information tool,” *The Guardian*, 15.03.2022.; Ukrzaliznytsia, *Укрзалізниця разом з Міністерством цифрової трансформації та Офісом Президента України запускає проект ‘Там, де вас чекають’*, t.me, 02.05.2022.; ОФІС ПРЕЗИДЕНТА УКРАЇНИ, *ТАМ, ДЕ ВАС ЧЕКАЮТЬ*, book-ing.help.gov.ua, nd.
- 238 Red Cross, *ПЕРЕДАЧА ГЕНЕРАТОРІВ УКРЗАЛІЗНИЦІ*, redcross.org.ua, 25.10.2022.
- 239 Vanora Bennett, *EBRD supports Ukraine rail company UkrZaliznytsya*, ebrd.com, 10.06.2022.
- 240 European Union, “EU-Ukraine Solidarity Lanes,” *European Union*, September 2023.
- 241 Cabinet of Ministers of Ukraine, *Order on the Establishment of a Commission to Inspect the Condition of Bridge Structures*, zakon.rada.gov.ua, 07.11.2023.
- 242 Andriy Ivko, *Road vs. War: How Ukravtodor restores destroyed bridges and roads*, mind.ua, 02.12.2022.
- 243 Ministry of Infrastructure of Ukraine, “Rebuild Ukraine: Challenges and Opportunities for the Infrastructure,” *Ukraine Recovery Conference*, 2022.
- 244 European Commission, *Airline slots: Commission proposes more flexible exceptions regime and targeted relief to airlines*, ec.europa.eu, 12.07.2022.; Airports Council International, *Urgent and longer-term support needed for Ukrainian airports*, aci-europe.org, 14.09.2023.; Ministry of Infrastructure of Ukraine, “Rebuild Ukraine: Challenges and Opportunities for the Infrastructure,” *Ukraine Recovery Conference*, 2022.
- 245 Railway Gazette International, *Ukrainian standard gauge railway plan*, railwaygazette.com, 27.05.2022.
- 246 Andriy Ivko, *Roads vs War: How Ukravtodor restores destroyed bridges and roads*, mind.ua, 02.11.2022.
- 247 Ministry of Finance of Ukraine, *EBRD will provide EUR 182 million for road modernization in Ukraine to improve transport links between Ukraine and the EU*, kmu.gov.ua, 05.09.2023.

- 248 Ali Kharrazi et al., "Redundancy, Diversity, and Modularity in Network Resilience: Applications for International Trade and Implications for Public Policy", *Current Research in Environmental Sustainability* 2 (2020).
- 249 Federal Office for Civil Protection FOCF, *Kritische Infrastrukturen*, [babs.admin.ch](https://www.babs.admin.ch), nd.
- 250 Federal Council, *Nationale Strategie zum Schutz kritischer Infrastrukturen Ganzheitlicher Ansatz zur Sicherstellung der Verfügbarkeit von essenziellen Gütern und Dienstleistungen*, [fedlex.admin.ch](https://www.fedlex.admin.ch), 2023.
- 251 European Parliament / Council of the European Union, *Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC*, eur-lex.europa.eu; European Parliament / Council of the European Union, *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)*, eur-lex.europa.eu.
- 252 EU-NATO Task Force on the Resilience of Critical Infrastructure, "Final Assessment Report", NATO, 2023.
- 253 NATO, *Resilience, civil preparedness and Article 3*, [nato.int](https://www.nato.int), 02.08.2023.
- 254 Verkhovna Rada of Ukraine, Проект Закону про критичну інфраструктуру, rada.gov.ua, 2021.
- 255 Augusten D. Givens / Max Gorbachevsky / Anita C. Biernat, "How Putin's Cyberwar Failed in Ukraine", *Journal of Strategic Security* 16:2 (2023), pp. 96–121.
- 256 Grace B. Mueller et al., "Cyber Operations during the Russo-Ukrainian War", *Center for Strategic and International Studies*, 2023.; Matthias Schulze / Mika Kerttunen, "Cyber Operations in Russia's War against Ukraine", *Stiftung Wissenschaft und Politik*, 2023.; Marcus Willett, "The Cyber Dimension of the Russia-Ukraine War", *Survival* 64:5 (2022), pp. 7–26.; Andy Greenberg, "Russia's Cyberwar on Ukraine Is a Blueprint for What's to Come", *Wired*, 20.06.2017.
- 257 Viktoriia Omelianenko et al., "Ukraine Digital Development Country Profile", *International Telecommunication Union*, 2023, p. 17.
- 258 Ibid.
- 259 Anna Gross, "Russian forces usurp Ukrainian internet infrastructure in Donbas", *Financial Times*, 05.05.2022.; Pete Bell, *Ukraine's Telecom Market, Explained*, telegeography.com, 23.03.2022.; Tim Strong, *What to Know About Fiber's Role in Ukraine's Information War*, telegeography.com, 01.03.2022.; Emile Aben, *The Resilience of the Internet in Ukraine*, labs.ripe.net, 10.03.2022.
- 260 IT Ukraine Association / Top Lead LLC, "Do IT Like Ukraine", *IT Ukraine Association*, 2022.
- 261 Wavestone, "Digital Public Administration factsheet 2022: Ukraine", *European Commission (DG DIGIT and DG CONNECT)*, 2022.
- 262 BBC, *Ukraine media guide*, [bbc.com](https://www.bbc.com), 21.06.2023.; Andrii Ianitskyi, *Ukraine, medialandscapes.org*, nd.; Yanina Shabanova, *How the Ukrainian media landscape has changed after February 24?*, betterplace-lab.org, 21.11.2022.
- 263 Maggie Miller, "Ukraine's largest telecom stands against Russian cyber-attacks", *Politico*, 07.09.2022.
- 264 Aviv Itzhak / Ur. Fer, "Russian-Ukraine armed conflict: Lessons learned on the digital ecosystem", *International Journal of Critical Infrastructure Protection* 43 (2023).
- 265 Ministry of Digital Transformation of Ukraine, Застосунок «Повітряна тривога», який завантажили 11 млн разів, попереджатиме про хімічну та радіаційну небезпеку, thedigital.gov.ua, 02.12.2022.; Nino Kubinidze et al., "Interim assessment on damages to telecommunication infrastructure and resilience of the ICT ecosystem in Ukraine", *International Telecommunication Union*, December 2022, pp. 34.
- 266 CyberPeace Institute, *Case Study Viasat, cyberconflicts.cyberpeaceinstitute.org*, 2022.; John Thornhill, "A global satellite blackout is a real threat – can hackers help?", *Financial Times*, 08.06.2022.; Christoph Bing / Raphael Satter, "Ukrainian telecom company's internet service disrupted by 'powerful' cyberattack", *Reuters*, 28.03.2022.
- 267 World Bank Group / Government of Ukraine / European Commission, *Ukraine Rapid Damage and Needs Assessment: February 2022 – February 2023 (English)* (Washington, D.C.: World Bank Group, 2023), pp. 95–97.
- 268 Nino Kubinidze et al., "Interim assessment on damages to telecommunication infrastructure and resilience of the ICT ecosystem in Ukraine", *International Telecommunication Union*, December 2022, p. 24.; Emile Aben, *The Resilience of the Internet in Ukraine*, labs.ripe.net, 10.03.2022.
- 269 William Mauldin, "Russian Strikes Sap Ukraine Mobile Network of Vital Power", *The Wall Street Journal*, 15.01.2023.
- 270 Vera Bergengruen, "The Battle for Control Over Ukraine's Internet", *Time*, 18.10.2022.
- 271 Tetyana Lokot, "Russia's Networked Authoritarianism in Ukraine's Occupied Territories during the Full-Scale Invasion: Control and Resilience", *LSE Public Policy Review* 3:1 (2023); Adam Satariano / Scott Reinhard, "How Russia Took Over Ukraine's Internet in Occupied Territories", *The New York Times*, 09.08.2022.; Vera Bergengruen, "The Battle for Control Over Ukraine's Internet", *Time*, 18.10.2022.
- 272 Vera Bergengruen, "The Battle for Control Over Ukraine's Internet", *Time*, 18.10.2022.
- 273 Catherine Stupp, "Ukraine Has Begun Moving Sensitive Data Outside Its Borders", *The Wallstreet Journal*, 14.06.2022.
- 274 IT Ukraine Association / Top Lead LLC, "Do IT Like Ukraine", *IT Ukraine Association*, 2022.
- 275 Forensic Architects, *Russian Strike on the Kyiv TV Tower*, forensic-architecture.org, 10.06.2022.; Vera Bergengruen, "The Battle for Control Over Ukraine's Internet", *Time*, 18.10.2022.
- 276 Gulsanna Mamedieva / Donald Moynihan, "Digital Resilience in War-time: The Case of Ukraine", *Public Administration Review* (2023); Emile Aben, *The Resilience of the Internet in Ukraine – One Year On*, labs.ripe.net, 14.04.2023.
- 277 Nino Kubinidze et al., "Interim assessment on damages to telecommunication infrastructure and resilience of the ICT ecosystem in Ukraine", *International Telecommunication Union*, December 2022, pp. 32–41.; Viktoriia Omelianenko et al., "Ukraine Digital Development Country Profile", *International Telecommunication Union*, 2023.
- 278 Aviv Itzhak / Ur. Fer, "Russian-Ukraine armed conflict: Lessons learned on the digital ecosystem", *International Journal of Critical Infrastructure Protection* 43 (2023); Emma Schroeder / Sean Dack, "A parallel terrain: Public-private defense of the Ukrainian information environment", *Atlantic Council*, 2023.
- 279 IT Ukraine Association / Top Lead LLC, "Do IT Like Ukraine", *IT Ukraine Association*, 2022.
- 280 Anna Gross, "Russian forces usurp Ukrainian internet infrastructure in Donbas", *Financial Times*, 05.05.2022.
- 281 Emma Schroeder / Sean Dack, "A parallel terrain: Public-private defense of the Ukrainian information environment", *Atlantic Council*, 2023, p. 13.
- 282 Anastasia Zanuda, "Як вдалось зберегти зв'язок та інтернет в Україні під час війни", *BBC News Ukraine*, 16.04.2022.
- 283 Ukrinform, *Ukraine's air defenses to focus on protecting critical infrastructure – spox*, ukrinform.net, 08.10.2023.; Karen DeYoung / Alex Horton / Serhiy Morgunov, "Leaked documents warn of weaknesses in Ukraine's defenses", *The Washington Post*, 08.04.2023.; Alex Horton et al., "These are the Western air defense systems protecting Ukraine", *The Washington Post*, 19.05.2023.
- 284 Nino Kubinidze et al., "Interim assessment on damages to telecommunication infrastructure and resilience of the ICT ecosystem in Ukraine", *International Telecommunication Union*, December 2022, pp. 34.; Vector, Мобільний зв'язок під час війни. Як lifecell під обстрілами ремонтує базові станції, vctr.media, 24.04.2022.
- 285 Vector, Мобільний зв'язок під час війни. Як lifecell під обстрілами ремонтує базові станції, vctr.media, 24.04.2022.; Nino Kubinidze et al., "Interim assessment on damages to telecommunication infrastructure and resilience of the ICT ecosystem in Ukraine", *International Telecommunication Union*, December 2022, p. 38.
- 286 Vera Bergengruen, "The Battle for Control Over Ukraine's Internet", *Time*, 18.10.2022.
- 287 Brad Smith, *Extending our vital technology support for Ukraine*, blogs.microsoft.com, 03.11.2022.
- 288 Emma Schroeder / Sean Dack, "A parallel terrain: Public-private defense of the Ukrainian information environment", *Atlantic Council*, 2023, pp. 14–15.; Catherine Stupp, "Ukraine Has Begun Moving Sensitive Data Outside Its Borders", *The Wall Street Journal*, 14.06.2022.
- 289 Isabel Schmidt / Avery Parsons Grayson / Mayesha Alam, "Cross-Cutting Responses to Strengthen Ukraine's Digital Resilience", *Digital Front Lines*, 28.06.2023.; Nick Beecroft, "Evaluating the International Support to Ukrainian Cyber Defense", *Carnegie Endowment for International Peace*, 03.11.2022.
- 290 Verkhovna Rada of Ukraine, Деякі питання оперативно-технічного управління телекомунікаційними мережами в умовах надзвичайних ситуацій, надзвичайного та воєнного стану, rada.gov.ua, 06.02.2019.
- 291 Adam Satariano et al., "With Starlink, Elon Musk's Satellite Dominance Is Raising Global Alarms", *The New York Times*, 28.07.2023.; Tom Simonite, "How Starlink Scrambled to Keep Ukraine Online", *Wired*, 11.05.2022.; Emma Schroeder / Sean Dack, "A parallel terrain: Public-private defense of the Ukrainian information environment", *Atlantic Council*, 2023, pp. 16–18.; Nino Kubinidze et al., "Interim assessment on damages to telecommunication infrastructure and resilience of the ICT ecosystem in Ukraine", *International Telecommunication Union*, December 2022, p. 39.

- 292 Vector, Мобільний зв'язок під час війни. Як lifecell під обстрілами ремонтує базові станції, [vctr.media](#), 24.04.2022.; Tim Strong, *What to Know about Fiber's Role in Ukraine's Information War*, [telegeography.com](#), 01.03.2022.; Viktoriia Omelianenko et al., "Ukraine Digital Development Country Profile," *International Telecommunication Union*, 2023.
- 293 Денис Каціло, "How Ukrzaliznytsia works during the war and evacuates Ukrainians. The history of the reformatting of railway companies is," *Forbes UA*, 04.04.2022.
- 294 Maywell Strachan, "DIY Volunteers Are Repairing Ukraine's Destroyed Internet Infrastructure," *Vice*, 23.03.2022.
- 295 State Service of Special Communications and Information Protection of Ukraine, Рішення НКЕК від 24.02.2022 № 3 Про схвалення тимчасового Порядку користування радіочастотним спектром спеціальними та загальними користувачами в особливий період та в умовах надзвичайного або воєнного стану, [nkrzi.gov.ua](#), nd.
- 296 State Service of Special Communications and Information Protection of Ukraine, *Implementation of the roaming within Ukraine is another important step that was made for securing communication at the beginning of Russia's full-scale invasion into Ukraine*, [cip.gov.ua](#), 02.04.2022.; National Commission for the State Regulation of Electronic Communications, Radio Frequency and Provision of Postal Services, Щодо внутрішнього роумінгу на території України, [nkrzi.gov.ua](#), nd.; Nino Kubinidze et al., "Interim assessment on damages to telecommunication infrastructure and resilience of the ICT ecosystem in Ukraine," *International Telecommunication Union*, December 2022, pp. 34–35.; Thomas Brewster, "Ukraine's Engineers Battle To Keep The Internet Running While Russian Bombs Fall Around Them," *Forbes*, 22.03.2022.
- 297 Nino Kubinidze et al., "Interim assessment on damages to telecommunication infrastructure and resilience of the ICT ecosystem in Ukraine," *International Telecommunication Union*, December 2022, pp. 39–41.; Amreesh Phokeer, *Case Study: Ukraine – A Role Model for Internet Resilience*, [internetsociety.org](#), 24.02.2023.
- 298 European Commission, *Joint Statement by EU and Ukrainian operators to help refugees from Ukraine stay connected*, [europa.eu](#), 05.04.2022.
- 299 Nino Kubinidze et al., "Interim assessment on damages to telecommunication infrastructure and resilience of the ICT ecosystem in Ukraine," *International Telecommunication Union*, December 2022, p. 37.
- 300 State Service of Special Communications and Information Protection of Ukraine, На період воєнного стану скасовується плата за доступ до елементів інфраструктури об'єктів електроенергетики (оновлено), [nkrzi.gov.ua](#), nd.
- 301 Justin Ling, "Batteries Are Ukraine's Secret Weapon Against Russia," *Wired*, 23.02.2023.; William Mauldin, "Russian Strikes Sap Ukraine Mobile Network of Vital Power," *The Wall Street Journal*, 15.01.2023.
- 302 IT Ukraine Association / Top Lead LLC, "Do IT Like Ukraine," *IT Ukraine Association*, 2022.
- 303 Stephanie Overby, *Ukraine IT's unparalleled resilience*, [cio.com](#), 27.02.2023.; Mary K. Pratt, *Working from a war zone: Ukrainian IT pros share their experiences*, [cio.com](#), 29.03.2022.
- 304 Yana Lyushnevskaya, "Analysis: Ukraine media maintain resilience amid tumultuous year," *BBC*, 09.12.2022.; InMind, "Ukrainian media use and trust in 2022," *USAID / Internews*, 2022.
- 305 Nino Kubinidze et al., "Interim assessment on damages to telecommunication infrastructure and resilience of the ICT ecosystem in Ukraine," *International Telecommunication Union*, December 2022, p. 37.
- 306 Matthias Williams, "Citing martial law, Ukraine president signs decree to combine national TV channels into one platform," *Reuters*, 20.03.2022.
- 307 Yana Lyushnevskaya, "Analysis: Ukraine's wartime TV marathon stokes media freedom fears," *BBC*, 28.04.2022.; Information Defence Hub, "War in Ukraine: Lessons identified and learned," *European Values Center for Security Policy*, 2023, pp. 36–38.
- 308 Ibid.
- 309 ЄВГЕНІЯ ПІДГАЙНА, "Інтернет-провайтери під час війни: «Безліч пошкоджень, відновлюємо мережі 24/7, тарифи не підвищуємо», *Mind*, 12.04.2022.
- 310 Thomas Brewster, "Ukraine's Engineers Battle To Keep The Internet Running While Russian Bombs Fall Around Them," *Forbes*, 22.03.2022.
- 311 Kyivstar, Київстар виділяє 300 мільйонів гривень для відновлення цифрової інфраструктури України, [kyivstar.ua](#), 04.07.2022.; Thomas Seal, "Ukrainian Telecom Giant to Rebuild With Chinese Kit for Now," *Bloomberg*, 21.06.2023.
- 312 IT Ukraine Association / Top Lead LLC, "Do IT Like Ukraine," *IT Ukraine Association*, 2022.
- 313 Ibid.
- 314 Vector, Мобільний зв'язок під час війни. Як lifecell під обстрілами ремонтує базові станції, [vctr.media](#), 24.04.2022.
- 315 IT Ukraine Association / Top Lead LLC, "Do IT Like Ukraine," *IT Ukraine Association*, 2022.
- 316 Vector, Міністр цифрової трансформації підписав лист, який закликає не мобілізувати IT-фахівців до лав ЗСУ, [vctr.media](#), 14.03.2022.
- 317 Nino Kubinidze et al., "Interim assessment on damages to telecommunication infrastructure and resilience of the ICT ecosystem in Ukraine," *International Telecommunication Union*, December 2022, p. 30.; IT Ukraine Association / Top Lead LLC, "Do IT Like Ukraine," *IT Ukraine Association*, 2022.; Romina Bandura / Janina Staguhn / Madeleine McLean, "Rebuilding and Modernizing Ukraine's ICT Infrastructure Will Be Essential to Attract Private Investment," *Center for Strategic & International Studies*, 02.10.2023.



The **Center for Security Studies (CSS) at ETH Zürich** is a center of competence for Swiss and international security policy. It offers security policy expertise in research, teaching and consulting. The CSS promotes understanding of security policy challenges as a contribution to a more peaceful world. Its work is independent, practice-relevant, and based on a sound academic footing.