



Interpreting cyber-energy-security events: experts, social imaginaries, and policy discourses around the 2016 Ukraine blackout

Lars Gjesvik & Kacper Szulecki

To cite this article: Lars Gjesvik & Kacper Szulecki (2022): Interpreting cyber-energy-security events: experts, social imaginaries, and policy discourses around the 2016 Ukraine blackout, European Security, DOI: [10.1080/09662839.2022.2082838](https://doi.org/10.1080/09662839.2022.2082838)

To link to this article: <https://doi.org/10.1080/09662839.2022.2082838>



© 2022 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group



[View supplementary material](#)



Published online: 16 Jun 2022.



[Submit your article to this journal](#)



Article views: 339





[View related articles](#)



[View Crossmark data](#)

Interpreting cyber-energy-security events: experts, social imaginaries, and policy discourses around the 2016 Ukraine blackout

Lars Gjesvik  and Kacper Szulecki 

Norwegian Institute of International Affairs (NUPI), Oslo, Norway

ABSTRACT

The digitalisation of the energy system brings out the question of cyber threats. How this area is perceived and how cyber-security policy in the energy sector develops is driven by the most spectacular cyber-incidents. How do these events shape public perceptions about the dangers of digitalisation? To understand this, we look at the 2016 CrashOverride cyberattack on Ukraine's grid. Hypothesising that cyber-energy security incidents are interpreted in the context of socio-technical imaginaries of the energy sector and security imaginaries linked to foreign policy, we distil four discourses that emerged around the Ukraine attack among Western experts and commentators. One represented it as evidence of an accelerating race towards disaster, another as merely a tip of the iceberg. The third portrayed it as less catastrophic than initially suggested, while the last one as part of Russia's cyber strategy. Not all of these were picked up by the broader public debate in Western security circles, and only the more alarmist discourses had a visible impact beyond niche communities.

ARTICLE HISTORY

Received 30 January 2022
Accepted 24 May 2022


KEYWORDS


Energy security; cyber-security; CrashOverride; Industroyer; private security expertise; imaginaries

Introduction

It will likely end with a calamitous cyber induced cyberattack. Something that would take out the grid, that could contaminate our water, that could hold hospitals to ransomware, so they have to turn away patients. Every piece of that we have seen, we saw Russia take out the power in Ukraine [...] (Nicole Perroth on the Lawfare Podcast 19 March 2021)

"Energy security" is often used as shorthand for the state's ability to secure affordable supplies of strategic fossil fuels (Yergin 2006). As modern lifestyles become increasingly dependent on energy, particularly electricity, understandings of energy security have evolved to account for the all-encompassing and complex nature of energy systems (Ciută 2010, Cherp and Jewell 2014). Once relatively static, centralised, and predictable, power grids are changing into multi-nodal and digital mega-machines with thousands of elements in constant motion (Szulecki and Kuszniir 2017). Combined with the rapid

CONTACT Kacper Szulecki  kacper.szulecki@stv.uio.no, kacper.szulecki@nupi.no

 Supplemental data for this article can be accessed online at <https://doi.org/10.1080/09662839.2022.2082838>.

© 2022 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group

This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives License (<http://creativecommons.org/licenses/by-nc-nd/4.0/>), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited, and is not altered, transformed, or built upon in any way.

uptake of digital innovation in other areas, epitomised by the idea of “smart” – phones, TVs, fridges, cities, lives – this evolution is also fuelling concern regarding cyber threats and their containment. As a result, concern over the cyber security of energy systems has become more commonplace (EECSF 2017), and it is discussed together with other areas of security and policy notions such as “digital sovereignty” (Madiaga 2020).

Despite the apparent consensus about its importance, the energy sector’s cybersecurity remains elusive. Defining what cybersecurity means for the energy system largely stems from the interpretations of a handful of key incidents, yet “despite the centrality of cyber-incidents in the cyber-security discourse, researchers have yet to understand their link to, and affects on politics” (Balzacq and Cavelti 2016). Hence, this paper seeks to examine how a cybersecurity incident is understood and interpreted by experts and how those interpretations affect understanding of the insecurities of the energy system.

To understand this, we look at the attack on the Ukrainian power grid in late 2016 dubbed *CrashOverride/Industroyer* (henceforth *CrashOverride*). Due to Russian intelligence-linked actors, the blackout lasted a few hours. It had a little material impact and was a relatively insignificant event in terms of damages and cost. Still, the incident and the malware used have played a large role in shaping how experts think about effective countermeasures, how policymakers act upon cyber threats, and how the broader society imagines cyber security. The incident is, therefore, emblematic of the role of representations and interpretations in creating security threats and the policies to address them in the period immediately preceding the February 2022 Russian invasion of Ukraine.

This paper makes three main contributions. Firstly, it adds to the growing literature on the socio-technical practice of cyber-security politics (Betz and Stevens 2013, Dunn Cavelti 2018, Dunn Cavelti and Wenger 2020, Liebetrau and Christensen 2021) by analysing the interplay between private sector expertise and the development of policy. Our analysis responds to Dunn Cavelti’s call to “focus on cyber-security as social practice – enacted and stabilized through the circulation of knowledge about vulnerabilities – and a focus on the practices employed in the discovery, exploitation and removal of those vulnerabilities” (Dunn Cavelti 2018). Secondly, it speaks to the small but growing literature that is emerging on the frontier of Information Technology, critical infrastructure security studies and interdisciplinary energy studies, which seek to grasp the nature and specificity of cyber threats towards the energy system (Qi *et al.* 2016, Maglaras *et al.* 2018, Mrabet *et al.* 2018, Sun *et al.* 2018), and which is likely to expand in the aftermath of the Russia-Ukraine war. Finally, it examines how expert analysis is selectively taken up into broader public discourses, offering a heuristic device complementing existing understandings of the influence of expertise on contemporary politics (Berling and Bueger 2016).

We start out putting the issue of cyber-energy security in the broader context of the increasing digitalisation of energy systems. Subsequently, we offer a theoretical framework drawing on the technopolitical role of experts and the concept of social imaginaries – collectively held meaning structures that enable the interpretation of social reality in specific realms, such as energy and security. In the empirical analysis, we first detail the incident itself and how it was interpreted in two private security firm reports published in the summer of 2017 that shaped its subsequent understandings. We identify four

main representations used to make sense of the incident before tracing how the incident impacted the broader public discourse in English-language media, teasing out which representations were taken up to inform policy in Western (i.e. NATO and European Union countries) and which were not. We show how a public discourse selectively engages with certain representations, making a small blackout in Ukraine representative of wider security concerns about the energy grid.

Cyber security in the energy sector

As energy transitions unfold and face rapid digitalisation, *cyber-security* of energy systems becomes an increasingly important issue. Digitalisation involves unrolling new technological solutions within existing energy systems, most importantly, Supervisory Control and Data Acquisition (SCADA) systems used by system operators to coordinate the increasingly distributed energy generation. Another element is smart grids and the Internet of Things (IoT), consisting of “potentially millions of online nodes, [making it] most vulnerable to significant cyberattacks” (Kimani *et al.* 2019, p. 39). The energy transition towards a system based on intermitted and dispersed renewables is likely to require blockchain to achieve the computational power necessary for steering and coordination (Glachant and Rosetto 2018, DENA 2019). The imagined future grid can become vulnerable to new kinds of threats, which are uncertain, often unknown, and difficult to grasp within existing energy security approaches.

However, the interdisciplinary research programme of energy security studies, rooted in the social sciences, is visibly lagging behind theoretical and real-world developments related to cyber-security. Existing approaches, even if they take a systemic perspective on energy supply chains (Hughes 2012, Cherp and Jewell 2013, 2014, Johansson 2013, Molyneaux *et al.* 2016, Kester 2018), are more preoccupied with the material/ideational tension between energy infrastructures, institutions, and practices, and can only accommodate cyber threats as an exogenous source of risks – “intentional” or “unpredictable” (Cherp and Jewell 2014). However, as energy security debates evolve away from the preoccupation with physical supply and the fear of scarcity (Kester 2022) and towards understanding security as the low vulnerability of energy systems (Cherp and Jewell 2014), the opportunity for integrating cybersecurity concerns opens.

Meanwhile, Security Studies’ writing on cyber security has evolved from a practical focus on the risks inherent in digitalisation and subsequent “doomsday” scenarios to more granular investigations, such as the dynamics of cyber-securitisation (Dunn Cavelty and Wenger 2020). Within this growing research field, a more stringent focus on the socio-technical practices of cyber security has been staked out as an agenda worth pursuing (Stevens 2018) among several articles on the topic (Dunn Cavelty 2013, Stevens 2015, Gomez and Villar 2018, Dunn Cavelty 2019).

Tentatively, this literature has started exploring the relationship between the social construction of threats and the inanimate objects of cyber security (Banks 2015, Balzacq and Cavelty 2016, Dunn Cavelty 2019). Examining what an inanimate object “does” for security also requires seeing it in the context of its interpretations. This is even more vital when examining the overlap of energy security and cyber security, as the overlap of two large technological systems makes the energy sector the perfect “bogeyman” for cyber security studies, illustrating the merits of studying cyber threats

and borrowing energy's potential for catastrophe, without really engaging with energy security as such.

Another related literature has examined the critical role of experts, often located in the private sector, in making sense of and developing digital and energy policy. Traditionally, it is the state that is tasked with ensuring security for its citizens, but in western states, it increasingly relies on the private sector in creating, governing and defining cyber security as well as exerting various forms of power in the digital domain (Powers and Jablonski 2015, Carr 2016, Bures and Carrapico 2017, Maurer 2017, McCarthy 2018). As energy and cyber security are relatively small fields in their own right, the combination of concerns makes for a niche in societal security filled by many private firms and consultants (Slayton and Clark-Ginsberg 2018). As a result, the dynamics of security privatisation, public–private partnerships, and the multitude of actors involved in producing cyber-security have remained a staple in cyber-security studies (Bureš and Carrapiço 2018, Collier 2018).

Research has primarily looked at various governance arrangements, the role of the private sector and of the epistemic community of “cyber experts” in maintaining security (Shires 2018, Tanczer *et al.* 2018). Yet, attention has shifted recently towards the role private firms play in shaping how cyber security is made sense of as well (Collier 2018, Lawson 2013, Stevens 2020), by, for example, investigating the practices involved in the attribution of cyber incidents (Egloff 2020). As technical knowledge to interpret cyber-energy incidents remains limited, statements and analyses by industry experts are crucial to inform policy and shape the public understanding of these incidents (Lee and Rid 2014, Rid and Buchanan 2015). Cyber-energy security is a political issue where experts play a central role in providing authority and legitimacy to certain frames and understandings. In this capacity, experts reformulate singular events as manifestations of larger phenomena, which become issues that policies attempt to solve (Bigo 2002, Aradau 2010, 2014, Balzacq *et al.* 2010, Rychnovska *et al.* 2017).

While the political role of such “cyber experts” has for a long time been relegated to the sidelines in cyber security, recent scholarship has put it at the centre of analysis, highlighting their importance in the making of cybersecurity (Tanczer *et al.* 2018). Combining lessons from the social construction of threats and risks, the importance of non-state actors in digital politics, and the critical role played by experts in interpreting and making sense of the complexities of contemporary politics, research has stressed how cyber experts play a notable and important role in our understanding of cyber security (Willers 2021a, 2021b).

Building on this work on the role of experts in cyber security and speaking to and drawing on the three literatures outlined above, this article examines how a single incident, and the malware at the heart of it, became understood and interpreted by a small expert community. The representations put forward were, in turn, filtered through a multitude of actors that adopted or rejected them from the expert community.

Theoretical approach and method

To understand how cyber-security incidents in the energy sector affect the public debate, we have to ask what actors are involved in explaining and interpreting the event, what existing collective systems of meaning do they draw, and which interpretations are

later picked up by the broader audiences and policymakers. To unpack this process, we first look at the (cyber)security experts and then analyse their representations of the incident, nested in broader structures of knowledge on the cyber and energy sectors (Figure 1). As these incidents take place on the overlap of energy, cyber and foreign policy spheres, we build on the concept of social imaginaries – socio-technical imaginaries of energy futures and security imaginaries of (inter)national pasts – to theorise the systems of meaning from which specific representations emerge.

Experts

The technical complexities that characterise digital and energy systems require definition, translation, and categorisations to make the security concerns and risks legible and governable (Amoore and Goede 2008, p. 13). Such interpretative work is being done by a group of cybersecurity professionals whose competencies or professional experience have important roles in shaping domestic public policies and even foreign and security policy (Haas 1992, Bigo 2002, Blyth 2003).

How can technological experts influence security, let alone foreign policy responses? In regular circumstances, experts act as interpreters, making complex systems such as the power grid governable by non-specialist policymakers. The very uncertainty and ambiguity of contemporary policy problems bolster and reinforce experts' claim to authority and influence (Beck 1992, Giddens stampa 1992, Henriksen and Seabrooke 2016), which is enhanced in times of crisis and emergency. Similarly,

when a crisis situation breaks out, whether it is a major accident, a catastrophic event, an environmental disaster, a terrorist attack or a military conflict, experts explain to us what has happened and what should be done next ... Experts also provide means to identify what is dangerous and what is not. (Berling and Bueger 2016)

The main difference, however, is that such emergency situations – as the COVID-19 pandemic clearly shows – reduce the space for deliberation and critical reflection, thus empowering experts beyond their usual capacity.

Contemporary security politics are, in part, imagined, created, and solved by the same group of professionals, who, by identifying a security concern, define the problem and the solution. This ability to speak on behalf of uncertain and unpredictable events with authority affords experts with influence (Hansen and Nissenbaum 2009). And so, the power and legitimacy of security experts' rests in part on the urgency resulting from security

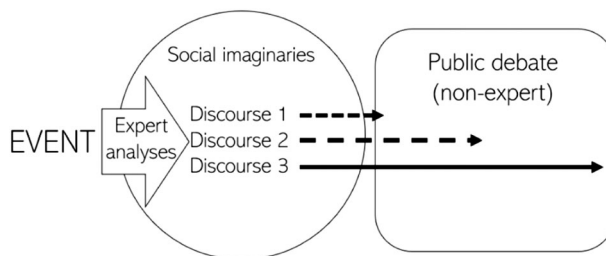


Figure 1. Theoretical model: experts, social imaginaries, and the influence on public debate.

incidents – that is events that these experts themselves identify and represent as security incidents. Experts become “professionals of unease” (Bigo 2002).

While experts in this capacity act as interpreters of incidents, the effects these interpretations have on the broader society might not always be those intended by the experts. The authority of experts cannot be claimed unilaterally but requires acceptance and recognition by a broader audience (Boswell 2008, Sending 2015, 2017, Seabrooke *et al.* 2020). In addition, portraying experts as empowered to frame incidents as they see fit, obscures tensions and fissures within expert communities themselves. Such portrayals stress how the authority of experts and the acceptance of their representations are always contingent on how they are received, a process of recognition that might not always play out as intended.

As alluded to by the debate in cybersecurity circles over the persistent hype surrounding cybersecurity (See, for example Lee and Rid 2014), experts might simultaneously provide the cognitive frames used to make sense of incidents and be displeased by how those frames are taken up and used politically. Disentangling the real effect of experts on political discourse ought to consider the vital role played by such experts in framing incidents and their relative powerlessness in controlling how those frames are used and taken up.

Social imaginaries

What happens when a cyber incident occurs? The task of experts is to deal with the incident and interpret it and narrate it for the broader public, firstly other experts and policy-makers, and ultimately journalists and the society at large. This interpretation does not occur in a void, and it is not reducible to the technological “fact”, as due to the degree of uncertainty and the socio-technical character of cyber space and the energy system, each interpretation is mediated through pre-existing structures of meaning. We draw on social imaginaries to conceptualise these structures in which cyber-energy security experts and their audiences are embedded. Social imaginaries, rooted in Durkheim’s notion of “collective representations”, are “collective systems of meaning that enable the interpretation of social reality” (Jasanoff and Kim 2009). Their central capacity is the “creative reinterpretation of the historical past” regarding new events or future projects (Adams and Smith 2019). Imagination, allowing for creative interpretation, is thus itself a social fact and “an organized field of social practices” (Appadurai 1996).

However, while social imaginaries writ large contain collective visions of social order and “a good life”, that is, the desired outcomes of political interactions, there are also narrower and more issue-specific imaginaries that allow actors to make sense of events occurring in particular spheres of social life. Those relevant for our analysis are *socio-technical imaginaries* and *security imaginaries*.

Jasanoff and Kim cast socio-technical imaginaries (STI) as collectively imagined forms of social life and social order that centre on the design and fulfilment of scientific and technological projects (Jasanoff and Kim 2009). These powerful cultural resources help shape social responses to innovation and change and are the “unique features of political cultures that serve to define what modifications of daily life are rational and desirable” (Tidwell and Tidwell 2018). Socio-technical imaginaries “reside in the reservoir of norms and discourses, metaphors and cultural meanings out of which actors build their policy

preferences” (Jasanoff and Kim 2009, p. 123). They are collectively held, but a central role in their reproduction and re-articulation rests with technocratic experts, while technopolitics grounded in STI may shape the broader political sphere. An important feature of STIs is their potential to inform (de)securitisation processes; imaginaries “warn against risks or hazards that might accompany innovation if it is pushed too hard or too fast. In activating collective consciousness, imaginaries help create the political will or public resolve to attain them” (Jasanoff and Kim 2009).

Similarly, Weldes defines security imaginaries (SI) as collective meaning structures that help make sense of social reality but are specific to foreign policy and state security. They are the “intersubjective and culturally embellished meanings on the basis of which state officials make decisions and act”, and a state’s security imaginary “provides what might be called the cultural raw materials out of which representations of states, of relations among states, and of the international system are constructed” (Weldes 1999). Security imaginaries can be drawn upon in casting issues as problems of security, as they enable representations that clarify for state officials and others who and what “we” are and who “our enemies” are, how we are threatened by them and how we might best deal with those threats.

Cyber-energy security: the overlap of socio-technical and security imaginaries

Cyber-energy security, we propose, is stretched between these two imaginary poles, the socio-technical and the security imaginary. Similar to Dunn-Cavelty’s ideas of cyber technologies as in part “apolitical, flawed, material objects that need to be fixed” and part “mere political tools in the hands of social actors” (Dunn Cavelty 2018, p. 1). While most sophisticated energy security theorisations, drawing on the idea of vital systems (Collier and Lakoff 2015), consider known and measurable impacts and risks (Cherp and Jewell 2011, 2014, Szulecki 2017), the relative novelty of cyber-security threats and the perceived “technical” nature of the issues make them a peculiar security problem. Translating incidents largely relies on metaphors, analogies and “cognitive hooks” that can catch the attention of a broader public. Secondly, while the growth in real-world incidents over the last decade has made the problem less acute, there remains a persistent concern over “disasters” in cyber-security discourses (Stevens 2015) that make socio-technical and security imaginaries vital for making sense of the perceived threats and risks stemming from digitalisation.

Method: discourse analysis

Understanding that social imaginaries are never easily fixed, we have to assume that there are more than two possible representations and that interpretations of a cyber-incident drawing on socio-technical and security imaginaries to different extents can create a continuum.

We analyse these interpretations as policy discourses, constructing “problems, objects, and subjects [...] simultaneously articulating policies to address them” (Hansen 2006). Discourse analysis is a means to “interrogate the ways in which specific systems of meaning-production have been generated, circulated, internalized, and/or resisted” (Dunn and Neumann 2016) through the close study of language in use. While focusing on socially

constructed and reproduced meanings – representations – discourse analysis constitutes “real world research” (Hansen 2006, p. 5), the ultimate aim is to show how much discourse matters for political practice, policy change and state action. Our goal is to analyse the representations of CrashOverride, uncovering the elements of socio-technical and security imaginaries that underpin them, and re-assembling them into identifiable representations that can be traced in policy discourses.

There are two important steps for conducting discourse analysis: identifying a corpus of relevant texts and only then analysing these texts in depth. We used combined data scraping and media analysis tools (Media Cloud) to identify critical texts and reports. Among 944 texts identified via data scraping, several reports and articles were cross-referenced by most others and were instrumental for setting the debate on CrashOverride. The two reports published in June 2017 and the most influential articles in the dataset,¹ constitute the core of the corpus. In addition, a similar dataset was constructed based on broader representations of energy/cyber security. These were complemented by manual searches in the 20 most influential online news outlets from the two datasets. The total corpus consisted of 180 texts, and a full bibliography of sources used for analysis can be found in the Appendix.²

The second step, conducted through a close reading of these texts, is an example of what Mutlu and Salter called elastic discourse analysis, oriented on tracing “new relations between signs, tropes and metaphorical schema” (Salter and Mutlu 2013), such as, in our case, socio-technical and security imaginaries of cyber and energy.

For this paper, limitations in language proficiencies and the selection of sources have introduced an anglophone bias in the corpus and the subsequent analysis. This bias can partly be explained by the transnational cyber-security community and the debates on cyber-incidents being predominantly anglophone, thus representing a broader bias in cybersecurity. Moreover, the selection criteria of media centrality in the corpus reinforce this bias by privileging sources with a global reach, which often are English-language sources.

While this bias is problematic, we argue that for the context of this paper, our approach is defended. Firstly, we are interested in the technical effect reporting has on the public discourse on cyber security. As shown in our analysis, the primary reports depicting and explaining the incident targeted an English-speaking audience, which, in turn, made outlets based in the United States, and to a lesser extent, the United Kingdom, central for initial reporting on the incident. Secondly, the initial reports were referenced by institutions (e.g. CERTs) in many European countries, and our experience with the European cyber-security community suggests that our findings apply to this context .

Analysis: making sense of CrashOverride

Background

The night between 17 and 18 December 2016, a power outage affected the Kyiv region for roughly an hour before the supply was restored. The incident was immediately speculated to be the result of a digital operation, and on 18 December, the head of Ukraine’s national transmission system operator Ukrenergo, suggested the attack could be ascribed to “an external interference through data networks” (Kovalchuk 2016).

This fit into the broader picture of the on-going Ukrainian conflict, as Ukrainian power stations had been affected by a cyber attack almost exactly a year before. Since Russia's annexation of Crimea in March 2014, the proclamation of the so-called Donetsk and Luhansk Republics in April 2014, and the following intervention of Russian forces on Ukrainian territory, the two states have been in a de facto war, which was dubbed "hybrid" due to the variety of unconventional and non-military means employed.

The incident centred on a high-voltage transmission substation, which is "automated and remotely controlled, while smaller ones maybe electro-mechanically operated and are certainly unsupervised" (Carullo 2016). Weeks later, the BBC reported that preliminary investigations confirmed a cyber attack as the likely culprit, according to the Ukrainian Security Firm ISSP. Initially, the incident was not seen as a new type of attack, rather fitting within the pattern of previous incidents. As Oleksii Yasnskiy, the head of ISSP, put it: "The attacks in 2016 and 2015 were not much different – the only distinction was that the attacks of 2016 became more complex and were much better organized" (BBC 2017). These initial reports were light on details and technical specifications, focusing instead on the context of the Ukraine-Russia conflict.

Narrating the incident: ESET and Dragos reports

On 12 June 2017, two independent but partly collaborating investigations into the incident appeared. The first report was published by the Slovak cyber-security firm ESET and described the workings of a new type of malicious software (shorthand: malware) utilised in the power outage. Later the same day, the US cyber-security firm Dragos described the same malware with some additional information. Both companies proposed names for the malware, with ESET's report ominously titled "Industroyer: Biggest malware threat to critical infrastructure since Stuxnet" (ESET 2017), while the Dragos report was called "CrashOverride – Analysis of the Threat to Electric Grid Operations" (Dragos 2017).

Both reports stressed the novelty and sophistication of the malware, especially when contrasted with previous attempts at affecting critical infrastructure through cyberattacks. ESET stated, for instance, that "the relatively low impact of December 2016's blackout stands in great contrast to the technical level and sophistication of the suspected malware behind Industroyer" (ESET 2017), while Dragos noted that "CrashOverride represents an evolution in tradecraft and capabilities by adversaries who wish to do harm to industrial environments" (Dragos 2017, p. 8).

They also gave a detailed, expert account of the incident and malware, with some key differences. The ESET report narrated the incident primarily through what-if scenarios more than actual effects concluding that it "can be used to attack any industrial control system" (ESET 2017). While Dragos in a corollary to the report, stressed that it "should not be taken with any 'doom and gloom' type scenarios", they nonetheless noted that there are "concerning scenarios" wherein outages could be extended "into a few days" (Lee 2017). Arguing that "this (analysis) should be a wake-up call for those responsible for the security of critical infrastructure (systems) worldwide" (ESET 2017) and that "adversaries are getting smarter, they are growing in their ability to learn industrial processes and codify and scale that knowledge, and defenders must also adapt"

(Dragos 2017, p. 11). The role of the malware is mainly important as a signifier of how future scenarios could play out.

The two reports published by private security firms laid the foundation for what was to become the accepted depiction of the incident, eclipsing the actual power outage in significance as the major news story. Beyond mass media, a host of institutions, security companies and experts have referred to and reinforced the perceptions put forward by the two reports (Accenture Consulting 2017, Incibe CERT 2017, Kaspersky 2017, UK National Cyber Security Centre 2017, US CERT 2017b, Bundesamt für Sicherheit in der Informationstechnik 2018), thereby further establishing them as the primary sources of knowledge of the incident. Once the incident was narrated, different actors began re-interpreting it within the context of different social imaginaries – either the socio-technical imaginaries of the digitalised energy system or (national and Western) security imaginaries. This generated divergent policy representations, as the following sections will show.

The two reports published by private security firms became the established depiction of the incident, eclipsing the actual power outage in itself in significance, the major news story dominating headlines in the outlets covering cyber-security and subsequently reaching the wider social and political. Beyond mass media, a host of institutions, including public cybersecurity agencies in the UK, Germany and the US (Incibe CERT 2017, UK National Cyber Security Centre 2017, US CERT 2017b, 2017c, Bundesamt für Sicherheit in der Informationstechnik 2018, U.S. CERT 15703/2018), as well as security companies (Accenture Consulting 2017, Kaspersky 2017) have referred to and reinforced the perceptions put forward by the two reports immediately after they were published, the US Computer Emergency Response Team (CERT) issued a warning for the public, referencing the reports, legitimising the analysis for a wider public (US CERT 2017c). Subsequent statements by the Department of Homeland Security referenced the Dragos and ESET reports (in addition to a warning published by US CERT), thereby further establishing them as the primary sources of knowledge of the incident (US CERT 2017a).

Representation 1: an accelerating race towards disaster

When they established the malware as a security problem, the cyber-experts at Dragos and ESET made sense of the 2016 incident along the socio-technical dystopian notion of the digitalising energy system as a worsening problem, as *an accelerating race towards disaster*. Representation of cyber incidents such as the one in Ukraine within the premises of this socio-technical imaginary lets them take on significance as harbingers of things to come and allows practitioners to detour the actual effects of the incident, instead of calling attention to the worrying *trend* as the real security problem to be dealt with.

Unlike typical national socio-technical imaginaries, which appear to be “dreamscapes” of energy futures, the digitalising energy system’s imaginary has a nightmarish and dystopian undertone. It draws attention to CrashOverride as a data point on an (imagined) trend. The important features of the malware are only understood considering other incidents that are deemed comparable. The history of targeting critical infrastructures using digital tools becomes a narrative of growing sophistication. What matters is not so much the malware and its functions as the assessment that by building on features seen in

previous attacks, it “did all of these things with added sophistication in each category” (Dragos 2017, p. 11).

Fears of a potentially more dangerous future stem from imaginaries tied into the techno-politics of digitalisation, and a perceived intention to be more reckless with digital technologies. The race towards disaster is grounded in the security challenges of the technology and the idea that malicious actors are looking to cause ever-increasing harm. This imaginary allows for the modular build-up of the malware, comprising interchangeable parts that can be swapped with others, to act as proof of an intention to cause more harm (Cherepanov 2017, p. 15).

Representation 2: the tip of the iceberg

A second representation does similar work in raising the severity of the blackout. At some point in the future “real cyberwar” will be unleashed, and the pent-up arsenals of militaries and intelligence agencies will be revealed. Its representation as a tip of the iceberg stems from the malware being understood as existing in an ambiguous state between offensive and defensive. Understood as both simultaneously, that is both as the early stages of a more destructive campaign and as a defensive operation, malware can “fuse cyber offense and cyber defense, to make them indistinguishable” (Kaplan 2016).

Furthermore, with the most advanced capabilities housed in intelligence agencies shrouded in secrecy, the exact nature and extent of these capabilities are unknown to all but a few insiders. Such ambiguities allow malware like CrashOverride to act as signals of far-worse capabilities that are unproven and not-yet-utilised by malevolent actors. This representation emerges from the meeting point of socio-technical imaginaries of the expanding cyber-network and power grid, and the security imaginaries portraying (particularly Western) developed societies as vulnerable to unexpected attacks from malicious and omnipresent but increasingly powerful (often non-state) actors.

Sharing the belief in the existence of far more sophisticated malware, both reports represent the 2016 incident as a test more than an actual attack. Taking a somewhat differing stance on the seriousness of the attack, both conclude a likely explanation was it being “more of a proof of concept than what was fully capable in the malware” (Dragos 2017, p. 11) or “a large-scale test” (ESET 2017).

The limited and short-lived impact of the incident is therefore not indicative of how a similar incident might play out, given that the metaphorical gloves come off. The seriousness of any malware is inexorably linked to the actor who created it, assuming that their real capabilities go well beyond the effects produced by the actual malware. This type of logic hinges on the assumption that “advanced actors” in cyber-space, most commonly denoting well-funded intelligence agencies or similar institutions, possess capabilities, competencies, and tools far beyond what is publicly known.

Representation 3: the end is not near

Appearing simultaneously as the representations portraying the incident as dangerous was a related attempt to play down what was perceived to be hyperbole. Directly challenging the two other representations, this approach drew attention to the relative security

of the grid and the built-in resilience of modern infrastructures. Stressing how security is improving, the representation of the cyber-energy nexus suggests that *the end is not near*.

Rather than a foreboding tale of the dangers of technology, this representation draws on a positive imaginary of a future wherein security for the grid is achieved. While not necessarily a “dreamscape”, the future to be achieved is utopian because the grid is secure and resilient enough. Improved technologies for detection and mitigation, and the tireless work of the cyber security community, promise a future of ease of mind and trust that the grid will continue operating. Rather than arguing that catastrophe is imminent due to worsening problems and dangers lurking under the surface, this representation, therefore, mobilises positive imaginaries to put forward a benign representation of the incident.

Of the two, this representation is by far more prominent in the Dragos report, which also made several attempts to scale down the concerns that followed. The report drew both on an image of the grid itself as a “well-designed system” (Dragos 2017) that was built to be “reliable and safe which has a natural byproduct of increased security” (Dragos 2017). The technologies developed to maintain security, in conjunction with vigilant security professionals, “can ensure that security is maintained” (Dragos 2017), because “as always, the defense is doable” (Dragos 2017).

Partially this representation used a positive spin on the grid’s security to argue that the incident should not drastically alter perceptions. It also highlighted the myriad challenges for anyone attempting to construct a malware able to cause widespread blackouts over longer periods. And finally, as illustrated above, it also drew upon positive depictions of the security expert community and its ability to prevent incidents. At times, this representation directly contradicted the negative portrayals of the incident. Subsequent investigations into the non-deployed parts of the malware contrasted the idea that these represented a test with an idea of a component that had failed (Slowik 2018).

Representation 4: Russia’s grand cyber-strategy

The incident received attention not only for its implications for cyber-energy security but also for how it tied into ideas of the motives and operations of the Russian Federation, which cast the incident as part of *a Russian grand strategy*. The 2016 blackout was represented equally as a Russian attack as a cyber-security incident. A similar event taking place elsewhere would probably gain less attention and spawn different interpretations. However, in parallel to the cyber-security expert-driven debate, CrashOverride gained additional meanings as an element of an on-going interstate conflict – a “hybrid” war.

This brings to the fore the question of Russian agency and national interests and the issues of intentionality and broader strategy. If CrashOverride is not merely a matter of technology but an element of foreign policy, it is interpreted within a pre-existing security imaginary, allowing all prior knowledge of Russia, its goals, practices and intentions, to be grafted onto the cyber-security discourse. Digitalisation, which is independent of foreign policy developments, plays an important role in enabling these wargame scenarios.

An important consequence of interpreting CrashOverride through the Western security imaginary, easily discernible in the commentariat’s and analysts’ coverage of Russian foreign policy, is the assumption of a broad strategic vision, in which every new move is seen not as an event in itself but a step up a ladder. However, Western scholars, as

well as Russian émigrés and more independent commentators within Russia, have signalled that this assumption of a long-term strategy (Sakwa 2014, Hill 2016, Galeotti 2019), planted in the Western security imaginary by Cold War “Kremlinology”, is misleading (Lukyanov 2016).

Technical representations in public discourse

In the broader public debates, the representations were selectively adopted. Portrayals of the incident as representative of an accelerating race to the disaster were picked up and disseminated. The increasing sophistication of the malware compared to previous incidents was portrayed as “a game changer” (Nakashima 2017) and “as scary as it sounds” (Hern 2017). The incident was notable not only for the step forward it represented but the accelerating pace with which developments were going, noted as “I knew we were going in this direction but I didn’t think it would be this soon” (Weise 2017). The perception that cyber-energy-security was a rapidly evolving concern saw articulations of a future where “cybergangs hold the power grid of entire cities for ransom” (Collagnier 2018).

Thus, most of the media publications accepted the implicit assumption that the incident was primarily concerning as a part of a broader trend towards a future where cyber incidents cause widespread harm (Untersinger 2019), perhaps most clearly expressed as a timeline of ever-more daring and threatening incidents (Livingston *et al.* 2019).

Similar to the imaginary of an accelerated race to disaster, portrayals of the incident as the tip of the iceberg were widely picked up by media coverage depicting it as a “test before a greater attack” (Cimpanu 2017). It was claimed that “CrashOverride could go even further, causing physical destruction by carrying out a well-crafted attack on multiple points in a power grid” (Greenberg 2017). The notion that the attack was supported by a nation-state gave further credibility to the “test” narrative and the idea that the limited damage was intended, as a determined attacker could target Washington DC and “take it out for two months without much issue” (Greenberg 2017).

That the malware was traced back to actors tied to Russian intelligence was similarly influential. When the New York Times suggested that Russian hackers were targeting the US power grid, both the 2016 and the 2015 Ukrainian blackouts were used to frame and enlighten the development (Sanger 2018), and similarly on allegations that the US was targeting the Russian power grid (Sanger and Perlroth 2019).

Of the representations put forward in the reports, the imaginary of the grid as resilient and defensible was largely omitted. Subsequent attempts by Dragos, in particular, to scale down the concerns did not receive the same traction and coverage, having far less impact in the media landscape than the original report. Thus, this representation did not seep into the broader public debates to the same degree, and counterclaims that likely scenarios were the malware “not cataclysmic and would result in hours, potentially a few days, of outages, not weeks or more” (Dragos 2017) were largely left out of the discourse.

In sum, the representations of CrashOverride that travelled into the public discourse portrayed the digitalised energy system as particularly vulnerable and threatened. Resultingly, calls for continued investment and attention to the insecurity of the energy grid

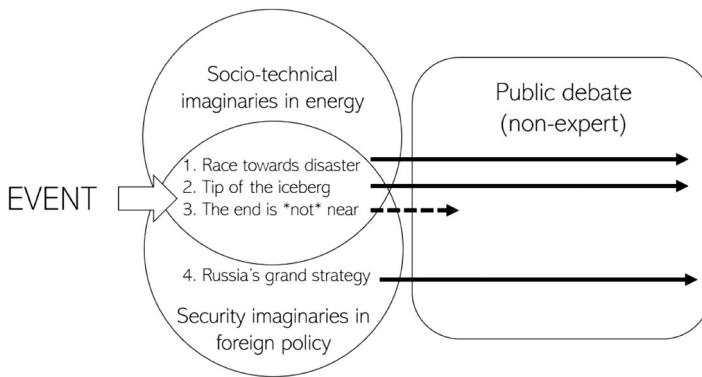


Figure 2. Expert representations and their adoption in public debates.

were made based on a widely held notion that these systems are fundamentally insecure (Brenner and Clark 2017, Weaver 2017). Within this framing, the danger in non-investment is that of societal collapse, and the fear is justified by extrapolating single events to a diverse set of worst-case scenarios and fears. CrashOverride and similar incidents acted as symbols that can explain and legitimise action by tying imagined scenarios to the real world, where lack of attention is “the kind of thing that causes lives to be lost, through accident or poor preparation” (Sheridan 2018) (Figure 2).

Conclusion

This article explored how a security incident in the Ukrainian power grid, the 2016 blackout triggered by a novel malware, became understood through, and a part of, the shared collective imaginaries that underpin “cyber security”. By identifying four different representations of the incident put forward by several experts, from information security and foreign policy commentators, different imaginaries and the role they played in shaping these representations were laid out. Three of these representations were dystopian: they portrayed an intractable security problem that is only getting worse by growing technical sophistication and heightened political tensions. The fourth, however, put forward a distinctively positive spin by stressing the vital role of security professionals in managing and limiting the impacts of incidents such as the 2016 blackout.

The different representations, and the imaginaries they draw on, are the basis for policy discourses around the incident, yet not all representations are taken up in the broader debate. Primarily, the representations that took hold were those framing the incident as severe, inducing an emergency and calling policy action to a significant and acute problem. Representing the incident as part of an accelerated race to disaster, as the tip of the iceberg, and as evidence of a Russian master plan were all embraced, reinforced, and highlighted in coverage and policy discussion. Representing the incident as something else was attempted by experts in the information security community, yet these representations did not travel. Putting a positive spin on the incident by highlighting the role of improved security practices in limiting the impact of the incident was left out almost in its entirety.

While experts play a key role in putting forward representations and making sense of the incident, they do not own the discussion. Instead, frustration was evident within expert communities towards what they perceived as hyperbole, exaggeration and fear-mongering. Expertise is a potent source of power and influence in constructing our shared sense of the world, yet is also highly performative. As with any performance, the audience might not adopt the interpretation the experts desire or hold themselves. Simplifying complex problems necessitates shortcuts, but in simplifying CrashOverride, the narrative became more severe than the incident might have warranted, or at least this appeared to be the opinion of many of the experts that helped formulate the initial representations. The representations that took hold and the imaginaries that resonated were the ones that stressed urgency and emergency, not calm and professional ethos.

To some extent, this should not be surprising; the security of digital systems embedded in critical infrastructures is a significant security problem, and inducing an emergency is a way of calling attention to it. At the same time, by stressing and possibly exaggerating the severity of the problem, key nuances are lost. The problem with such omissions is making reality seem more dangerous than it might be, reinforcing a sense of helplessness in confronting a novel security problem. Moreover, by selecting the representations that “fit” policy-makers can use these representations to further proposals that do little for energy security but have negative side effects, such as continuing reliance on coal. Both developments are troubling if we construct cyber energy security as an intractable problem beyond solutions.

The 2016 incident played a similar role for the cybersecurity sector as the gas crises of 2006 and 2009 had for the European energy sector – a lesson and a wake-up call for some. With the growing attention to digital security among policy-makers and the broader public, unpacking the social construction of cyber security and the key role played by single incidents is more important than ever. Not least so in the wake of the Russian invasion of Ukraine, where digital technologies have played a diverse, complex, and often opaque role. As geopolitical tensions rise across Europe, the risk that misrepresentations of the dangers of digitalisation and dystopian hyperbole distorts public perceptions is something scholars ought to grapple with seriously. We urge researchers to move beyond anglophone sources, look at how incidents are understood differently in different societal contexts and towards deeper engagement with the build-up and political role of transnational networks of experts are key to understand better of such processes of social construction.

Notes

1. Influential measured as the highest-rated relevant articles in terms of media in links.
2. Outlets include: The Guardian, Tripwire, Vox, Utilitydive, SCMagazine, E&E News, BBC, Boston Globe, Lawfare, The Hill, MIT Technology Review, Bleeping Computer, ZD Net, Forbes, Vice, Foreign Policy, The Conversation, USA Today, Gizmodo, Christian Science Monitor, Reuters, Ars Technica, Wall Street Journal, Wired, NPR, CNet, Dark Reading, Infosecurity Magazine, Slate, Business Insider, The Hacker News, CNN, Le Monde, Cyberscoop, Newsweek, Washington Post, The Daily Beast, Bloomberg, New York Times, The Atlantic, War On The Rocks, Times of Israel, Telesur, TechCrunch, CBS News.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This work supported by the Norges forskningsråd [grant number 288744].

ORCID

Lars Gjesvik  <http://orcid.org/0000-0002-3199-6301>

Kacper Szulecki  <http://orcid.org/0000-0002-1835-3758>

References

- Accenture Consulting, 2017. Outsmarting grid security threats. Available from: https://web.archive.org/web/20190822092048/https://www.accenture.com/_acnmedia/pdf-62/accenture-outsmarting-grid-security-threats-pov.pdf#zoom=50 [Accessed 22 Aug 2019].
- Adams, Suzi and Smith, Jeremy C.A., eds., 2019. *Social imaginaries. Critical interventions*. London: Rowman & Littlefield International.
- Amoore, Louise and Goede, Marieke de, 2008. *Risk and the war on terror. Transferred to digital print*. Abingdon: Routledge.
- Appadurai, Arjun, 1996. *Modernity at large. Cultural dimensions of globalization*. 8. Print. Minneapolis: University of Minnesota Press (Public worlds, 1).
- Aradau, Claudia, 2010. Security that matters: critical infrastructure and objects of protection. *Security dialogue*, 41 (5), 491–514. doi:10.1177/0967010610382687.
- Aradau, Claudia, 2014. The promise of security: resilience, surprise and epistemic politics. *Resilience*, 2 (2), 73–87. doi:10.1080/21693293.2014.914765.
- Balzacq, Thierry, et al., 2010. Security practices. In: R.A. Denemark, ed. *The international studies encyclopedia online*, 1–16. Oxford: Oxford University Press.
- Balzacq, Thierry and Cavelti, Myriam Dunn, 2016. A theory of actor-network for cyber-security. *European journal of international security*, 1 (2), 176–198. doi:10.1017/eis.2016.8.
- Banks, James, 2015. The heartbleed bug: insecurity repackaged, rebranded and resold. *Crime, media, culture*, 11 (3), 259–279. doi:10.1177/1741659015592792.
- BBC, 2017. Ukraine power cut “was cyber-attack”. *BBC Online*, 11 Jan. Available from: <https://www.bbc.com/news/technology-38573074>.
- Beck, Ulrich, 1992. *Risk society. Towards a new modernity*. Los Angeles, CA: Sage Publications (Theory, culture & society).
- Berling, Trine Villumsen and Bueger, Christian, eds., 2016. *Security expertise. Practice, power, responsibility*. London: Routledge, Taylor & Francis Group (PRIO new security studies).
- Betz, David J. and Stevens, Tim, 2013. Analogical reasoning and cyber security. *Security dialogue*, 44 (2), 147–164. doi:10.1177/0967010613478323.
- Bigo, Didier, 2002. Security and immigration: toward a critique of the governmentality of unease. *Alternatives*, 27 (1_suppl), 63–92. doi:10.1177/030437540202705105.
- Blyth, Mark, 2003. Structures do not come with an instruction sheet: interests, ideas, and progress in political science. *Perspectives on politics*, 1 (4), 695–706. doi:10.1017/S1537592703000471.
- Boswell, Christina, 2008. The political functions of expert knowledge: knowledge and legitimation in European Union immigration policy. *Journal of European public policy*, 15 (4), 471–488. doi:10.1080/13501760801996634.
- Brenner, Joel and Clark, David, 2017. What the Trump administration must do to protect critical infrastructure. 28 Mar. Available from: <https://web.archive.org/web/20190822172549/https://www.lawfareblog.com/what-trump-administration-must-do-protect-critical-infrastructure> [Accessed 22 Aug 2019].

- Bundesamt für Sicherheit in der Informationstechnik, 2018. Angriffs-Kampagne gegen EnergieFirmen und andere KRITIS-Sektoren. Available from: https://web.archive.org/web/20190826074736/https://www.eenews.net/assets/2018/06/20/document_ew_01.pdf [Accessed 26 Aug 2019].
- Bures, Oldrich and Carrapico, Helena, 2017. Private security beyond private military and security companies: exploring diversity within private-public collaborations and its consequences for security governance. *Crime law and social change*, 67 (3), 229–243. doi:10.1007/s10611-016-9651-5.
- Bureš, Oldřich and Carrapiço, Helena, eds., 2018. *Security privatization. How non-security-related private businesses shape security governance*. Cham: Springer.
- Carr, Madeline, 2016. *US power and the internet in international relations. The irony of the information age*. Basingstoke: Palgrave Macmillan.
- Carullo, Moreno, 2016. Attack on Ukrainian power company causes blackouts in Kiev. *ISBuzz News*, 22 Dec. Available from: <https://www.informationsecuritybuzz.com/expert-comments/attack-ukrainian-power-company-causes-blackouts-kiev/>.
- Cherepanov, Anton, 2017. *Win32/industrial. A new threat for industrial control systems*. Bratislava: ESET. Available from: https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industrial.pdf.
- Cherp, Aleh and Jewell, Jessica, 2011. The three perspectives on energy security: intellectual history, disciplinary roots and the potential for integration. *Current opinion in environmental sustainability*, 3 (4), 202–212. doi:10.1016/j.cosust.2011.07.001.
- Cherp, Aleh and Jewell, Jessica, 2013. Energy security assessment framework and three case-studies. In: Hugh Dyer and Maria Julia Trombetta, eds. *International handbook of energy security*. Cheltenham: Edward Elgar, 146–173.
- Cherp, Aleh and Jewell, Jessica, 2014. The concept of energy security: beyond the four As. *Energy policy*, 75, 415–421. doi:10.1016/j.enpol.2014.09.005.
- Cimpanu, Catalin, 2017. New “industrial” malware targets power grids. *Bleeping Computer*, 12 Jun. Available from: <https://web.archive.org/web/20170614044222/https://www.bleepingcomputer.com/news/security/new-industrial-malware-targets-power-grids/> [Accessed 25 Aug 2019].
- Ciută, Felix, 2010. Conceptual notes on energy security: total or banal security? *Security dialogue*, 41 (2), 123–144. doi:10.1177/0967010610361596.
- Collagnier, Jean-Marc, 2018. Cyberattacks are becoming a greater challenge for the energy industry. *Forbes*, 10 Jan. Available from: <https://web.archive.org/web/20190826093743/https://www.forbes.com/sites/jeanmarcollagnier/2018/10/01/the-next-cyberattack-staying-ahead-of-hackers-is-becoming-a-greater-challenge/> [Accessed 22 Aug 2019].
- Collier, Jamie, 2018. Cyber security assemblages: a framework for understanding the dynamic and contested nature of security provision. *Politics and governance*, 6 (2), 13. doi:10.17645/pag.v6i2.1324.
- Collier, Stephen J. and Lakoff, Andrew, 2015. Vital systems security: reflexive biopolitics and the government of emergency. *Theory, culture & society*, 32 (2), 19–51. doi:10.1177/0263276413510050.
- DENA, 2019. *Blockchain in der integrierten Energiewende*. Berlin: Deutsche Energie-Agentur GmbH (DENA Multi-stakeholder-studie).
- Dragos, 2017. *CrashOverride. Analysis of the threat to electric grid operations*. Hanover, MD: Dragos.
- Dunn, Kevin and Neumann, Iver, 2016. *Undertaking discourse analysis for social research*. Ann Arbor: University of Michigan Press.
- Dunn Cavelt, Myriam, 2013. From cyber-bombs to political fallout: threat representations with an impact in the cyber-security discourse. *International studies review*, 15 (1), 105–122. doi:10.1111/misr.12023.
- Dunn Cavelt, Myriam, 2018. Cybersecurity research meets science and technology studies. *Politics and governance*, 6 (2), 22. doi:10.17645/pag.v6i2.1385.
- Dunn Cavelt, Myriam, 2019. The materiality of cyberthreats: securitization logics in popular visual culture. *Critical studies on security*, 7 (2), 138–151. doi:10.1080/21624887.2019.1666632.

- Dunn Cavelti, Myriam and Wenger, Andreas, 2020. Cyber security meets security politics: complex technology, fragmented politics, and networked science. *Contemporary security policy*, 41 (1), 5–32. doi:10.1080/13523260.2019.1678855.
- EECSP, 2017. *Cyber security in the energy sector. Recommendations for the European Commission on a European strategic framework and potential future legislative acts for the energy sector*. Energy Expert Cyber Security Platform. Available from: https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf [Accessed 29 Apr 2020].
- Egloff, Florian J., 2020. Contested public attributions of cyber incidents and the role of academia. *Contemporary security policy*, 41 (1), 55–81. doi:10.1080/13523260.2019.1677324.
- ESET, 2017. *Industroyer: biggest malware threat to critical infrastructure since Stuxnet*. Bratislava: ESET.
- Galeotti, Mark, 2019. *We need to talk about Putin. Why the west gets him wrong*. London: Ebury Press, an Imprint of Ebury Publishing.
- Giddens, Anthony, 1992. *Modernity and self-identity. Self and society in the late modern age*. Cambridge: Polity Press.
- Glachant, Jean-Michel and Rosetto, Nicolo, 2018. *The digital word knocks at electricity's door. Six building blocks to understand why*. Florence: FSR (FSR Policy Brief).
- Gomez, Miguel Alberto and Villar, Eula Bianca, 2018. Fear, uncertainty, and dread: cognitive heuristics and cyber threats. *Politics and governance*, 6 (2), 61. doi:10.17645/pag.v6i2.1279.
- Greenberg, Andy, 2017. "Crash override": the malware that took down a power grid. *Wired*, 6 Dec. Available from: <https://www.wired.com/story/crash-override-malware/> [Accessed 22 Aug 2019].
- Hansen, Lene, 2006. *Security as practice. Discourse analysis and the Bosnian war*. New York, NY: Routledge (The new international relations). Available from: <http://site.ebrary.com/lib/alltitles/docDetail.action?docID=10163794>.
- Hansen, Lene and Nissenbaum, Helen, 2009. Digital disaster, cyber security, and the Copenhagen school. *International studies quarterly*, 53 (4), 1155–1175. doi:10.1111/j.1468-2478.2009.00572.x.
- Henriksen, Lasse Folke and Seabrooke, Leonard, 2016. Transnational organizing: issue professionals in environmental sustainability networks. *Organization*, 23 (5), 722–741. doi:10.1177/1350508415609140.
- Hern, Alex, 2017. This article is more than 2 years old "industroyer" virus could bring down power networks, researchers warn. *Guardian*, 13 Jun. Available from: <https://web.archive.org/save/https://www.theguardian.com/technology/2017/jun/13/industroyer-malware-virus-bring-down-power-networks-infrastructure-wannacry-ransomware-nhs> [Accessed 26 Aug 2019].
- Hill, Fiona, 2016. Putin: the one-man show the west doesn't understand. *Bulletin of the atomic scientists*, 72 (3), 140–144. doi:10.1080/00963402.2016.1170361.
- Hughes, Larry, 2012. A generic framework for the description and analysis of energy security in an energy system. *Energy policy*, 42, 221–231. doi:10.1016/j.enpol.2011.11.079.
- Haas, Peter M., 1992. Introduction: epistemic communities and international policy coordination. *International organization*, 46 (1), 1–35. Available from: <http://www.jstor.org/stable/2706951>.
- Incibe CERT, 2017. CrashOverride, the malware that sabotaged the electric grid. 12 Jun. Available from: <https://web.archive.org/web/20190822141520/https://www.incibe-cert.es/en/early-warning/cybersecurity-highlights/crashoverride-malware-sabotaged-electric-grid> [Accessed 22 Aug 2019].
- Jasanoff, Sheila and Kim, Sang-Hyun, 2009. Containing the atom: sociotechnical imaginaries and nuclear power in the United States and South Korea. *Minerva*, 47 (2), 119. doi:10.1007/s11024-009-9124-4.
- Johansson, Bengt, 2013. Security aspects of future renewable energy systems – a short overview. *Energy*, 61, 598–605. doi:10.1016/j.energy.2013.09.023.
- Kaplan, Fred M., 2016. *Dark territory. The secret history of cyber war*. First Simon & Schuster trade paperback edition March 2016. New York: Simon & Schuster.
- Kaspersky, 2017. Threat landscape for industrial automation systems in H1 2017. Available from: <https://ics-cert.kaspersky.com/wp-content/uploads/sites/6/2017/10/KL-ICS-CERT-H1-2017-report-en.pdf> [Accessed 23 Aug 2019].
- Kester, Johannes, 2018. *The politics of energy security. Critical security studies, new materialism and governmentality*. Abingdon: Routledge (Routledge explorations in energy studies).

- Kester, Johannes, 2022. The scare behind energy security: four conceptualisations of scarcity and a never-ending search for abundance. *Journal of international relations and development*, 25 (1), 31–53. doi:10.1057/s41268-021-00216-0.
- Kimani, Kenneth, Oduol, Vitalice, and Langat, Kibet, 2019. Cyber security challenges for IoT-based smart grid networks. *International journal of critical infrastructure protection*, 25, 36–49. doi:10.1016/j.ijcip.2019.01.001.
- Kovalchuk, Vsevolod, 2016. Facebook post. Post informing of the power outage on Facebook. 18 Dec. Available from: https://www.facebook.com/permalink.php?story_fbid=1798082313797621&id=100007876094707 [Accessed 29 Aug 2019].
- Lawson, Sean, 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. doi:10.1080/19331681.2012.759059.
- Lee, Robert M., 2017. CRASHOVERRIDE: analyzing the malware that attacks power grids. *Dragos.com*. Available from: <https://dragos.com/resource/crashoverride-analyzing-the-malware-that-attacks-power-grids/> [Accessed 29 Apr 2020].
- Lee, Robert M. and Rid, Thomas, 2014. OMG cyber! *The RUSI journal*, 159 (5), 4–12. doi:10.1080/03071847.2014.969932.
- Liebetau, Tobias and Christensen, Kristoffer Kjærgaard, 2021. The ontological politics of cyber security: emerging agencies, actors, sites, and spaces. *European journal of international security*, 6 (1), 25–43. doi:10.1017/eis.2020.10.
- Livingston, Steve, et al., 2019. Managing cyber risk in the electric power sector. Emerging threats to supply chain and industrial control systems. *Deloitte Insights*. Available from: <https://web.archive.org/save/https://www2.deloitte.com/us/en/insights/industry/power-and-utilities/cyber-risk-electric-power-sector.html.html> [Accessed 26 Aug 2019].
- Lukyanov, Fyodor, 2016. The west is overestimating Putin. Fyodor Lukyanov in conversation with Lukasz Pawlowski. In: Kacper Szulecki, ed. *Cracking borders, rising walls. The crisis of the European order*. Warsaw: Kultura Liberalna, 65–74.
- Madiaga, Tambiana, 2020. Digital sovereignty for Europe. *EPRS Ideas Paper*. Available from: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI\(2020\)651992_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf) [Accessed 18 May 2022].
- Maglaras, Leandros A., et al., 2018. Cyber security of critical infrastructures. *ICT express*, 4 (1), 42–45. doi:10.1016/j.icte.2018.02.001.
- Maurer, Tim, 2017. *Cyber mercenaries*. Cambridge: Cambridge University Press.
- McCarthy, Daniel R., 2018. Privatizing political authority: cybersecurity, public-private partnerships, and the reproduction of liberal political order. *Politics and governance*, 6 (2), 5. doi:10.17645/pag.v6i2.1335.
- Molyneux, Lynette, et al., 2016. Measuring resilience in energy systems. Insights from a range of disciplines. *Renewable and sustainable energy reviews*, 59, 1068–1079. doi:10.1016/j.rser.2016.01.063.
- Mrabet, Zakaria El, et al., 2018. Cyber-security in smart grid: survey and challenges. *Computers & electrical engineering*, 67, 469–482. DOI:10.1016/j.compeleceng.2018.01.015.
- Nakashima, Ellen, 2017. Russia has developed a cyberweapon that can disrupt power grids, according to new research. *Washington Post*. 6 Dec. Available from: <https://web.archive.org>.
- Powers, Shawn M. and Jablonski, Michael, 2015. *The real cyber war. The political economy of Internet freedom*. Urbana: University of Illinois Press (History of communication). Available from: <http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&AN=953632>.
- Qi, Junjian, et al., 2016. Cybersecurity for distributed energy resources and smart inverters. *IET cyber-physical systems: theory & applications*, 1 (1), 28–39. doi:10.1049/iet-cps.2016.0018.
- Rid, Thomas and Buchanan, Ben, 2015. Attributing cyber attacks. *Journal of strategic studies*, 38 (1–2), 4–37. doi:10.1080/01402390.2014.977382.
- Rychnovska, Dagmar, Pasgaard, Maya, and Berling, Trine, 2017. Science and security expertise: authority, knowledge, subjectivity. *Geoforum*. doi:10.1016/j.geoforum.2017.06.010.
- Sakwa, Richard, 2014. *Putin redux: power and contradiction in contemporary Russia*. London: Routledge.

- Salter, Mark B. and Mutlu, Can E., eds., 2013. *Research methods in critical security studies. An introduction*. London: Routledge.
- Sanger, David, 2018. Russian hackers appear to shift focus to U.S. power grid. *New York Times*, 27 Jul. Available from: <https://www.nytimes.com/2018/07/27/us/politics/russian-hackers-electric-grid-elections.html> [Accessed 26 Aug 2019].
- Sanger, David and Perloth, Nicole, 2019. U.S. escalates online attacks on Russia's power grid. *New York Times*. 15 Jun. Available from: <https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html> [Accessed 26 Aug 2019].
- Seabrooke, Leonard, Tsingou, Eleni, and Willers, Johann Ole, 2020. The political economy of policy vacuums: The European Commission on demographic change. *New political economy*, 25 (6), 1007–1021. doi:10.1080/13563467.2019.1669549.
- Sending, Ole Jacob, 2015. *The politics of expertise*. Ann Arbor: University of Michigan Press.
- Sending, Ole Jacob, 2017. Recognition and liquid authority. *International Theory*, 9 (2), 311–328. doi:10.1017/S1752971916000282.
- Sheridan, Kelly, 2018. Looking back and thinking ahead on cyberwar, nation-state attacks. *Dark Reading*. 23 Mar. Available from: <https://web.archive.org/save/https://www.darkreading.com/vulnerabilities---threats/looking-back-and-thinking-ahead-on-cyberwar-nation-state-attacks/d/d-id/1331355-attacks/d/d-id/1331355> [Accessed 26 Aug 2019].
- Shires, James, 2018. Enacting expertise: ritual and risk in cybersecurity. *Politics and governance*, 6 (2), 31. doi:10.17645/pag.v6i2.1329.
- Slayton, Rebecca and Clark-Ginsberg, Aaron, 2018. Beyond regulatory capture: coproducing expertise for critical infrastructure protection. *Regulation & governance*, 12 (1), 115–130. doi:10.1111/rego.12168.
- Slowik, Joseph, 2018. CRASHOVERRIDE: when “advanced” actors look like amateurs. Available from: <https://web.archive.org/save/https://pylos.co/2018/11/03/crashoverride-when-advanced-actors-look-like-amateurs/> [Accessed 26 Aug 2019].
- Stevens, Clare, 2020. Assembling cybersecurity: the politics and materiality of technical malware reports and the case of Stuxnet. *Contemporary security policy*, 41 (1), 129–152. doi:10.1080/13523260.2019.1675258.
- Stevens, Tim, 2015. *Cyber security and the politics of time*. Cambridge: Cambridge University Press. Available from: <https://dragos.com/wp-content/uploads/TRISIS-01.pdf>.
- Stevens, Tim, 2018. Global cybersecurity: new directions in theory and methods. *Politics and governance*, 6 (2), 1. doi:10.17645/pag.v6i2.1569.
- Sun, Chih-Che, Hahn, Adam, and Liu, Chen-Ching, 2018. Cyber security of a power grid: state-of-the-art. *International journal of electrical power & energy systems*, 99, 45–56. doi:10.1016/j.ijepes.2017.12.020.
- Szulecki, Kacper, ed., 2017. *Energy security in Europe: divergent perceptions and policy challenges*. London: Palgrave Macmillan.
- Szulecki, Kacper and Kuszniur, Julia, 2017. Energy security and energy transition: securitisation in the electricity sector. In: Kacper Szulecki, ed. *Energy security in Europe: divergent perceptions and policy challenges*. London: Palgrave Macmillan, 117–148.
- Tanczer, Leonie Maria, Brass, Irina, and Carr, Madeline, 2018. CSIRTs and global cybersecurity: how technical experts support science diplomacy. *Global policy*, 9, 60–66. doi:10.1111/1758-5899.12625.
- Tidwell, Jacqueline Hettel and Tidwell, Abraham S.D., 2018. Energy ideals, visions, narratives, and rhetoric: Examining sociotechnical imaginaries theory and methodology in energy research. *Energy research & social science*, 39, 103–107. doi:10.1016/j.erss.2017.11.005.
- U.S. CERT, 15703/2018. Alert (TA18-074A). Russian government cyber activity targeting energy and other critical infrastructure sectors. Available from: <https://web.archive.org/save/https://www.us-cert.gov/ncas/alerts/TA18-074A> [Accessed 26 Aug 2019].
- UK National Cyber Security Centre, 2017. Weekly threat report 16th June 2017. Available from: <https://web.archive.org/save/https://www.ncsc.gov.uk/report/weekly-threat-report-16th-june-2017> [Accessed 22 Aug 2019].

- Untersinger, Martin, 2019. Quelle est la bonne équation pour pacifier le cyberspace? *Le Monde*, 29 Jan.
- US CERT, 2017a. CRASHOVERRIDE Malware. 25 Jul. Available from: <https://web.archive.org/web/20190822142557/https://www.us-cert.gov/ics/alerts/ICS-ALERT-17-206-01> [Accessed 22 Aug 2019].
- US CERT, 2017b. ICS alert (ICS-ALERT-17-206-01). CRASHOVERRIDE malware. 25 Jul. Available from: <https://web.archive.org/web/20190826095000/https://www.us-cert.gov/ics/alerts/ICS-ALERT-17-206-01> [Accessed 26 Aug 2019].
- US CERT, 2017c. Alert (TA17-163A). CrashOverride malware. 12 Jun. Available from: <https://web.archive.org/web/20190826071252/https://www.us-cert.gov/ncas/alerts/TA17-163A> [Accessed 26 Aug 2019].
- Weaver, Nicholas, 2017. A cyber-weapon warhead test. *Lawfareblog*, 14 Jun. Available from: <https://web.archive.org/web/20190822140515/https://www.lawfareblog.com/cyber-weapon-warhead-test> [Accessed 22 Aug 2019].
- Weise, Elisabeth, 2017. Malware discovered that could threaten electrical grid. *USA Today*, 6 Dec. Available from: <https://web.archive.org/save/https://www.usatoday.com/story/tech/news/2017/06/12/malware-discovered-could-threaten-electrical-grid/102775998/>.
- Weldes, Jutta, 1999. *Constructing national interests. The United States and the Cuban missile crisis*. Minneapolis: University of Minnesota Press (Borderlines, v. 12). Available from: <http://www.jstor.org/stable/10.5749/j.cttttd99>.
- Willers, Johann Ole, 2021a. *Experts and markets in cybersecurity. On definitional power and the organization of cyber risks*. 1st ed. PhD School of Economics and Management (Ph.D.-serie / Copenhagen Business School, 35.2021).
- Willers, Johann Ole, 2021. *Seeding the cloud: consultancy services in the nascent field of cyber capacity building*. In Public Admin. doi:10.1111/padm.12773.
- Yergin, Daniel, 2006. Ensuring energy security. *Foreign Affairs*.