Fear, Uncertainty, and Dread: Cognitive Heuristics and Cyber Threats

Journal Article

Author(s):
Gomez, Miguel Alberto; Villar, Eula B.

Publication date:
2018

Permanent link:
https://doi.org/10.3929/ethz-b-000264912

Originally published in:
Politics and Governance 6(2), https://doi.org/10.17645/pag.v6i2.1279

Politics and Governance (ISSN: 2183–2463)
2018, Volume 6, Issue 2, Pages 61–72
DOI: 10.17645/pag.v6i2.1279

Article

Fear, Uncertainty, and Dread: Cognitive Heuristics and Cyber Threats

Miguel Alberto Gomez [1,*] and Eula Bianca Villar [2]

[1] Center for Security Studies, ETH Zurich, 8092 Zurich, Switzerland; E-Mail: miguel.gomez@sipo.gess.ethz.ch
[2] Department of Business and Technology, La Salle Universitat Ramon Llull, 08022 Barcelona, Spain; E-Mail: ebvillar@salleurl.edu

* Corresponding author

Submitted: 22 November 2017 | Accepted: 7 March 2018 | Published: 11 June 2018

Abstract
Advances in cyber capabilities continue to cause apprehension among the public. With states engaging in cyber operations in pursuit of its perceived strategic utility, it is unsurprising that images of a "Cyber Pearl Harbor" remain appealing. It is crucial to note, however, that the offensive action in cyberspace has only had limited success over the past decade. It is estimated that less than 5% of these have achieved their stated political or strategic objectives. Moreover, only five states are thought to have the capabilities to inflict or threaten substantial damage. Consequently, this raises the question of what accounts for the continued sense of dread in cyberspace. The article posits that this dread results from the inappropriate use of cognitive shortcuts or heuristics. The findings herein suggest that the lack of experience in dealing with cyber operations encourages uncertainty, which motivates decision-makers to base their judgements on pre-existing, and possibly incorrect, conceptions of cyberspace. In response, the article segues into potential solutions that can mitigate unsubstantiated dread towards cyberspace by peering into the role that attributes at the organizational level can play in tempering the position of individuals. The suggested considerations are rooted in the interactions between the micro and macro level processes in forming judgments, sensemaking, and ultimately, mobilizing actions.

Keywords
cybersecurity; cyber threats; dread; experiment; heuristics

Issue
This article is part of the issue "Global Cybersecurity: New Directions in Theory and Methods", edited by Tim Stevens (King's College London, UK).

1. Introduction

On Friday, May 12, 2017, the United Kingdom's National Health Service (NHS), Spain's Telefonica, and other entities were incapacitated by the WannaCry malware which infected over 200,000 computers in nearly 150 countries (R. Goldman, 2017). In 2001, Code Red exploited vulnerabilities leading to the infection of over 300,000 computers (Perrone, 2001). In 2003, Slammer initiated a denial-of-service attack and stalled Internet traffic while compromising approximately 75,000 computers within ten minutes (Boutin, 2003). These events reinforce negative perceptions towards cyber threats, yet overstate the scope of the problem. Anderson et al. (2013) note that the actual cost of cybercrime is much lower than that reported by the private sector or the media. Expounding on this argument, Jardine (2015, 2017) notes that malicious activity in cyberspace is far less likely to occur when viewed relative to the growth of the domain and when vulnerable actors are disaggregated and studied in isolation. More closely related to this article, Maness and Valeriano's (2016) study highlights that out of 68 states with cybersecurity programs, only five (5) demonstrated the capability to inflict noteworthy damage. Furthermore, less than 5% of these operations have resulted in behavioural changes on the part of the target as intended by the aggressor. Consequently, this raises the question as to why dread continues to persist as a re-

sponse to cyber operations (Jarvis, Macdonald, & Whiting, 2017).

Dread is defined in this article as the apprehension of the negative consequences of an event. This perception of dread in cyberspace is often attributed to increasing technological dependence and the strategic exploitation by state actors. The literature analyses this phenomenon mainly through the lens of rational choice theory, while underemphasizing individual cognitive processes (Dean & McDermott, 2017; Edwards, Furnas, Forrest, & Axelrod, 2017; Gartzke & Lindsay, 2015). Consequently, this article explores dread in response to cyber operations as a reflection of heuristic usage resulting in sub-optimal judgements.

Using two vignette survey experiments, it forwards three main arguments. First, the lack of experience and the novelty of this threat generates an environment of uncertainty with respect to cyber operations (Gigerenzer, 2008; Hafenbradl, Waeger, Marewski, & Gigerenzer, 2016; Kruglanski, Orehek, Dechesne, & Pierro, 2010). Second, judgmental errors that facilitate elevated levels of dread are not suggestive of irrationality but rather stem from the use of inappropriate cognitive strategies. Finally, errors may be tempered by attributes defined at the organizational level.

Before proceeding with the rest of the article, it should be noted that the results do not serve to explicitly identify the use of a specific heuristic. Rather, heuristic usage is inferred from the level of dread demonstrated by participants and suggests that the use of these strategies in this context merits further inquiry.

2. Framing Cyber Threats

A cyber threat, in the context of this article, is an expectation of harm to a political body through the malicious manipulation of cyberspace which reduces its capability to meet strategic, political, or economic objectives (Creppell, 2011). While threat conceptualizations vary, these are dependent on the domain's technological characteristics. Increased dependence on cyberspace elevates a society's exposure to potential threats, and consequently, the perception of dread brought by unforeseen consequences (Hansen & Nissenbaum, 2009; Kuehl, 2009). Furthermore, its growth coincides with Perrow's (2011) claim that complexity and interdependency result in *normal accidents* that emerge from the inherent characteristics of systems—compounding attempts to secure the domain. Experience, however, has proven less consequential. In 2010, Stuxnet affected nearly a third of Iran's nuclear centrifuges; yet damage did not exceed expected operational wear-and-tear (Lindsay, 2013). Likewise, disruption to segments of Ukraine's power grid in 2015 required the exploitation of interdependent systems but only resulted in temporary disruption (Zetter, 2016). Given its coercive intent, aggressors failed to achieve their objectives despite the exploitation of these valuable systems[1] (Iasiello, 2013; Maness & Valeriano, 2016).

Besides its technological fragility, the domain's strategic value also enjoys attention (Dunn Cavelty, 2012). Specifically, its perceived offensive advantage reflected by its low cost of entry and the difficulty of defending against aggressors is thought to serve as an equalizer within the international system (Lawson, 2013). For instance, the availability of tools stands in contrast with how hard it is to defend against aggressors. Consequently, weaker powers may offset their material disadvantage through cyberspace (Valeriano & Maness, 2014). Moreover, offensive acts are thought to be easier than defensive acts, further emboldening aggressors (Edwards et al., 2017).

No actor, however, has met its objectives by cyber means alone (Iasiello, 2013). Its low cost of entry is proportional to the expected gains (Pytlak & Mitchell, 2016; Slayton, 2017). While disruptive events require minimal effort, degradative operations demand substantial investments on the part of the aggressor. This is due to the organizational demands of an effective offensive campaign that is often overlooked in favour of technological considerations (Buchanan, 2017; Rid & Buchanan, 2015; Slayton, 2017). Consequently, this weakens arguments in favour of a cyber offensive-advantage. In addition, the evidence also illustrates restraint on the part of aggressors with their actions occurring below thresholds that are likely to result in escalation (Valeriano & Maness, 2015).

Despite its suggested exceptionalism, cyberspace remains subject to systemic, organizational, and material constraints such that operations have, thus far, achieved limited gains (Healey, 2016; Iasiello, 2013; Lawson, 2013; Sheldon, 2014). Yet whether one ascribes it to one or all of the above reasons, empirical evidence has yet to account for the continued sense of dread (Jarvis et al., 2017).

3. A Case for Cognitive Heuristics

The previous section suggests that a degree of irrationality influences judgements vis-à-vis cyber operations. Assuming the uniformity of the underlying technologies[2] and the move towards greater societal dependence, these deviations cannot be justified solely by technological or systemic variations. A classical understanding of rationality requires that decision-makers possess knowledge of all possible alternatives. Such conditions are rarely met and result in bounded rationality where individuals operate as satisfiers rather than optimizers (Dawes, 1979; De Neys, Rossi, & Houde, 2013; Kahneman, 2003; Thompson, Turner, & Pennycook, 2011).

Extending this argument further, Savage (1972) labels conditions of perfect information as *small worlds*,

[1] Stuxnet did not result in the discontinuation of the Iranian Nuclear Programme and the Ukraine attack did not shift the balance of the conflict in favour of Russia.

[2] A similar sense of dread has occurred in response to novel technologies. It is crucial to note that cyberspace is not exceptional in this case.

distinguishing these from *large worlds* where judgements informed by rational choice cannot be presumed to be the correct response. Research demonstrates that strategies that deviate from normative models are preferred when conditions with less than or almost perfect information exist (Binmore, 2008). The resulting less-is-more effect challenges the convention of rational cognition and brought renewed interest to the concept of heuristics.

Gigerenzer and Gaissmaier (2011, p. 454) define heuristics as a strategy that "ignores part of the information, with the goal of making decisions more quickly, frugally, and/or accurately than more complex methods". Although the classical approach to heuristics emphasizes its propensity to generate sub-optimal judgements, satisfactory results are possible when the strategy exploits the statistical characteristics of the information environment (Gigerenzer, 2008; Kruglanski et al., 2010; Martignon & Hoffrage, 1999).

The information environment plays a crucial role in making judgements. Assuming that information is readily available, the introduction of free parameters is unproblematic. This, however, is rarely the case. Most environments wherein judgements concerning future events are crucial involve *large worlds* in which relevant information is unknown or uncertain and is derived from a small sample. The introduction of additional parameters to improve fit risks the introduction of noise. Consequently, normative strategies such as expected utility are disadvantaged.

4. Cyberspace: A Very Large World

Heuristics may outperform normative strategies in uncertain environments. While it may be counterintuitive to assert that judgements regarding cyberspace are best approached through this frugal process, its characteristics are better aligned with the notion of a large rather than a small world.

4.1. An Uncertain Domain

Cyberspace is unpredictable. While its history is marked by efforts to reduce uncertainty, these do not eradicate the effects of increased complexity that limit predictive accuracy. Consequently, the significance of offensive or defensive acts cannot be fully anticipated (Farrell & Glaser, 2017).

The growth of technologically-driven solutions does not abolish the challenge of uncertainty. First, additional information does not translate to a generalizable view of threats. Although cyberspace operates on pre-defined rules[3], the interconnection between components varies by function. Relying on public threat information generated from a limited sample does not adequately capture this reality. Second, trust in automated systems to collect, identify, and model threats aggravate the problem of overfitting. These systems are dependent on pre-existing signatures, the development of which is left to individuals or organizations with a limited worldview and are unable to capture the full spectrum of threats. Finally, efforts to reduce bias through increased information sharing and exchange[4] is problematic. The exchange of information is non-obligatory and active participants share similarities in terms of technology and worldview. Moreover, the integrity of such information cannot be guaranteed.

4.2. Limited Experience

Cyber operations that significantly affect a state's strategic interests or normal day-to-day life are rare. This infrequency provides decision-makers with a limited sample from which to generalize. Valeriano and Maness (2014), for instance, identified less than fifty (50) instances where cyber threats inflicted noticeable damage to critical infrastructure. Judgements emerging from these may not reflect reality. Furthermore, efforts to increase the availability of threat intelligence, as mentioned above, may increase the volume of information, but not necessarily its quality.

In reference to Slovic's (2016) model of risk perception, events that are both uncertain and exhibit the potential (real or imagined) for catastrophe increase the level of dread. Translating this into the realm of politics, decision-makers operating in an uncertain environment with incomplete information tend to over-estimate risks associated with events such as the threat posed by an adversarial state (Jervis, 2017). Note, however, that while research has shown that appropriate judgements may still emerge using heuristics. This, however, is contingent on its fit with the existing information environment—also known as a heuristic's ecological rationality (Gigerenzer & Gaissmaier, 2011).

4.3. Constraints on Ecological Rationality

While the characteristics of cyberspace make it an ideal candidate for heuristic use, the selected heuristic must be able to exploit the environmental structures of uncertainty, sample size, redundancy, and variability in cue weights (Todd & Gigerenzer, 2012). The environmental structures of redundancy and variability in cue weights are of particular interest for this article. The former refers to the correlation between cues or the extent to which two or more sources of evidence are related to one another. For instance, to what extent does the ability to compromise the banking system in Country A indicate the vulnerability of the same country's power generation facilities? Relatedly, the variability of cue weights deter-

[3] The underlying components of cyberspace interact with the aid of pre-defined architectures (e.g., the Von Neumann architecture common to most modern-day computers) and protocols (e.g. Hypertext Transfer Protocol, HTTP).
[4] In the form of crowd-sourced threat intelligence such as the Open Threat Exchange (OTX).

mines whether the relevance of these cues is normally distributed or skewed. Building on the previous example, to what extent would Country B's banking system be vulnerable if that of Country A was exploited? Although heuristics have been proven to outperform more deliberate strategies, the ability to discern these characteristic is crucial for this task. Failure to do so results in ecologically irrational strategies being selected that, in turn, leads to inappropriate judgements. While factors such as time-pressure, cognitive resources, and pre-existing bias hinder the ability to select ecologically rational strategies, this article is interested primarily in the enabling role of domain expertise with respect to cyberspace (Kruglanski & Gigerenzer, 2011).

Although cyberspace appears monolithic to laymen, its inner workings are greatly segmented. Such abstraction is crucial to allow individuals to exploit its functionality for their professional or day-to-day tasks. However, attempts to explain its finer points have resulted to the use of analogies that poorly explain the functioning of this domain and which have resulted in many misconceptions amongst the public (Betz & Stevens, 2013; E. Goldman & Arquilla, 2014). While simplification aids communication, it limits the ability to form sound judgements which could otherwise emerge in light of a better, if not complete, understanding of cyberspace. Authors such as Hansen and Nissenbaum (2009) have cited knowledge discrepancies between experts and non-experts as the source of alarmism over cyberspace. Similarly, a recent study of media articles covering cyber operations has found no difference in how threats are perceived between different states and those that occur domestically (Jarvis et al., 2017). In the earlier example, if both power generation (Country A) and banking (Country B) used identical systems and were equally vulnerable then heuristics such as "Take the Best" would work just as well, if not better, than more deliberate cognitive strategies (Gigerenzer, 2008). However, expertise gained through experience or formal training would prompt decision-makers to recognize the differences between these systems resulting in the use of more ecologically rational strategies. Taken collectively, questions concerning the lack of experience and expertise towards cyber operations leads to two key propositions:

(a) Hypothesis 1: *Limited of experience with cyber operations creates an environment of uncertainty resulting in the use of cognitive heuristics*.

(b) Hypothesis 2: *The absence of domain knowledge in cyberspace prompts the selection of inappropriate heuristics resulting in elevated levels of dread*.

5. Experimental Design

5.1. Operationalization and General Design

To demonstrate the role of heuristics, the article implements a 2×2 between-group vignette survey experiment (Auspurg & Albanese, 2015; Rousseau & Garcia-Retamero, 2007; Sniderman, 2011). The treatment is applied through the manipulation of *Internal* and *External* variables that reflect positive or negative events. For the purposes of this experiment, these events are cyber operations targeting a state's power generation facilities. These are made to vary slightly with respect to their cause, impact, and time, and to reflect the uncertainty of the informational environment. Participants are also denied information regarding other events besides that of a second state's experience with a cyber operation. These are meant to operationalize the concept of uncertainty and limited experience which is crucial to the above framework. Furthermore, the countries depicted in the vignette are portrayed as being nearly identical to one another in terms of their usage of cyberspace. No specific information is provided regarding the specific technologies used or how they vary. This is intended to stimulate the participant's knowledge of cyberspace and operationalizes the concepts of redundancy and variability, which entails that those with greater knowledge of the domain ought to be able to recognize the possible differences that may exist. These characteristics meant that both hypotheses could be tested.

Before reading the vignette, participants responded to a set of questions to measures their trust in cyberspace to act as a control for pre-treatment effects. The questionnaire is based on Jian, Bisantz and Drury's (2000) measure of trust in automated systems. This is followed by the vignette in which the participants are instructed to evaluate the extent to which they perceive cyberspace as threatening. Threat is measured with a 10-point Likert scale.[5] The baseline value is five (5), which suggests a neutral perception of the domain.[6] Higher values indicate elevated levels of dread while lower values reflect its absence.

The choice to operationalize the concept of dread as the threatening (or not) nature of cyberspace is grounded in the vernacular understanding of a threat. A threat may be an indication of something impending (e.g. threat of a blackout). In the context of the vignette, this is presented as the threat of the negative consequences of a cyber operation. Analytically, this is equivalent to Slovic's (2016) notion of dread which is viewed as the apprehension of the negative consequences of an activity.

[5] The Likert scale is a widely used instrument for measuring a participant's attitude in survey research. For more information, refer to the Sage Research Methods webpage (Lavrakas, 2008).
[6] As there is no available baseline as to the "appropriate" level of dread, this value was deemed appropriate given the objectives of the study.
[7] An Internet-based platform for recruiting participants specifically for research.

5.2. Participant Recruitment

Participants were recruited through Prolific[7]. While concerns regarding data quality from Internet sources persist, no significant difference has been found with respect to experiments investigating cognitive processes (Casler, Bickel, & Hackett, 2013; Crump, McDonnell, & Gureckis, 2013; Peer, Brandimarte, Samat, & Acquisti, 2017). Special care, however, is required as participants are often less engaged with the experiment. Consequently, two attention check questions are included such that failing one requires the removal of a participant.

The participants consist of university students divided into two groups. The first are those pursuing degrees in Computer Science and related disciplines while the second are those who do not have the same educational background. The former represents "domain experts" while the latter are viewed as "domain non-experts". Participants are then randomly assigned to one of four versions of the vignette. Given the absence of methodologically similar research for this problem domain, the authors assumed a moderately large effect size ($f = 0.3$). Consequently, a minimum sample size with appropriate statistical power ($1 - \beta = 0.8$) was estimated at 90.[8] It ought to be noted that the results contained herein are valid with respect to the samples used and are therefore not immediately generalizable. Replications studies are necessary before more generalizable conclusions are made.

6. Experimental Results

6.1. Experiment 1: Domain Non-Experts

The first experiment recruited 202 participants. Of these, 50.99% (103) were female and the remaining 49.01% (99) were male. Issues concerning engagement were encountered leading to the removal of 27.72% (56).[9] To ensure a balanced analysis, random samples were drawn based on the size of the smallest treatment group resulting in 120 samples with thirty (30) samples per treatment group.

Analysis reveals that 65.9% (79) of participants began the experiment with a distrust of cyberspace while the remaining 34.1% (41) indicated that they either trusted the domain or held no preference. The mean for *Threat*, however, does not suggest an elevated sense of dread ($\bar{x} = 5.5$, baseline = 5.0).

To determine the effect of *Trust* and the absence or presence of *External* and *Internal* events on *Threat*, a blocked factorial Analysis of Variance (ANOVA)[10] was performed. For this analysis, the effects on *Trust* (i.e. Positive, Negative, Neutral) was controlled for through blocking.

The results of the experiment shows a significant Average Treatment Effect (ATE) due to the *External*, $F(1,114) = 10.33$ and *Internal* $F(1,114) = 7.37$ treatments as well the pre-existing level of *Trust* $F(2,144) = 4$ on *Threat* at the $p < 0.05$ level.[11] A Post Hoc comparison reveals that the main effects are significant at $p < 0.05$. The presence of an *External* event had a main effect of 1.34 on *Threat*. An Internal event, on the other hand, had a main effect of 1.13. Finally, *Trust* had a significant main effect of 1.27 between Positive and Negative groups. No significant interactions were observed in this experiment.

6.2. Experiment 2: Domain Experts

The second experiment recruited 166 participants. Of these, 22.29% (37) were female and the remaining 77.71% (129) were male. Issues concerning engagement were encountered leading to the removal of 32.53% (54). To ensure a balanced analysis, random samples were drawn based on the size of the smallest treatment group resulting in 112 samples with twenty-eight (28) samples per treatment group.

Analysis reveals that 50.89% (57) of participants began the experiment with a distrust of cyberspace while the remaining 49.11% (55) indicated that they either trusted the domain or held no preference. The mean for *Threat*, however, does not suggest an elevated sense of dread ($\bar{x} = 5.71$, baseline = 5.0). To determine the effect of *Trust* and the absence or presence of *External* and *Internal* events on *Threat*, a blocked factorial ANOVA was performed. For this analysis, the effects to *Trust* was controlled for through blocking.

The analysis does not reveal a significant ATE of the *Internal*, or *Trust* treatments on *Threat* at the $p < 0.05$ level[12]. External $F(1,106) = 2.72$, $p = 0.06$, however, had a barely significant main effect on *Threat*. A Post Hoc comparison illustrates that there is no statistically significant difference across different treatment groups in terms of *Threat* for this given experiment. No significant interactions are observed in this experiment.

7. General Discussion

7.1. Non-Experts and Motivated Reasoning

The results indicate that dread is not noticeably elevated for domain non-experts ($\bar{x} = 5.5$). When comparisons

[8] The approximation that 90 participants are necessary to ensure that the findings were not simply the result of chance and that the treatment has resulted in a valid and observable effect.

[9] Studies concerning the lack of attention on Internet-based platforms suggest that attrition can be as high as 50%. A rate less than 30% exceeds expectations (Peer et al., 2017).

[10] A collection of statistical techniques used to analyze the difference of means between groups. For further information, refer to *Introduction to Analysis of Variance* (Turner & Thayer, 2001).

[11] Effect Size (Cohen's f): $\text{Trust}_f = 0.265$; $\text{External}_f = 0.301$; $\text{Internal}_f = 0.254$.

[12] Effect Size (Cohen's f): $\text{Trust}_f = 0.206$; $\text{External}_f = 0.187$; $\text{Internal}_f = 0.136$.

are made between treatment groups, however, a different picture emerges. Treatment groups exposed solely to *External* events ($\bar{x} = 5.7$, $p = 0.044$) and those that experienced both *External* and *Internal* events ($\bar{x} = 6.7$, $p = 0.0$) reflect elevated and statistically significant levels of dread in comparison to the control ($\bar{x} = 4.167$).

While the design of the experiment does not permit the identification of specific cognitive heuristic, it allows one to infer the possible processes involved. For groups in which negative *External* and *Internal* events occurred, the imagery of an extended period of power loss experienced by a similar country is set in the memory of the participant. The participant is then informed of a similar event taking place in their hypothetical country—resulting in an emotional association between the two events. This process of emotional association has been identified as a cornerstone of motivated reasoning in which decision-makers strive to maintain cognitive consistency with respect to their existing beliefs (Jervis, 2017). Furthermore, these beliefs are self-reinforcing with later experiences confirming or strengthening one's position on the matter (Holmes, 2015; Mercer, 2010; Roach, 2016). Yet this association may not be dependent solely on the debilitative experience of a third-party. The existing levels of *Trust* by participants may have also played a role.

For treatment groups experiencing only negative *External* events, the mean of *Threat* was 2.2 points higher for participants who distrusted cyberspace ($p = 0.01$). This similarity in direction between *Trust* and *Threat* suggests an association between the two, which may have led participants to use the former to inform their judgements. Unfortunately, this process is not observed in cases where both *External* and *Internal* events are negative in nature where the difference due to *Trust* is only 0.8 points ($p = 0.5$). This does not discredit earlier arguments.

The level of dread may have been a manifestation of motivated reasoning—the need to believe in the dangers of cyberspace. But the emotional association may have been caused by the recency effect (Krosnick, Li, & Lehman, 1990). When participants are asked to evaluate the level of *Threat*, those exposed to negative *Internal* events begin their associated memory search with their most recent experience. If a negative *External* event had recently been shown, the recency effect could result in an association forming between the two. In its absence, participants would have to extend the search of their stored memory which may include pre-existing trust in cyberspace.

The above process also accounts for the absence of elevated levels of *Threat* (i.e. negative *Internal* event only). Prior to applying the *Internal* treatment, participants are informed that "domestically, your country, like others, occasionally experiences trouble with criminals in cyberspace who target individuals and small to medium-sized enterprises for financial gain". Consequently, it is possible that participants form an association with this statement. The absence of a negative *External* event reinforces the benign nature of cyberspace as other countries with seemingly similar characteristics have not encountered problems. Additionally, the similarity in the levels of *Threat* irrespective of *Trust* rules the latter out as a source of association. Finally, the lack of difference between the level of *Threat* of this group and that of the control suggests that the participants perceive the situation as routine.

7.2. Motivated Reasoning and Inappropriate Strategies

The presence of motivated reasoning in the formation of judgement does not necessarily result in sub-optimal outcomes. The literature on motivated reasoning identifies two modes of thinking: accuracy-oriented and goal-oriented (Kunda, 1990; Taber, Lodge, & Glathar, 2001). The former assumes that individuals will engage in more deliberate and cognitively demanding processing to reach the best conclusion. The latter, in contrast, motivates individuals to maintain pre-determined beliefs resulting in selective information processing which reinforces existing biases.

With respect to the article, the situation in the vignette is framed such that it encourages a goal-oriented mindset. Participants play the role of an appointed elite with no apparent accountability to the public. Moreover, there are no explicitly stated consequences that may result from bad judgement (Lerner & Tetlock, 1999). Furthermore, the stereotypical use of *External* and *Internal* events (as well as *Trust*) suggests an attempt to maintain pre-existing beliefs by building associations (specified in the vignette or from past experience) to serve as reference points to assess the current state of cyberspace.

The representativeness heuristic is employed when making judgements in uncertain environments. When in use, individuals resort to the comparison of salient features exhibited by objects or events (Kahneman, 2011). In the experiment, participants appear to draw similarities between their hypothetical country and others regarding the use of cyberspace and its corresponding vulnerability as well as between the situation presented in the vignette and their own pre-existing notions concerning cyberspace (i.e. *Trust*).

A cursory evaluation of the vignette encourages readers to identify and find similarities between the countries being discussed. Both hypothetical countries invested in and enjoyed the economic benefits of ICT. For those that experienced negative *External* and *Internal* events, both had their power plants affected to varying degrees. A few assumptions may be made given these. First, ICT (and in turn cyberspace) is a monolithic and homogenous construct. Second, all power plants that depend on these technologies are vulnerable. Third, these vulnerabilities can easily be exploited. Finally, the consequences of such a compromise are predictable. These raise questions whether the redundancy and variability of cues within the information environment were suffi-

ciently recognized by the participants. Failure to do so results in the selection of ecologically irrational strategies and accounts for the observed level of dread.

As logical as these propositions may be, they fail to grasp certain realities. Indeed, cyberspace is by no means a homogenous entity. While these technologies do share commonalities that allow for integration, they retain enough individual characteristics to make each unique. For instance, while both Windows and Unix systems share common protocols, a vulnerability in the former is not necessarily shared by the latter. And even if a vulnerability is found to exist, it is not a confirmation of its exploitability. Both intent and capabilities need to exist for this to occur (Edwards et al., 2017; Maurer, 2018). Absent an interested actor, a vulnerability may continue to exist without any further repercussions. Moreover, the successful exploitation of a vulnerability also depends on the capabilities of both parties involved. In the case of Stuxnet, significant resources were invested to overcome the physical and technological barriers raised to secure the targeted systems. Finally, the consequences of such an interdependent and interconnected system failing cannot be predicted beforehand with absolute certainty (Perrow, 2011).

This depth of knowledge cannot be expected from the average participant in Experiment 1. This results in uncertainty that prompts the use of the representativeness heuristics. The results suggest that participants attempted to find similarities between the events and structures presented resulting in unsuitable stereotypes being drawn between *External* and *Internal* events as well as between these and their personal experiences with cyberspace. Consequently, the behaviour observed with non-experts confirms the assertions of Hypothesis 1 that limited experience with cyber operations creates an environment of uncertainty that prompts the use of heuristics.

7.3. A Brief Note on Domain Experts

As with the first experiment, the level of dread reflected by experts does not appear to rise significantly above the established baseline ($\bar{x} = 5.71$). When treatment groups are compared to the control, however, no statistical difference is noted. This suggests that experts maintain a consistent perception of cyberspace regardless of the treatment provided. This is corroborated by the fact that neither *External*, *Internal*, or *Trust* had a statistically significant impact on the outcome. This supports the argument that knowledgeable individuals would not create inappropriate stereotypes and appears. Consequently, this supports Hypothesis 2 which asserts that domain knowledge would result in lower levels of dread given the use of appropriate heuristics. However, it does not allow us to rule out the use of goal-oriented motivations as a means of maintaining bias-prone beliefs. Although findings are inconclusive, it opens the possibility of further inquiry into the decision-making processes used by experts. Past research demonstrates that experts formulate sound judgements while utilizing cognitive shortcuts. This, however, is dependent on the past information environment matching the present (Lau & Redlawsk, 2001).

The past decade has seen the growth of malicious interstate activities in cyberspace. Yet the aggressive use of these technologies existed long before events in Estonia (i.e. 2007). The context, however, has changed. Although the participants in Experiment 2 are most likely aware of these developments, the body of knowledge they possess through their formal education was developed from combating non-state actors[13]. While the authors are not arguing that the current mechanisms in place are insufficient, the possibility exists that they are not the most efficient and may limit the ability of states to act.

The inconclusive results of the second experiment should not be treated as a failure. Rather, it serves to inform future research how experiments involving domain experts ought to be designed. Specifically, it narrows the factors that may serve to influence the quality of expert judgements.

8. Tempering Bias and the Organization

The findings demonstrate that decision-makers can resort to motivated reasoning when formulating judgements regarding cyberspace. These tendencies have implications in two related ambits: (a) the cost consequences within the immediate context that decisions must be made, and (b) considerations for tempering bias to minimize cost consequences.

8.1. Consequences for Mobilization due to Perceptions of Dread

The context in which judgements regarding cyberspace are made occur within specific institutional boundaries. Policies are formed as a result of judgements undertaken within an organized context. On that note, consequences for this context are spread across two levels—the organization, and the state that the organization represents. When decision-makers resort to intuitive thinking, the probability that their perception of dread relative to a specific cyber issue is reasonably congruent with the actual level of dread varies according to three likely scenarios: (a) deflation, where the perceived threat is less than the actual threat; (b) congruence, where the perceived threat is congruent with the actual threat; and (c) inflation, where the perceived threat is greater than the actual threat.

Consequently, any of the scenarios above can frame the deployment of capabilities and tools in response to

[13]The curriculum used to teach Information Security in Computer Science departments is built on past efforts to combat hacking and cyber-crime. Frameworks such as the $(ISC)^2$ Common Body of Knowledge (Brecht, 2017) are examples of this. While some of the technical concepts are applicable to state actors, the political context may be unique and requires additional insights beyond these frameworks.

an impending event in the cyberspace (Dunn Cavelty, 2013). This has consequences for the resulting strategy for mobilization, which in turn comes with costs incurred by the organization.

As far as consequent mobilization strategies are concerned, there are three possibilities. First, it can occur in a form of a race to the extent that it may be intended as an offensive position. Second, it can occur in a form that meets the minimum capabilities necessary to be in a position of defence. Finally, it can occur in a manner where base capabilities are developed for decreasing vulnerabilities and increasing resilience to potential attacks. The underlying costs for the deployment of capabilities is a complex feat because approximating the symmetry between the perceived threat and the actual threat is not always optimal. An individual making the judgment who is at the same in a position of authority may either overestimate or underestimate the threat and could, therefore, impose material and immaterial costs for both the organization and the state.

Beyond theoretical assertions, the implications of (in)correctly providing security assessments ought to be considered considering the pace at which states are developing their respective cyber capabilities. While congruence has long been the desired state, the inherent characteristics of the domain compounds the persistent difficulty of assessing an adversary's intent and capabilities (Buchanan, 2017). The essential secrecy that obscures capabilities in cyberspace generates uncertainty on the part of assessor states. In the absence of knowledge regarding a potential adversary's true capabilities, states are left to form judgements based on past behaviour; judgements which may, in themselves, be subject to bias.

Interestingly, the need for insight into a potential adversary's capabilities may itself lead to greater instability. Regardless of whether a cyber operation is meant for intelligence gathering or as a first step of a larger offensive campaign, unauthorized access to a secure system is necessary. If discovered, the inherent characteristics of cyberspace do not permit the victim to determine which of the two objectives led to this event. At this point, the victim's own pre-existing beliefs may determine its potential response which could range from a tacit acknowledgement of routine (and expected) espionage to one of an escalatory spiral (Buchanan, 2017).

Consequently, the need for sufficient, if not optimal judgement, is mandatory on both sides of an interstate interaction. Parties must temper pre-existing beliefs to avoid engaging in either provocative action (aggressor) or unnecessary escalatory responses. Although the escalation of hostilities into the physical domain is unlikely, the disruption of cyberspace carries potential and avoidable costs.

8.2. Tempering Bias to Minimize Unnecessary Costs

This, in turn, begs the question: how can bias be tempered to minimize the likelihood of accruing costs? Our findings reveal the recurring use of heuristics at the individual level, which is critical because individuals who respond to cyber operations are assumed to be in a position of authority and able to make decisions which may, in turn, have repercussions for the organizations and states they represent. Indeed, judgments formed at the individual level frame decisions, and in turn, incur cost implications and related repercussions within the immediate social context for which the decision-maker is undertaking the decisions for. To this end, considerations for minimizing costs at the organizational level which emanate from inaccurate judgments at the individual level are inevitably linked with considerations for how micro-level processes contribute to macro-level outcomes.

However, our findings are limited to the extent that they do not consider the embeddedness of the individual within the organizational setting in undertaking decisions. Considering that decisions pertaining to cyber operations are undertaken within a context with institutional boundaries, it is possible that the direction of effects of the inaccurate judgments on the organization does not occur in one direction from the individual to the organization. Instead, we posit the likelihood that the organizations which individuals represent also possess certain attributes that can modulate individual biases. In the study of organizations, these micro-macro process considerations during uncertain contexts such as cyber operations are reminiscent of sensemaking within organizations (Weick, Sutcliffe, & Obstfeld, 2005), and how institutions enter the meaning-making processes of individuals in critical times (Weber & Glynn, 2006).

Sensemaking is broadly defined as a process by which people seek to make plausible sense of ambiguous, equivocal, or confusing issues and events (Brown, Colville, & Pye, 2015; Maitlis & Sonenshein, 2010) so as to be able to mobilize an appropriate response (Weick et al., 2005). Sensemaking has been studied particularly within the context of crises and emergencies (Maitlis & Sonenshein, 2010; Weick, 1993) where individual members of an organization become suddenly faced with a situation that is difficult to approximate with certainty, while at the same time being constrained by both information and time, as well as having to provide an immediate justifiable response. Given that the findings of this article infer the use of heuristics by individuals, it would also be interesting to extend the investigation regarding how intuitive judgements can be minimized during an overall sensemaking process that involves various cues from the organization that the individuals are a part of. Note that sensemaking is a means by which individuals are enabled to continuously stay in action amidst a disruptive shock (Weick et al., 2005) and to stay in action, individuals draw from certain "frameworks including institutional constraints, organizational premises, plans, expectations, acceptable justifications and traditions inherited from predecessors" (Weick et al., 2005). In cyber operations, as much as individuals with a position of authority articulate a judgment, it is also important to consider

the institutional boundaries that shape ways in which decisions are made. Empirically, it would be interesting to extend the experiment in a context where individuals are exposed to interactions with other individuals with the same organizational membership and see how such interactions may either weaken or strengthen the extent of ecological rationality in cyberspace operations.

Broadly, institutions influence the sense-making process (Weber & Glynn, 2006). These institutional influences are exerted concretely through various ways within the sensemaking process of the individual. For example, institutions can affect individual sensemaking through institutional policing, which may be embedded in the structural hierarchies and command-and-control approaches of the organization. This can be explored by considering how structure, templates, and other manifestations of organizational control may affect the way decision-makers in cyberspace make meaning. Sensemaking can also be triggered by the institution through interactions within groups that are oriented towards a specific organizational goal. Cyberspace operations are presently deemed ubiquitous for purposes that involve policy of the state, where conventions regarding its use have yet to converge and be institutionalized. This has an implication for the composition of groups involved in cyberspace operations, namely, those with positions of authority to enact certain policies related to cyberspace have a variety of backgrounds and turf representations. Future research may thus investigate how group composition, group dynamics, and group interaction among various individuals with specific types of judgments and biases can influence collective sensemaking, and ultimately temper the perception of dread in cyberspace.

9. Conclusions

The phenomenon of dread in cyberspace is a confluence of the domain's inherent characteristics and individual cognitive processes. The complex interdependencies within the domain generate a significant amount of uncertainty regarding the consequences of cyber operations aimed at disrupting its routine operations. While preventive measures may be taken to reduce its impact, its true scope cannot be determined beforehand. Consequently, individual decision-makers, particularly those lacking experience, resort to similar (though possibly unrelated) events to form judgements regarding the situation at hand. This causes decision-makers fall into the trap of finding correlations between events where none exist, resulting in the use of strategies that are deemed ecologically irrational. In doing so, the resulting judgements may either overestimate or underestimate the level of threat that can result in inappropriate policies which can complicate existing interstate relations.

To mitigate these issues, organizations to which these individuals belong should take appropriate steps to encourage accuracy-oriented reasoning on the part of decision-makers. While this does not eliminate the influence of bias, it increases the likelihood that assessments will be congruent to current realities. This minimizes the likelihood that costs will be incurred through the unnecessary development of capabilities or as the consequences of escalation between parties.

Interstate interactions in cyberspace is an emergent phenomenon that demands further analysis. While existing theories concerning material or systemic constraints have proven useful, it is necessary to move towards micro- and meso-level factors to better account for behaviour in this man-made domain. To this end, this article contributes to the on-going discourse by providing the initial steps needed to strengthen this line of inquiry.

Acknowledgements

We would like to thank Dr. Margarita Petrova for allowing us to conduct the initial pilot study for these experiments at the *Institut Barcelona d'Estudis Internacionals* (IBEI); the results contributed significantly to the development of the experimental instruments. We would also like to extend our gratitude to Nadiya Kostyuk, Dr. Christopher Whyte and the other members of the Digital Issues Discussion Group (DIDG) whose insights allowed us to better frame our arguments.

Conflict of Interests

The authors declare no conflict of interests.

References

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M., Levi, M., . . . Savage, S. (2013). Measuring the cost of cybercrime. In R. Böhme (Ed.). *The economics of information security and privacy* (pp. 265–300): New York, NY: Springer.

Auspurg, K., & Albanese, J. (2015). *Factorial survey experiments*. Los Angeles, CA: SAGE.

Betz, D. J., & Stevens, T. (2013). Analogical reasoning and cyber security. *Security Dialogue*, *44*(2), 147–164.

Binmore, K. (2008). *Rational decisions*. Princeton, NJ: Princeton University Press.

Boutin, P. (2003). *Slammed! Wired Magazine*. Retrieved from https://www.wired.com/2003/07/slammer

Brecht, D. (2017). The CISSP CBK domains: Information and updates. *Infosec Institute*. Retrieved from http://resources.infosecinstitute.com/category/certifications-training/cissp/domains/#gref

Brown, A. D., Colville, I., & Pye, A. (2015). Making sense of sensemaking in organization studies. *Organization Studies*, *36*(2), 265–277.

Buchanan, B. (2017). *The cybersecurity dilemma: Hacking, trust and fear between nations*. London: Hurst & Company.

Casler, K., Bickel, L., & Hackett, E. (2013). Separate but equal? A comparison of participants and data gathered via Amazon's MTurk, social media, and face-to-

face behavioral testing. *Computers in Human Behavior*, *29*(6), 2156–2160.

Creppell, I. (2011). The concept of normative threat. *International Theory*, *3*(3), 450–487.

Crump, M., McDonnell, J. V., & Gureckis, T. M. (2013). Evaluating Amazon's Mechanical Turk as a tool for experimental behavioral research. *PloS one*, *8*(3), e57410.

Dawes, R. M. (1979). The robust beauty of improper linear models in decision making. *American Psychologist*, *34*(7), 571–582.

De Neys, W., Rossi, S., & Houde, O. (2013). Bats, balls, and substitution sensitivity: Cognitive misers are no happy fools. *Psychonomic Bulletin & Review*, *20*(2), 269–273.

Dean, B., & McDermott, R. (2017). A research agenda to improve decision making in cyber security policy. *Penn State Journal of Law & International Affairs*, *5*, 29–164.

Dunn Cavelty, M. (2012). The militarisation of cyberspace: Why less may be better. In C. Czosseck, R. Ottis, & K. Ziolkowski (Eds.), *2012 4th international conference on cyber conflict* (pp. 1–13). Tallinn: IEEE.

Dunn Cavelty, M. (2013). From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse. *International Studies Review*, *15*(1), 105–122.

Edwards, B., Furnas, A., Forrest, S., & Axelrod, R. (2017). Strategic aspects of cyberattack, attribution, and blame. *Proceedings of the National Academy of Sciences*, *114*(11), 2825–2830. doi:1700442114

Farrell, H., & Glaser, C. L. (2017). The role of effects, saliencies and norms in US cyberwar doctrine. *Journal of Cybersecurity*, *3*(1), 7–17.

Gartzke, E., & Lindsay, J. R. (2015). Weaving tangled webs: Offense, defense, and deception in cyberspace. *Security Studies*, *24*(2), 316–348.

Gigerenzer, G. (2008). Why heuristics work. *Perspectives On Psychological Science*, *3*(1), 20–29.

Gigerenzer, G., & Gaissmaier, W. (2011). Heuristic decision making. *Annual Review Of Psychology*, *62*, 451–482.

Goldman, E., & Arquilla, J. (2014). *Cyber analogies*. Monterey: Naval Postgraduate School.

Goldman, R. (2017). What we know and don't know about the international cyberattack. *The New York Times*. Retrieved from https://www.nytimes.com/2017/05/12/world/europe/international-cyberattack-ransomware.html?_r=0

Hafenbradl, S., Waeger, D., Marewski, J. N., & Gigerenzer, G. (2016). Applied decision making with fast-and-frugal heuristics. *Journal of Applied Research in Memory and Cognition*, *5*(2), 215–231.

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the copenhagen school. *International Studies Quarterly*, *53*(4), 1155–1175.

Healey, J. (2016). Winning and losing in cyberspace. In N. Pissanidis, H. Rõigas, & M. Veenendaal (Eds.), *2016 8th international conference on cyber conflict* (pp. 37–49). Tallinn: IEEE.

Holmes, M. (2015). Believing this and alieving that: Theorizing affect and intuitions in international politics. *International Studies Quarterly*, *59*(4), 706–720.

Iasiello, E. (2013). Cyber attack: A dull tool to shape foreign policy. In K. Podins, J. Stinissen, & M. Maybaum (Eds.), *2013 5th international conference on cyber conflict* (pp. 451–470). Tallinn: IEEE.

Jardine, E. (2015). *Global cyberspace is safer than you think: Real trends in cybercrime*. Waterloo: Centre for International Governance Innovation.

Jardine, E. (2017). *Sometimes three rights really do make a wrong: Measuring cybersecurity and Simpson's paradox*. Paper presented at the Workshop on the Economics of Information Security, La Jolla, CA.

Jarvis, L., Macdonald, S., & Whiting, A. (2017). Unpacking cyberterrorism discourse: Specificity, status, and scale in news media constructions of threat. *European Journal of International Security*, *2*(1), 64–87.

Jensen, B., Maness, R. C., & Valeriano, B. (2016). *Cyber victory: The efficacy of cyber coercion*. Paper presented at the Annual Meeting of the International Studies Association, Atlanta, USA.

Jervis, R. (2017). *Perception and misperception in international politics*. Princeton, NJ: Princeton University Press.

Jian, J.-Y., Bisantz, A. M., & Drury, C. G. (2000). Foundations for an empirically determined scale of trust in automated systems. *International Journal of Cognitive Ergonomics*, *4*(1), 53–71.

Kahneman, D. (2003). A perspective on judgment and choice—Mapping bounded rationality. *American Psychologist*, *58*(9), 697–720.

Kahneman, D. (2011). *Thinking, fast and slow*. New York, NY: Farrar, Straus and Giroux.

Krosnick, J. A., Li, F., & Lehman, D. R. (1990). Conversational conventions, order of information acquisition, and the effect of base rates and individuating information on social judgments. *Journal of Personality And Social Psychology*, *59*(6), 1140–1152.

Kruglanski, A. W., & Gigerenzer, G. (2011). Intuitive and deliberate judgments are based on common principles. *Psychological Review*, *118*(1), 97–109.

Kruglanski, A. W., Orehek, E., Dechesne, M., & Pierro, A. (2010). Lay epistemic theory: The motivational, cognitive, and social aspects of knowledge formation. *Social and Personality Psychology Compass*, *4*(10), 939–950.

Kuehl, D. T. (2009). From cyberspace to cyberpower: Defining the problem. In F. D. S. Kramer, Stuart H.; Wentz, Larry (Eds.), *Cyberpower and national security* (pp. 24–42). Dulles, VA: Potomac Books.

Kunda, Z. (1990). The case for motivated reasoning. *Psychological Bulletin*, *108*(3), 480–498.

Lau, R., R., & Redlawsk, D. P. (2001). Advantages and disadvantages of cognitive heuristics in political decision making. *American Journal of Political Science*, *45*(4), 951–971.

Lavrakas, P. J. (2008). Likert scale. *Sage Research Methods*. Retrieved from http://methods.sagepub.com/reference/encyclopedia-of-survey-research-methods/n273.xml

Lawson, S. (2013). Beyond cyber-doom: Assessing the limits of hypothetical scenarios in the framing of cyber-threats. *Journal of Information Technology & Politics*, *10*(1), 86–103.

Lerner, J. S., & Tetlock, P. E. (1999). Accounting for the effects of accountability. *Psychological Bulletin*, *125*(2), 255–275.

Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. *Security Studies*, *22*(3), 365–404.

Maitlis, S., & Sonenshein, S. (2010). Sensemaking in crisis and change: Inspiration and insights from Weick (1988). *Journal of Management Studies*, *47*(3), 551–580.

Maness, R. C., & Valeriano, B. (2016). The impact of cyber conflict on international interactions. *Armed Forces & Society*, *42*(2), 301–323.

Martignon, L., & Hoffrage, U. (1999). Why does one-reason decision making work? In G. Gigerenzer, P. M. Todd, & T. A. R. Group (Eds.), *Simple heuristics that make us smart* (pp. 119–140). New York, NY: Oxford University Press.

Maurer, T. (2018). *Cyber mercenaries: The state, hackers, and power*. New York, NY: Cambridge University Press.

Mercer, J. (2010). Emotional beliefs. *International Organization*, *64*(1), 1–31.

Peer, E., Brandimarte, L., Samat, S., & Acquisti, A. (2017). Beyond the Turk: Alternative platforms for crowdsourcing behavioral research. *Journal of Experimental Social Psychology*, *70*, 153–163.

Perrone, J. (2001). Code Red worm. *The Guardian*. Retrieved from https://www.theguardian.com/world/2001/aug/01/qanda.janeperrone

Perrow, C. (2011). *Normal accidents: Living with high risk technologies*. Princeton, NJ: Princeton University Press.

Pytlak, A., & Mitchell, G. E. (2016). Power, rivalry, and cyber conflict: An empirical analysis. In K. Friis & J. Ringsmose (Eds.), *Conflict in cyber space: Theoretical, strategic and legal perspectives* (pp. 65–82). London: Routledge.

Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies*, *38*(1/2), 4–37.

Roach, S. C. (2016). Affective values in international relations: Theorizing emotional actions and the value of resilience. *Politics*, *36*(4), 400–412.

Rousseau, D. L., & Garcia-Retamero, R. (2007). Identity, power, and threat perception—A cross-national experimental study. *Journal of Conflict Resolution*, *51*(5), 744–771.

Savage, L. J. (1972). *The foundations of statistics*. New York, NY: Dover Publications.

Sheldon, J. B. (2014). Geopolitics and cyber power: Why geography still matters. *American Foreign Policy Interests*, *36*(5), 286–293.

Slayton, R. (2017). What is the cyber offense-defense balance? Conceptions, causes, and assessment. *International Security*, *41*(3), 72–109.

Slovic, P. (2016). *The perception of risk*. New York, NY: Earthscan.

Sniderman, P. M. (2011). The logic and design of the survey experiment. In J. N. Druckman, D. P. Green, J. H. Kuklinski, & A. Lupia (Eds.), *Cambridge handbook of experimental political science* (pp. 102–114). New York, NY: Cambridge University Press.

Taber, C. S., Lodge, M., & Glathar, J. (2001). The motivated construction of political judgments. In J. H. Kuklinski (Ed.), *Citizens and politics: Perspectives from political psychology* (pp. 198–226). Cambridge: Cambridge University Press.

Thompson, V., Turner, J. A., & Pennycook, G. (2011). Intuition, reason, and metacognition. *Cognitive Psychology*, *63*(3), 107–140.

Todd, P., & Gigerenzer, G. (2012). *Ecological rationality: Intelligence in the world*. New York, NY: Oxford University Press.

Turner, J. R., & Thayer, J. F. (2001). *Introduction to analysis of variance: Design, analysis, & interpretation*. Thousand Oaks, CA: Sage Publications.

Valeriano, B., & Maness, R. C. (2014). The dynamics of cyber conflict between rival antagonists, 2001–11. *Journal of Peace Research*, *51*(3), 347–360.

Valeriano, B., & Maness, R. C. (2015). *Cyber war versus cyber realities: Cyber conflict in the international system*. Oxford; New York, NY: Oxford University Press.

Weber, K., & Glynn, M. A. (2006). Making sense with institutions: Context, thought and action in Karl Weick's theory. *Organization Studies*, *27*(11), 1639–1660.

Weick, K. E. (1993). The collapse of sensemaking in organizations—The Mann Gulch disaster. *Administrative Science Quarterly*, *38*(4), 628–652.

Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (2005). Organizing and the process of sensemaking. *Organization Science*, *16*(4), 409–421.

Zetter, K. (2016). Inside the cunning, unprecendented hack of Ukraine's power grid. *Wired Magazine*. Retrieved from https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid

About the Authors

Miguel Alberto Gomez is Senior Researcher with the Center for Security Studies (CSS) at the ETH in Zurich and is a doctoral candidate at the School of Law and Politics at Cardiff University. His current research focuses on political psychology and its implications for the coercive use of cyber power.

Eula Bianca Villar is a Researcher and PhD Candidate at the Department of Business and Technology in La Salle Universitat Ramon Llull in Barcelona, Spain. She was a grant recipient of the European Union Marie Curie Fellowship for the project "A Networked and IT-Enabled Firm's Approach to Crisis Management". Her research focuses on organizing processes in extreme environments.