

Cyber security meets security politics: Complex technology, fragmented politics, and networked science

Myriam Dunn Cavelty & Andreas Wenger

To cite this article: Myriam Dunn Cavelty & Andreas Wenger (2019): Cyber security meets security politics: Complex technology, fragmented politics, and networked science, Contemporary Security Policy, DOI: [10.1080/13523260.2019.1678855](https://doi.org/10.1080/13523260.2019.1678855)

To link to this article: <https://doi.org/10.1080/13523260.2019.1678855>



© 2019 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group



Published online: 14 Oct 2019.



Submit your article to this journal [↗](#)



Article views: 634



View related articles [↗](#)



View Crossmark data [↗](#)

Cyber security meets security politics: Complex technology, fragmented politics, and networked science

Myriam Dunn Cavelty  and Andreas Wenger



Center for Security Studies, ETH Zürich, Zürich, Switzerland

ABSTRACT

In the last decade, cyber incidents have become more expensive, more disruptive, and in many cases more political, with a new body of theoretically informed research emerging in parallel. This article provides the intellectual history to situate this literature in its broader evolutionary context. After identifying and discussing six drivers from the fields of technology, politics, and science that have been influential in the evolution of cyber security politics and how it is studied, we describe three historically contingent clusters of research. Using the same driving factors to look into the future of research on cyber security politics, we conclude that it is a vibrant and diverse biotope that is benefitting from its interdisciplinarity, its relevance for policy, and its cognizance of the interplay between technological possibilities and political choices of state actors.

KEYWORDS Cyber security; cyber conflict; international security; sociology of knowledge; security studies

Societies in many parts of the world rely on the uninterrupted operation of digital technologies for the delivery of essential services. This dependency has brought forth new security concerns. In the past decade, cyber incidents such as Stuxnet (Baezner & Robin, 2017a), WannaCry, and NotPetya (Baezner, 2018a), or the interference in the American elections (Baezner & Robin, 2017b) have given the impression that cyber attacks are becoming more targeted, more expensive, more disruptive, and in many cases more political and strategic. As a result, cyber incidents, understood as disruptions of the routine operations of digital technologies, have come to hold a prominent position in national and international security policy, with state actors trying to find adequate answers to counter the new threat.

CONTACT Myriam Dunn Cavelty  dunn@sipo.gess.ethz.ch  Center for Security Studies (CSS), ETH Zurich, Haldeneggsteig 4, IFW, 8092 Zurich, Switzerland

© 2019 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.

In 2006, Eriksson and Giacomello stated that the discipline of international relations (IR) was struggling to apply its varied theoretical toolbox to the topic of cyber security, therein detecting “great difficulties for theoretical adaptation and application in analyses of the complexities of the emerging new digital world” (p. 236). This observation no longer holds true. Due to interlinked changes occurring in the fields of technology, politics, and science, research that applies international relations or security studies theory to different facets of the phenomenon is no longer as rare, inviting us to look at this emergent body of research in depth at this point in time (for a similar undertaking see Deibert, 2017a, 2017b).

This special issue displays the latest wave of cyber security politics research. The articles position themselves mostly in a post-positivist research tradition and use a set of different theories and conceptual frameworks to analyze the current state of cyber security in politics. Some articles examine the contested nature of public attributions of cyber incidents, the norm-setting day-to-day behavior of intelligence agencies, and discuss the consequences for governments and governance. Another group of articles explores the knowledge-shaping practices of IT-security companies, the co-production of risks and vulnerabilities by technology and experts, and aim at better understanding the role of firms and experts in strategic state interactions.

In this introductory article, we provide the intellectual history to situate the literature in its broader evolutionary context. In a first part, inspired by Buzan and Hansen’s framework from their “The Evolution of International Security Studies” (2009), we discuss six drivers that have been influential in the evolution of (Western) cyber security politics and how it is studied. In a second part, we identify three clusters of research. In each of them, we highlight the interplay between technological possibilities and political choices of state actors in combination with scientific factors. The focus on “the state” is appropriate and necessary, because security politics is inevitably tied to questions of authority and power. That said, the state is not the only important actor in this space—rather, it is at the intersection between state and non-state actors, nationally and internationally, that the specificities of cyber security politics emerge.

In the conclusion, we use these same drivers to look into the possible future of cyber security politics research. We claim that it should not be conceptualized as a sub-field of anything, so that inquiry is not overly restricted by the disciplining power of disciplines. Cyber security transcends levels of analysis, necessitates considerable interdisciplinary knowledge, and will be shaped by the availability of new data and methods. Its relevance for society is likely to become even bigger in the future, with new digital technologies expanding the spatial boundaries of cyberspace and with new complex issues emerging. Scientific knowledge of both the problem-solving and the reflexive kind is crucial to understand what politics these technologies will

have and how they will be linked to broader socio-economic changes affecting the society, the economy, and the state in the future.

Factors driving the evolution of cyber security politics research

Mapping a body of research is no trivial and certainly no purely objective undertaking. In order to simplify and abstract, a series of choices have to be made about what to include and what to exclude. As critical cartographers know, “[m]apping is epistemological but also deeply ontological – it is both a way of thinking about the world, offering a framework for knowledge, and a set of assertions about the world itself” (Kitchin, Perkins, & Dodge, 2009, p. 1). First, we hone in on “cyber security politics,” highlighting two areas that help to structure the debate. What we aim for in these pages is an understanding of cyber security politics that is flexible enough to deal with the dynamics of the phenomenon, yet precise enough to demarcate the research focus sufficiently to be of use. Second, and loosely following Buzan and Hansen (2009), we identify six driving forces that explain the dynamic co-evolution of cyber security politics and the academic engagement with it. These factors help us to understand what researchers choose to write about, what subjects and issues they define as the main cyber security problem(s) and which ontologies, epistemologies, and methods carry legitimacy (Buzan & Hansen, 2009, pp. 39–40).

Staking out cyber security politics

What is “cyber security” and how is it related to security politics? Far from allowing a straightforward answer, this question lies at the heart of the political and academic debates about the issue. First, cyber security is a relatively new term for a set of older practices around the security of computer networks (Von Solms & Van Niekerk, 2013). Second, definitions for the term are contested, exemplified by the refusal of some state actors to agree on a common vocabulary (Giles & Hagestad, 2013). Third, the meaning of the term is changing across time. Not so long ago, a limited circle of experts discussed cyber security primarily as a technical risk management issue in critical information infrastructure protection. Now the highest government circles deal with cyber security as a key challenge of national security (Dewar, 2018). Fourth, parallel to the advancing digitalization of ever more aspects of the economy, society, and politics, cyber security concerns are expanding to additional policy domains (Dunn Cavelty & Egloff, 2019). In sum, cyber security is at the same time moving upwards in the political agenda and expanding sideways as a problem area to a multitude of additional policy domains.

Simple and static definitions are not well suited to deal with constantly changing contexts. However, if we look down on the conceptual space from

a sufficient height, we notice that cyber security politics' common ground is characterized by two main factors: First, by *digital technologies*, specifically their use and misuse by human actors in economic, social, and political contexts; and second, by enduring and often highly conflictual *negotiation processes* in formal and informal settings between the state and its bureaucracies, society, and the private sector, geared towards defining roles, responsibilities, legal boundaries and acceptable rules of behavior.¹

The first dimension is tied to the use of a set of distinct digital technologies and how these technologies are linked to broader conceptions of socio-economic changes (Papp, Alberts, & Tuyahov, 1997). The marriage of computers and telecommunications, the integration of these technologies into a global multimedia system, and their worldwide inexpensive availability is the bedrock for heralding multiple, rapid and consequential transformations in production, management, societal interaction, and governance (Schwab, 2018) though it remains to be seen just how revolutionary these changes will really be. The most pertinent questions in cyber security politics with regard to digital technologies are what their characteristics are, what actions they make possible and which ones they restrain, but also who develops them in what ways and why and who has the power to shape their use and misuse.

The second dimension is tied to the role of states and their engagement with other actors nationally and internationally. "Security" in cyber security politics can be read in two ways: As *cyber security politics* (the security political aspects of the issue) or as *cyber security politics* (the politics engaging with questions of cyber security more broadly). This ambiguity is deliberate because we consider the question of what type of politics emerges under what kind of rules and with what kind of boundaries to be crucial. From a theoretical point of view, the question of how much politics there is or should be in security—and how much security in politics—allows us to link research in cyber security to debates in security studies (Hagmann, Hege-mann, & Neal, 2019). Importantly, the state has different roles in cyber security, ranging from security guarantor, legislator and regulator, to threat actor and danger to society and other states (Dunn Cavelti & Egloff, 2019). Hence, cyber security politics are defined by national and international negotiation processes about the boundaries of the responsibilities of state, economic, and societal actors and the agreement or disagreement over the means these actors use. This second dimension includes the projection of power by certain actors, like the control over populations and information flows, and the push-back against it as well.

Six driving factors

In their intellectual history of international security studies, Buzan and Hansen develop a framework of five interrelated factors (2009, pp. 39–

100)–great power politics, technology, key events, academic debates, and institutionalization—that drove the evolution of the field. For cyber security politics, we propose a slightly different framework, purporting that changes in research are linked to changes in the empirical phenomenon, whereby these changes can go both ways: A research phenomenon often influences directions of research, but research also illuminates aspects of the phenomenon that have gone unnoticed before.

We focus on the interrelationship between technology and the world of policy and state practice—on what political actors *say* they are doing and on what they *are* doing in the field of cyber security as a political issue, both nationally and internationally, often in relation to other actors—and on the different ways to observe this interrelationship (Figure 1). The intellectual history of cyber security politics is thus shaped by the interplay of three broad spheres: Technology, Politics, and Science.² Technological dynamics interact with social and political dynamics. Technological possibilities and constraints influence socio-economic processes. In turn, political preferences and contexts shape the evolution of digital technologies. This also applies fundamentally to the actors developing these technologies and to the dynamic interplay of cyber security markets and cyber security politics.

Within each of the three spheres, we identify two main drivers. In different combinations during different times, these six factors stimulate or dissuade scholars from picking up specific research questions. A summary can be seen in Table 1, with a more detailed description in what follows.

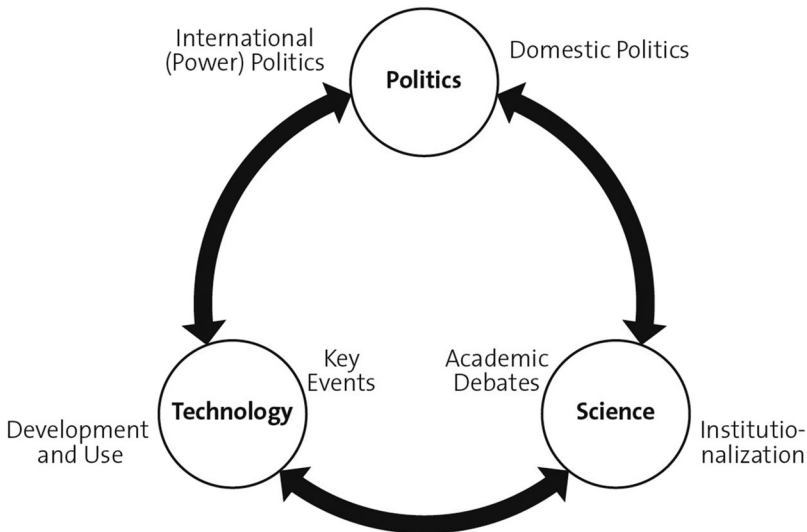


Figure 1. Six factors driving cyber security politics.

Table 1. Summary of driving factors.

Spheres	Driving Factors	Description
Technology	Development and Use of Digital Technologies	Technologies are shaped by political ideas and power structures and shape the possibilities of political action in turn
	Key Events (cyber-related)	Events outside the cyber realm with influence on cyber security politics and events from the cyber realm in the form of cyber incidents
Politics	International (Power) Politics	Belief in new sources of power (“cyber power”) and patterns of cooperation and conflict between great powers
	Domestic Politics	Potentially conflictual negotiation processes about roles and responsibilities for state institutions, economy, and society (nationally and internationally)
Science	Academic Debates	Broader ontological and epistemological trends that shape the discipline of International Relations and Security Studies
	Institutionalization	Opportunities and constraints for researchers in the form of positions, funding, publication outlets, and research networks

Technology as a driver

It seems like an obvious choice to include “technology” as a category, since the issue of cyber security is linked to the development and use of cyberspace, a technological environment entirely built by humans. Yet scholars have rightly pointed out that the vision of one unique cyberspace is itself based on a social construction (Bingham, 1996; Graham, 1998). Indeed, the conception of what cyberspace is and what can be done with it has changed considerably throughout its history, highlighting the need for historically contingent understandings of the development and use of technologies. However, a core characteristic of IR scholarship’s dealing with digital technology is “technological determinism” (Herrera, 2003). The majority of IR approaches chooses to deal with technology as an exogenous variable (McCarthy, 2018, p. 4), seeing technologies as a material objects or power resources that drive social change or as neutral tools that acquire meaning only through their use (Leese & Hoijsink, 2019).

In contrast, we understand technologies as embodiments of societal knowledge in the tradition of science and technology studies (STS), as sites where power relations can be seen in operation and where the shaping and coordination of the behavior of social and political actors happens (Behrent, 2013, p. 57). During the design stage of technologies, the intentions, norms, and values of their developers find their way into the artefacts, while existing power structures influence the desirability of specific aspects or forms of technology. Once technologies diffuse, they are often given particular meanings and acquire purposes other than the one initially intended by their developers (Matthewman, 2011), but always within certain inescapable material bounds (see also Fischerkeller & Harknett, 2018). For example: A pen can be used for writing, but it can also be used to stab someone. It can, however, not be used to make phone calls.

That digital technologies “have politics” is hardly a contested statement (Deibert, 2003, 2013; DeNardis, 2014; Mueller, 2010; Price, 2018). Design decisions made by engineers in the late 1960s have implications until today, especially for security. From the early prototype phase as ARPANET (1967-1972) to the gradual development into “the Internet” (1973-1983), technological protocols that define how data is exchanged were written in an egalitarian spirit (Naughton, 2016). The decision to have a system with minimal rules that had no central power and no censor was deliberate and based on philosophical and political beliefs of the technical community (Berners-Lee, 1999). Cyber security as we understand it today became an issue only gradually, when the system architecture changed from large proprietary machines with little connection to “smaller and far more open systems (not built with security in mind) coupled with the rise of networking” (Libicki, 2000), yet still ran on the same basic protocols.

The perception that cyberspace is creating and perpetuating insecurity with potentially catastrophic consequences is shaped by different key events linked to the technological sphere as a second important driving factor. In line with what we noted above, these events are not understood as causal forces that unidirectionally influence politics or science (cf. Buzan & Hansen, 2009, p. 54ff.) but rather as interrelated catalyzers. The category consists of events outside the cyber realm with influence on cyber security politics (examples include 9/11, the Snowden revelations, or the Arab Spring), and cyber incidents themselves. In its most basic form, a cyber incident is a disruption that challenges the normal operation of digital technologies. Undesired change inside machines create technical effects. Yet these technical effects alone are not sufficient to explain the salience of cyber security in politics. Between the initial effect in the machine and the political effect lies a knowledge production process that creates an incident embedded in a specific social context. A technical effect needs to be discursively linked to something with sufficient social or political value to become security politically relevant—which also explains why only some cyber incidents reach that stage while others do not (Balzacq & Dunn Cavelty, 2016).

Such moments of disruption highlight previously hidden characteristics of socio-technical artifacts, opening up opportunities for the study of new aspects of the phenomena that were not easily observable before or did not seem important (Best & Walters, 2013, p. 346; Latour, 1999). Incidents are also linked to another fundamental issue in the study of cyber security: the availability of data. Our current knowledge about cyber security relies heavily on data from commercial threat reporting and news reports. Yet this data provides a partial and biased view of cyber threat activity, because it is often politicized and influenced by the demands of powerful buyers and the interests of capable providers (Lindsay, 2017).

Politics as a driver

The discipline of IR is mainly interested in patterns of cooperation and conflict among states and how these patterns relate to shifts in the distribution and character of power in the international system: international power politics. As the issue of cyber security gained in importance in state interactions, experts and policy makers pondered whether digital technologies gave rise to a “new” type of power and how this power source would influence the existing power distribution in the system (Nye, 2011). Given that IR began as an “American discipline, was focused on American security and written by Americans” (Buzan & Hansen, 2009, p. 51), the debate about the security implications arising from the spread of information technologies also originated in America, with a series of implications for how the subject was studied. Though definitions vary, cyber power is understood as the use of resources related to cyberspace to achieve specific (political) ends inside and outside of cyberspace (cf. Nye, 2010, p. 3). In the contemporary U.S. setting, a discourse of simultaneous empowerment and disempowerment characterized the conceptual debate from the beginning. While the technological realm carried the promise of wielding a new sort of power, it highlighted new dependencies and vulnerabilities at the same time (Rattray, 2001).

Apart from giving the digital domain a particular weight in the broader questions that IR scholars are interested in, we also need to consider how international politics influence the use of these technologies. Given the interconnection between technology and politics, we can expect the overall state of world politics to have a noticeable influence on the forms of use/misuse of these technologies. Buzan and Hansen call this larger context “patterns of enmity and amity between great powers” (2009, p. 52). This highlights questions of cooperation and conflict, about the formation of alliances and the maintenance of strategic stability, about the proliferation and control of dual-use technologies, but also about the efforts of states to come to international agreements in the form of norms and institutions.

In our conception of politics, the international dimension is just one aspect of a broader set of political interactions. Cyber security is not only about enmity and amity and the potential for war and peace. In fact, it is not very often about situations of great urgency, but more often about “normal” domestic politics. Like many other complex policy issues, cyber security is cutting across different areas of responsibility, requiring coordination and cooperation between a wide variety of public actors at different levels of government, but also actors from business and society. When government tasks and authority are delegated downwards (localization), upwards (supranationalization), or sideways (privatization) (Krahmann, 2003), governance in networks becomes important. Under such conditions, governments no longer simply issue instructions and monitor their implementation, but seek to shape the framework conditions so that cooperation operates as smoothly

as possible even without constant oversight (Peters & Pierre, 1998; Salamon, 2002), coming with a set of challenges for state-society relationships.

Science as a driver

The last two factors are situated in the realm of science that is understood here as a collective term for “academic work,” “intellectual labor,” or “knowledge production.” Like Buzan and Hansen (2009, pp. 57-65), we focus on academic debates and on institutionalization. This introduces an element of internal conflict into our intellectual history, because even if academics would agree on the key events or issues that need to be studied, *how* they would study it would still differ widely. As a case in point, cyber security politics research is no subfield of anything—it is characterized and united by the engagement with a multifaceted and dynamic phenomena, but the disciplinary approaches used, the ontological and epistemological choices, vary greatly.

Debates about ontology, epistemology, and methodology are at the heart of some of the most fruitful key debates in security studies, but at the same time they divide the discipline. The biggest cleft exists between problem-solving theories and critical theories: the former do not explicitly question the prevailing social and power relationships, while the latter problematize these very relationships by analyzing their origins and their evolution (Cox, 1986). Which of these two approaches is favored in certain research settings however depends on many different factors (Bourbeau, Balzacq, & Dunn Caveltty, 2015). Building on decades of IR scholarship, traditional approaches have seen incremental theoretical innovation since the end of the Cold War. By contrast, critical approaches have gone through a phase of rich theory development and are only slowly becoming ripe for empirical work based on critical methods (Aradau, Huysmans, Neal, & Voelkner, 2014). The key focus of interest has been the analysis of the (social) power relations that underpin security policies in liberal states, highlighting security as a powerful political technology for social (and political) control (Dillon & Reid, 2009); as a collection of discourses that serve to empower and reproduce hierarchies (Shepherd, 2008); or as routinized and patterned practices carried out by bureaucrats and security professionals (Bigo, 2002). These overall research trends have an important impact on cyber security politics research, since the topic has been picked up by all approaches, leading to distinct takes on what cyber security politics is and how it should be studied.

The second important driver is related, but different. Academic debates do not unfold in a vacuum—there are economic and structural factors that shape research in all fields of science. Of importance are organizational structures, academic positions, Ph.D. programs, funding possibilities, and the ability to disseminate knowledge, for example through specialized journals (Buzan & Hansen, 2009, pp. 60–61). The status and availability of security scholars to comment on particular issues and the demand for certain types of knowledge

also need to be considered. When “new issues” arise, there usually is a high demand for problem-solving, actionable knowledge. Consequently, we often see that policy-relevant knowledge, produced in think tanks, comes first and only then turns into an “academic specialty” (Waever, 2010, p. 652). As an indicator for how “new” the focus on cyber security politics still is, we have only very recently seen the establishment of specialized journals such as the *Journal of Cybersecurity* (Oxford University Press, established in 2015) or the *Journal of Cyber Policy* (Taylor & Francis, established 2016). Dedicated places for doctoral trainings such as the Centre for Doctoral Training in Cyber Security at the University of Oxford, the Centre for Doctoral Training in Cyber Security at the University College London, or the CISPA-Stanford Center for Cybersecurity are still few in number.

Cyber security politics research: Empirical trends and topical clusters

In the second part of the article, we outline the evolution of cyber security as a security political issue and its dominant reflections in science. First, there are trends discernible in the spheres of technology, politics, and science that shaped the emergence of today’s state of the art in cyber security politics research. These processes unfold over time and “change the knowledge, understanding and consciousness that support existing practices” (Buzan & Hansen, 2009, p. 55), getting us to the current point in the history of cyber security politics. Second, we move on to identify three current research clusters that emerged next to each other as distinct ways of looking at the subject area.

Trends in cyber security politics

Today, cyber security is increasingly discussed at the level of international politics and, both as a stimulus and a consequence, integrated into the dynamics of (great) power competition and cooperation. Three developments in cyber conflict stand out, signifying how digital technologies are used in political contexts and how the link to state actors is made: First, attention is shifting from theoretical “doomsday” cyber attack scenarios towards the reality of persistent (low-level) cyber operations in different types of conflict settings. Second, attention has partially shifted to targeted cyber attacks. Third, and as a corollary of growing unease about the destabilizing role of cyber operations, state and non-state actors are more actively searching for ways to control the risk of escalation and conflict through different means. At the same time, they are redoubling their efforts to ascertain their respective roles and responsibilities at the domestic and bureaucratic level.

From critical infrastructures and theoretical doomsday ...

From the very beginning the two strategic key concerns in thinking about cyberspace and conflict were the low entry costs for disruptive cyber “weapons” and the high vulnerability of critical infrastructures, which are dependent on digital technologies for a variety of functions. This dependency (and inter-dependency) elevated cyber security from low politics to high politics and turned a primarily technical issue into an issue of national and international security politics (Dunn Cavelty, 2008).

These early conceptions of cyber doom were linked to two ways of discussing cyberspace’s effect on power. The first was driven by utopian visions of a cosmopolitan society, which was emancipated thanks to the democratizing effects of the new technologies (Barlow, 1996). The (technologically deterministic) belief was that control over knowledge, beliefs, and ideas would complement the control over more tangible resources such as military forces, raw materials, and productive capacities (Rothkopf, 1998), for some even topping them in importance (Rosecrance, 1999). As a consequence, many observers anticipated not only a redistribution of power relationships at the expense of the traditional state actors, but also fundamental changes in the nature of power (cf. Alberts & Papp, 1997; Keohane & Nye, 1998; Rosenau, 1998).

In second debate, military strategists in the United States (but also in Russia and in China) started to think about the importance of networked computers for war fighting (Berkowitz, 2003). During the 1990s, militaries began to treat cyberspace as “domain of warfare” in theory and practice (Arquilla & Ronfeldt, 1997). By 2011, the Pentagon had officially added cyberspace as the so-called “fifth” domain of warfare, next to land, sea, air, and space. From early on, this particular debate was characterized by the double-edged sword perspective mentioned already: strategists saw great opportunities for winning wars through technology-aided “information dominance,” but at the same time they anticipated growing security-relevant vulnerabilities due to increasing dependencies on computers (Ratray, 2001).

This notion of growing vulnerabilities as a consequence of ever tighter interconnectedness was expanded from military networks to the whole society in the second half of the 1990s through a link to “critical infrastructures” as the backbone of modern societies (Dunn Cavelty & Kristensen, 2008). The political importance of digital technologies reflected a growing awareness that information infrastructures support and enable crucial services for the functioning of the economy, the government, the military, and society overall. As a result, the biggest threat discussed in strategic circles for years, sometimes under the buzzword “Electronic Pearl Harbor” (Schwartau, 1994), was a destructive cyber attack out of the blue that would bring the United States to its knees within seconds.

... To the empirical reality of persistent cyber operations across the conflict spectrum

Over time, experts began to shift their attention to the reality of persistent cyber operations across the conflict spectrum. On the one hand, strategic cyber war or cyber terrorism—understood as stand-alone, out-of-the-blue cyber-attacks against critical infrastructures—failed to make the expected appearance while on the other hand, political and strategic implications of low-level cyber conflict became more relevant to international affairs. Mounting evidence suggested that it was becoming routine for state and non-state actors to try and influence the larger information sphere before and during political disputes or conflicts, sometimes coupled with mildly disruptive attacks (Baezner, 2018b).

At the same time, and on the opposite end of the capabilities' spectrum, the phenomenon of computer network attack campaigns gained more widespread attention, starting with GhostNet in 2009 and later, the discovery of Stuxnet in 2010 (Deibert & Rohozinski, 2009; Farwell & Rohozinski, 2011). These campaigns are stealthy and continuous cyber operations targeting a specific entity's information or functionality. The growing empirical relevance of such attacks reflects two interconnected trends: on the one hand, cyber crime markets were increasingly professionalized; on the other hand, covert state involvement seemed to become the new normal in the context of such attacks—an empirical reality that abruptly gained international visibility in the context of the Snowden leaks (see Georgieva, 2019; also Maurer, 2017).

These two trends—the normalization of low-level cyber conflict and the increase of cyber campaigns linked to covert state involvement—demonstrate that the tools for and use of cyber operations for political purposes have matured considerably (Dunn Cavelty, 2015). The overall perception in many strategic circles is that the problem has gotten worse both in quantity as well as quality—an insight that is supported by threat intelligence reports from private companies. Some experts regard the build-up of cyber capabilities by state actors as part of a cyber arms race—although it may as well be conceptualized as a competition that plays out primarily in the field of espionage and intelligence (see Georgieva, 2019). The uncertainty about the intentions of other states and the practical inability to know whether such capabilities are used for offense or defense drive a classical security-dilemma, increasing the incentives of intelligence agencies and military cyber commands to build up (offensive) capabilities (Buchanan, 2016).

Reactions: Cyber grand strategy, cyber norms, and an increase in repression

In the context of an increasing sense of insecurity, political actors have re-doubled their efforts to control the risk of escalation and conflict. Two types of mechanisms aimed at upholding strategic stability have become visible over the past years: The first concerns the establishment of norms for good behavior in

cyberspace, including transparency and confidence building measures and discussions about how the international rules of war apply to cyber conflict (Hitchens & Gallagher, 2019; Sabbah, 2018). Since state-led endeavors have been crippled by opposing ideological standpoints, mutual distrust and diverging interests, a fair number of corporate as well as non-governmental entities have started to get involved. The second is an attempt to adapt the concept of deterrence to cyberspace, integrating insight from criminological conceptions of deterrence and shifting emphasis from deterrence by punishment to deterrence by denial (Libicki, 2009). An important precondition for upholding the credibility of both cyber norms and cyber deterrence is the (sometimes public) attribution of cyber incidents to a politically responsible actor (Egloff & Wenger, 2019).

Such political action is only possible if states begin to understand cyber security politics as part of their “grand strategy,” meaning if they deploy all the resources of a nation state—economic, military, diplomatic, social, and informational—in both peacetime and wartime to ensure that state, society and economy remain secure. Most states still struggle to integrate national and international cyber security policy and practice into their broader national and international security political frameworks (Weber, 2018). This includes the transition from viewing cyber security as a technical issue to tackling it as a (security) political task. The coordination and integration of all existing sectoral policies—which often operate in silos—into one coherent, interconnected and streamlined framework or grand strategy remains a challenge for all types of political institutions. The heterogeneity of actors that need to cooperate—at the vertical level (national, regional, local) and the horizontal level (civilian and military; public and private)—to uphold cyber security creates additional coordination and cooperation problems. On the downside, the easy availability of offensive cyber capabilities provide states with additional means for controlling citizens, both domestically and abroad, as demonstrated by the rise of offensive mandates and the growth of the market for surveillance and spyware tools as services (Deibert, 2013).

Clusters of research on cyber security politics

We did not choose how the authors in this special issue conceptualize technology in relation to politics. However, the influence of different research traditions is discernible in how cyber security is approached. Following the division between problem solving theories and reflective theories, cyber security is either viewed as something that is objectively measurable and that can therefore be isolated as an independent or dependent variable, or alternatively as a discourse or practice, something whose political *Gestalt* is not objectively given, but is socially constructed. Based on the account of trends in cyber security politics above, we suggest three current research clusters. They do not happen consecutively, but have temporal overlaps and other interconnections.

Cluster 1: The reality of cyber conflict: Explaining state restraint and practices

In the beginning of this intellectual history, political aspects of cyber security were discussed almost exclusively in publications originating in U.S. think tanks and war colleges (for example: Arquilla & Ronfeldt, 1992). This literature had little ambition to contribute to an academic debate. The two main questions it tackled were “who (or what) is the biggest danger for an increasingly networked nation/society/military/business environment” and “how to best counter the new and evolving threat.”

The first cluster is characterized by a reevaluation of the threat based on empirical evidence and a gradual application and adaption of “old” IR and strategic studies concepts to cyber security (Kello, 2013). Two cyber incidents—the discovery of Stuxnet in 2010 and later the Snowden disclosures in 2013—were instrumental in shifting the focus of both policymakers and researchers from the threat politics of “what if”-scenarios that had dominated the 1990s and early 2000s to the reality of the strategic use of cyberspace by state actors. In this new context, literature in IR and strategic studies could be used to examine how state actors use cyber instruments for their political or military advantage and analyze their impact on national and international security (Borghard & Lonergan, 2017; Kello, 2017; Maness & Valeriano, 2016). A strong disciplinary “pull” is visible in how early works zoomed in on an alleged offensive advantage in cyberspace due to the ubiquity of technical vulnerabilities (Peterson, 2013), grappled with the problem of escalation dynamics in cyberspace (Liff, 2012), and asked how deterrence might be adapted in order to uphold stability in cyberspace (Wilner, 2019).

As researchers began to build data sets of cyber operations (Kostyuk & Zhukov, 2019; Valeriano & Maness, 2014) to link cyber issues to the larger agenda of conflict studies, an empirical puzzle emerged that challenged many of the theoretical tenets and standards assumptions of the older literature. Most cyber operations did not seem escalatory, nor were they determined by power asymmetries or changed the existing strategic balance. Overall, states seemed to exercise a fair amount of restraint in cyberspace (Gartzke, 2013; Gartzke & Lindsay, 2015; Valeriano & Maness, 2015). At the same time, however, a lot of cyber operations linked to state rivalries occurred, though as mere add-ons to existing conflict dynamics and not independent of a broad range of other foreign policy instruments (Betz & Stevens, 2011).

Reacting to this puzzle, the literature in this cluster has begun to move in two directions: First, and comparable to the evolution of the strategic studies literature during the nuclear age, some authors have started to integrate additional non-systemic explanatory factors into their analyses of cyber conflict. While some explore the role of beliefs and cognitive biases in cyber policy decision making (Gomez, 2019), others zoom in on the destabilizing

role of bureaucratic politics and other deficiency of the policy process especially in crisis decision making. Second, and more consequentially, many authors acknowledge that the emerging empirical picture reflects the structural feature of cyberspace as an operating environment, which is marked by a high degree of technical interconnectedness and constant political contestation (Fischerkeller & Harknett, 2018; Smeets, 2018). Taking this into account, operating strategically in cyberspace seems to be more technically and organizationally demanding than the “cheap and easy”-metaphor suggests, while at the same time offering little enduring strategic gains in the sense of changing a rival’s political goals (Lewis, 2018; Slayton, 2017).

From a theoretical point of view, the literature is trying to make sense of the puzzling co-existence of strategic restraint of states in cyber conflict and constant low-level cyber operations (Gartzke & Lindsay, 2016). First, some authors acknowledge that the technical and structural characteristics of cyberspace fundamentally challenge some of IR’s core concepts—power, sovereignty, territoriality—so that they lose traction for explaining state behavior (Fischerkeller, 2018). Yet the literature offers little theoretical innovation so far to understand and explain why in cyberspace, the power to subvert seems to trumpet both the power to coerce and the power to attract. Second, in order to analytically sort out the difference between mutually acceptable espionage in support of strategic stability and unacceptable political meddling in the internal affairs of another state, researcher need to move more thoroughly inside and beyond the state.

Cluster 2: Moving inside and beyond the state

The coming together of strategic restraint and stability at the high end of conflict and permanent subversion and instability at the low end of conflict has more recently been addressed by a second cluster of research that focuses on the role of actors inside the state—like intelligence agencies—and beyond the state—like cybersecurity firms. Part of the problem in understanding state behavior in cyberspace is due to the opaqueness of cyber operations and the limited visibility and ambiguity of many of the involved actors. Little is known about the mechanisms that link the socio-technical aspects of cybersecurity to the socio-political dynamics of cyber security politics. Three partially overlapping approaches—linked to markets, norms, and governance—have emerged that all reflect a realization that the development of digital technologies is only partially influenced by states and political considerations.

The first approach attempts to understand the political dynamics of cyber conflict by linking them to cyber market dynamics, applying insights from economic and organizational studies as well as from international political economy. There is a growing interest in cyber security companies, particularly in understanding how they influence state policy and practice at the national and international level. The companies have become important actors in

publicly attributing cyber operations to specific perpetrators, sometimes even to states (Rid & Buchanan, 2015). While they have a financial interest in demonstrating their analytical capabilities, they also have sound motives—linked to trade secrets and confidentiality agreements—not to provide insight in all their data and tools (Egloff, 2019; Egloff & Wenger, 2019). Moreover, they sell their services to governments, organizations, and individuals, regardless of the fact that protecting one customer might weaken another, in effect primarily shedding light on those cyber incidents that affect the wealthy and the powerful.

A second approach focuses on why cyber norms emerge only slowly, building on the existing IR norms literature (Finnemore & Hollis, 2016). Early works in this area focused on the debate among states, especially at the United Nations, followed by a growing number of proposal from the private and the civil sector (Hurwitz, 2014). However, cyber norms remain contested at the international level (Grisby, 2017). More recently, the interest of researchers shifted to the role of the creators (mostly private entities) and exploiters (sub-, semi-, and non-state actors) of digital technologies in shaping the behavioral standards that new regulation needs to take into account (Hurel & Lobato, 2018). States need to know how their intelligence services work in cyberspace, because through their tools and practices they set practical norms of acceptable (cyber) espionage with far-reaching effects on state behavior in cyberspace (Georgieva, 2019). The focus on the role of intelligence agencies in cyber conflict—as both the biggest threat and the most capable provider of safety—opens up interesting questions linked to the larger transformation of these agencies in the context of the digitization of society. Some authors argue that cyber conflict is primarily an intelligence game, because setting up cyber exploitation is much more expensive than countering released exploitation, which increases the incentive to keep the target at risk (Lindsay, 2017).

A third approach explores the broader repercussion of cyber conflict dynamics for government and governance. The concept of networked governance seems especially apt at capturing the essence of cyberspace as co-constituted by technical devices and networks and socio-political institutions (Hofmann, 2016). The key governance challenge in cyberspace is fragmentation of authority and accountability. A case in point is the lack in public transparency and trusted knowledge about the perpetrators behind most cyber incidents. Although the number of public attributions of cyber incidents by states and threat intelligence firms has been on the rise, both types of actors have political and economic reasons not to fully disclose their evidence (Egloff, 2019). As a consequence, attribution claims remain contested in the public domain, undermining the legitimacy of state action—from insurance matters and criminal proceedings to mechanism of international cooperation and potentially escalation control.

Cluster 3: Securitization, practice, and assemblages

Looking back at the beginnings of the cyber threat story, the policy debate was riddled with cyber-doom scenarios and constant attempts to mobilize in the political process. As a reaction to what was considered a “hype,” some scholars started to get interested in why and how this issue was presented the way it was and with what consequences. Early work to analyze the issues surrounding the politics of Internet from IR and critical security studies perspectives emerged at the end of the 1990s (Deibert, 2002; Eriksson, 2001; Saco, 1999). A bit later, there was a concentrated effort to apply variations of securitization theory to the issue of cyber security politics (cf. Dunn Cavelty, 2008; Hansen & Nissenbaum, 2009; Lawson, 2013). Securitization signifies the representation of a fact, a person, or a development as a danger for the military, political, economic, ecological, and/or social security of a political collective and the acceptance of this representation by the respective political addressee (Buzan, Waever, & De Wilde, 1998). The successful securitization of a topic justifies the use of all available means to counter it—including those outside the normal political rules of the game.

Following the theory, the prime questions this literature engaged with were related to the object of security, to what or whom was considered the main threat, and to what policy responses flowed from these threat constructions (Deibert & Rohozinski, 2010). Given its theoretical underpinnings, the Copenhagen School focuses mainly on official statements by heads of state, high-ranking officials or heads of international institutions (Hansen, 2006, p. 64). What a focus on elite speech acts ignores, however, is how these discursive practices are facilitated or prepared by practices of actors that are not so easily visible. The social competition for the definition of reality is not only held in the open political arena. There are always state and non-state actors “under the radar”—that is, specialized bureaucratic units, consultants or other experts—which have the capacity to establish “the truth” about certain threats, thus pre-structuring the discursive field in relevant ways (Huysmans, 2006, p. 72).

Cyber security, so the common assumption, arises from the interaction of technologies, processes, and everyday practices. Thus, the literature pays particular attention to how a variety of actors uses different representations of danger to create or change different political, private, social, and commercial understandings of security in selected public spheres. In addition, it gives more weight to material aspects of the issue in the tradition of STS (Balzacq & Dunn Cavelty, 2016; Collier, 2018; Shires, 2018; Stevens, 2016), looking at the co-constitution of technology and politics. In particular, it recognizes that the political reading of cyber security cannot be divorced from particular knowledge practices in different communities.

As the most recent research focus to emerge, literature in this cluster covers a variety of topics, united by a focus on understanding how cyber security

emerges as an assemblage of people, objects, and enacted ideas. Questions of authority and power are most directly addressed by research in this cluster. C. Stevens (2019) sets out to better understand the role of cyber security companies by looking at Symantec's analysis of Stuxnet and the publication of their reports in the public. Tanczer (2019) focuses on the increasingly blurred boundaries between field of security professionals and hackers, pointing to changes in the larger context of security and insecurity that are reflected in the practices of these technical experts and in the conception of them. Shires (2019) looks at how the cyber security industry portrays cyberspace as a terrain of persistent threat, systemic vulnerability, and intelligence ambiguity, a classic "noir" narrative that results from systemic economic deficiencies (distorted incentives for protection) and from systemic political deficiencies (black markets for new exploits). By focusing on non-traditional actors and aspects of politics, this type of research is able to make invisible aspects of cyber security visible.

Conclusion: Where is cyber security politics research headed?

Over the past decade, research in cyber security politics has seen the emergence of a growing interdisciplinary body of work that is at the same time theoretically informed, grounded in empirical observations, and policy-relevant in many of its insights. We have ended our intellectual history by outlining three research clusters. In place of a summary of the past and present evolution of cyber security as a security political issue, we want to look into a possible future of research on cyber security politics in this concluding section. We do this based on the same assumption discussed at the beginning of this article: that the trajectory of both cyber security research and cyber security policy will continue to be shaped by the interplay between technology, politics, and science. The direction in which research and policy will move will be co-constituted by technological possibilities, political choices, and scientific practices. We end our intellectual history with a brief outlook on likely developments in all three areas.

Digital technologies have politics, and technological possibilities and developments will require new governance mechanisms, while at the same time being shaped by politics. First, the interconnectedness between ever more complex socio-technical systems is bound to increase. Cyber security will grow in importance as a topic as countries all around the world strive to shape digital transformation processes that affect society, economy, and the state alike. In the context of what has been called fourth industrial revolution, the complexity of socio-technical systems will increase due the ubiquitous digitalization and automation of technical processes that support a great variety of socio-political institutions. As these technical system become tighter coupled and integrate more aspects of society and economy, cyber

security concerns will inevitably expand to more policy fields at both the national and international level. These developments will create new demands for technical and organizational research that needs to be better integrated with approaches from the social and political science.

Second, cyberspace will become increasingly dependent on space-based technologies and interlinked with newly emerging technologies in the fields of quantum computing and artificial intelligence (AI). This will increase the size of cyberspace. More importantly, as an enabling technology with diverse applications in all areas of life, AI will link cyberspace to more policy fields. AI will become an essential element of cyber security and will have a profound impact on the speed, scale, duration, autonomy, and complexity of cyber operations, for both offense and defense. These new technologies will be primarily developed by global technology firms and the private sector. As a consequence, state actors will likely become more dependent on technology firms and independent technology experts, further transforming the relationship between public and private actors. The fact that there is considerable uncertainty regarding the tempo and scope of these technological developments creates new demands for research that maps, assesses, models, and forecasts new technological possibilities. As social scientists, we need to understand the increasingly salient political and social aspects that will affect the patterns of cooperation and conflict in politics and society at the national and international level.

Political choices at the national and international level have a technological dimension. Politics will influence and govern technology development while at the same time being pre-structured by technology. First, we can expect that political and military actors will attempt to better understand the (limited) strategic utility of cyber operations below the level of armed conflict, in order to find the right balance between restraint and exploitation. One key challenge in this context is how best to manage the transformation of state intelligence services in the digital age and their growing dependence on private intelligence firms. Another key challenge is linked to information operations and propaganda that might be spread more targeted and effectively via AI technologies and social media platforms. These political developments raise important research questions that require interdisciplinary answers.

Second, public actors will uphold their efforts to control the risk of escalation through international cooperation. States cannot secure cyberspace on their own, without taking into account market and social forces; yet no stable cyber governance framework will emerge without greater convergence on responsible behavior among great powers. As long as great powers disagree about what represents responsible use of cyber operations in state interactions, and for that matter what forms of espionage and interference in the political process of other states through cyberspace are acceptable, little top-down progress will materialize. Bottom-up progress, on the other hand,

presupposes that the actors become more visible for each other in order to successfully work together in a multi-stakeholder framework. Research can shed light on invisible actors and analyze the interaction between market dynamics and political dynamics in stabilizing cyberspace, it can evaluate if the socio-technical institutions that secure cyberspace reflect the tools and practices of public and private actors.

Third, the key governance challenge at the domestic political level is how to overcome fragmentation of authority and accountability. Tighter coupling of technical systems and their growing interconnectedness with socio-political institutions creates growing demand for governance in networks, which in turn means that governments increasingly share responsibility with actors from business and society. The integration of policy into a coherent overall framework involves difficult trade-offs between security and privacy and creates horizontal and vertical coordination and cooperation problems across government and at the intersections between state, economy, and society. Research can evaluate how states can fine-tune their multidimensional roles. How states decide to regulate their technology base is moreover directly linked to how they anticipate this will influence their relative economic, political, and military power at the international level. Academics in this context can study how different (democratic and authoritarian) political systems balance regulation and market forces differently and what this means for state access to the private technology sector, export control systems of dual-use technologies, and screening mechanisms of foreign investment into the strategically relevant technology base.

Scientific practice, as our third and final sphere of interest, will keep co-evolving with the anticipated changes in the spheres of technology and politics. We started the article with the ascertainment that there is no “field” or “subfield” of cyber security politics—and we conclude with a wish that this remains true in the future. Research at the intersection of cybersecurity and security politics in order to remain relevant to policy choices and cognizant of technological possibilities needs to speak to a variety of other bodies of research, free to choose interesting and pressing issue without disciplinary constraints; it needs to co-opt some of the new data analytical tools offered by AI, and it needs to flexibly overcome some of the institutional barriers that slowed down its independent contribution to cyber security.

A first key challenge for cyber security politics research is conceptual and linked to the integration of theoretical knowledge from different disciplines and research traditions. Researchers need to better integrate concepts and mechanisms from IR and security studies, IPE, and intelligence studies to analyze the transformation of intelligence services and how this affects their relationship with private cyber security and intelligence firms. They need to better understand the interplay between (black) security markets and (covert) security political dynamics if they want to explain the co-existence

of strategic restraint and low-level subversion in cyberspace. Cyber security politics research must pay more attention to economic aspects of the phenomena at hand. Practice theory with its focus on technological possibilities and socio-technical processes allows to integrate these different approaches at the empirical level. STS offers a productive lens for understanding the mutual interplay between the technical and the socio-political sphere and, from an analytical point of view, to deal with the opaqueness of cyber operations. Such an approach is of critical importance in an attempt to shed light on how the cyber security policy and practice of states, both at the national and the international level, are facilitated or thwarted by the interests and practices of actors that are not easily visible, in- and outside of governments.

A second key challenge or indeed an opportunity for cyber security politics research is linked to the fact that more data about cyber operations by many different actors around the world and better tools to monitor and analyze this data are becoming available. While there is room for theory development and theory testing, we will likely enter an era of empirical work. In-depth qualitative studies on the role of invisible actors in state interactions linked to cyber security can be combined with more data-driven approaches that evaluate how new AI tools affect the cyber offense-defense balance. As state actors begin to integrate these tools in their border guards, police corps, armies and disaster response structures, important social and political questions will arise linked to privacy, bias, and control. Conversely, governments and societies will need to discuss how much of this new data should be made publicly available and what this means for data protection and privacy. From a research point of view, these developments call for more interdisciplinary research at the intersection of computer science, mathematics, economics, and political science.

A third key challenge for cyber security politics research is linked to overcoming the institutional barriers that slow down its independent contribution to cyber security and cyber security politics. Universities can help the public actors at the national and international level to catch up in their technology competence, while educating the next generation of experts for society and industry. Academia can contribute to the study of cyber conflict and through its independent and peer-reviewed knowledge broaden the knowledge base for some of the difficult policy choices discussed above. Science can collaborate with the private and public actors in the development of evidentiary standards and norms that will underpin the future resilience of socio-technical systems, and in the negotiation and establishment of new norms and institutions that should govern the use and misuse of these systems. Yet in order to free its full potential, universities must overcome the institutional barriers that slow down interdisciplinary and more so transdisciplinary research intersection of science, technology, while building a network of

institutions and programs that together can considerably expand the body of public knowledge surrounding these societally and politically relevant questions.

Notes

1. This claim is based on our previous knowledge of cyber security politics in (Western) democratic states that make such divisions possible. However, even in the absence of a clear division between state, society, and private sector, or in the absence of a political voice of one or two of these actor groups, we believe that our basic assumptions should hold more or less true.
2. “Science” understood as a collective term for “academic work,” “intellectual labor,” or “knowledge production,” not only “natural sciences.”

Acknowledgements

The ideas for this article are based on the stimulating discussions at a two-day cyber security politics conference in September 2018 as well as on our previous work on cyber security politics. We would like to thank all the conference participants, the anonymous reviewers, our colleagues at the Center for Security Studies, ETH Zürich and in particular Jasper Frei for his help with referencing and formatting the paper.

Disclosure statement

No potential conflict of interest was reported by the authors.

Notes on contributors

Myriam Dunn Cavelti is a senior lecturer for security studies and deputy for research and teaching at the Center for Security Studies (CSS) at ETH Zurich. She holds a Ph.D. from the University of Zurich. She was a visiting fellow at the Watson Institute for International Studies (Brown University) in 2007 and fellow at the stiftung neue verantwortung in Berlin, Germany 2010–2011. Her research focuses on the politics of risk and uncertainty in security politics and changing conceptions of (inter-)national security due to cyber issues (cyber-security, cyber-war, critical infrastructure protection) in specific. She has published, inter alia, in *Security Dialogue*, *International Political Sociology*, *European Journal of International Security*, and *International Studies Review*.

Andreas Wenger is professor of International and Swiss Security Policy at ETH Zurich and has been the Director of the Center for Security Studies (CSS) since 2002. He holds a Ph.D. from the University of Zurich. He was a visiting fellow at the Woodrow Wilson School of Public and International Affairs and the Center of International Studies, Princeton University. During that period, he wrote his doctoral dissertation analyzing the role of nuclear weapons in the Cold War international system. Andreas Wenger was a guest scholar at Princeton University (1992–1994), Yale

University (1998), the Woodrow Wilson Center (2000), and the George Washington University (2005). The focus of his main research interests lies on security and strategic studies and the history of international relations. He has published, inter alia, in the *Journal of Cold War Studies*, *Cold War History*, and *Presidential Studies Quarterly*.

ORCID

Myriam Dunn Cavelty  <http://orcid.org/0000-0002-3775-1284>

Reference list

- Alberts, D. S., & Papp, D. (Eds.). (1997). *The information age: An anthology of its impacts and consequences*. Washington, DC: National Defense University.
- Aradau, C., Huysmans, J., Neal, A., & Voelkner, N. (Eds.). (2014). *Critical security methods: New frameworks for analysis*. Abingdon, Oxon: Routledge.
- Arquilla, J., & Ronfeldt, D. F. (1992). *Cyberwar is coming!*. Santa Monica, CA: RAND Corporation.
- Arquilla, J., & Ronfeldt, D. F. (Eds.). (1997). *In Athena's camp: Preparing for conflict in the information age*. Santa Monica: RAND Corporation.
- Baezner, M. (2018a). *Hotspot analysis: Cyber disruption and cybercrime: Democratic people's Republic of Korea*. Zurich: Center for Security Studies (CSS), ETH Zurich.
- Baezner, M. (2018b). *Hotspot analysis: Synthesis 2017: Cyber-conflicts in perspective*. Zurich: Center for Security Studies (CSS), ETH Zurich.
- Baezner, M., & Robin, P. (2017a). *Hotspot analysis: Stuxnet*. Zurich: Center for Security Studies (CSS), ETH Zurich.
- Baezner, M., & Robin, P. (2017b). *Cyber-conflict between the United States of America and Russia*. Zurich: Center for Security Studies (CSS), ETH Zurich.
- Balzacq, T., & Dunn Cavelty, M. (2016). A theory of actor-network for cyber-security. *European Journal of International Security*, 1, 176–198. doi:10.1017/eis.2016.8
- Barlow, J. P. (1996, February 8). A declaration of the independence of cyberspace. *Electronic Frontier Foundation Website*. Retrieved from <http://homes.eff.org/~barlow/Declaration-Final.html>
- Behrent, M. C. (2013). Foucault and technology. *History and Technology*, 29, 54–104. doi:10.1080/07341512.2013.780351
- Berkowitz, B. D. (2003). *The new face of war: How war will be fought in the 21st century*. New York, NY: Free Press.
- Berners-Lee, T. (1999). *Weaving the web: The original design and ultimate destiny of the world wide web*. New York, NY: Harper Collins.
- Best, J., & Walters, W. (2013). Translating the sociology of translation. *International Political Sociology*, 7, 345–349. doi:10.1111/ips.12026_5
- Betz, D., & Stevens, T. (2011). *Cyberspace and the state: Toward a strategy for cyber-power*. London: The International Institute for Strategic Studies.
- Bigo, D. (2002). Security and immigration: Toward a critique of the governmentality of unease. *Alternatives: Global, Local, Political*, 27, 63–92.
- Bingham, N. (1996). Objections: From technological determinism towards geographies of relations. *Environment and Planning D: Society and Space*, 14, 635–657. doi:10.1068/d140635
- Borghard, E. D., & Lonergan, S. W. (2017). The logic of coercion in cyberspace. *Security Studies*, 26, 452–481. doi:10.1080/09636412.2017.1306396

- Bourbeau, P., Balzacq, T., & Dunn Cavelty, M. (2015). Celebrating eclectic dynamism: Security in international relations. In P. Bourbeau (Ed.), *Security: Dialogue across disciplines* (pp. 111–136). Cambridge: Cambridge University Press.
- Buchanan, B. (2016). *The cybersecurity dilemma: Hacking, trust, and fear between nations*. Oxford: Oxford University Press.
- Buzan, B., & Hansen, L. (2009). *The evolution of international security studies*. Cambridge: Cambridge University Press.
- Buzan, B., Waever, O., & De Wilde, J. (1998). *Security: A new framework for analysis*. Boulder, CO: Lynne Rienner.
- Collier, J. (2018). Cyber security assemblages: A framework for understanding the dynamic and contested nature of security provision. *Politics and Governance*, 6, 13–21. doi:10.17645/pag.v6i2.1324
- Cox, R. W. (1986). Social forces, states and world orders: Beyond international relations theory. In R. O. Keohane (Ed.), *Neorealism and Its Critics* (pp. 204–253). New York, NY: Columbia University Press.
- Deibert, R. (2002). Circuits of power: Security in the internet environment. In J. P. Singh, & J. Rosenau (Eds.), *Information technologies and global politics: The changing scope of power and governance* (pp. 115–142). New York, NY: SUNY Press.
- Deibert, R. (2003). Black code: Censorship, surveillance, and militarization of cyberspace. *Millennium: Journal of International Studies*, 32, 501–530. doi:10.1177/03058298030320030801
- Deibert, R. (2013). *Black Code. Surveillance, privacy, and the dark side of the internet*. Toronto: McClelland & Stewart.
- Deibert, R. (2017a). Trajectories of cyber security research. In A. Gheciu, & W. C. Wohlforth (Eds.), *Oxford handbook of international security* (pp. 531–546). Oxford: Oxford University Press.
- Deibert, R. (2017b). Cyber security. In M. D. Cavelty and T. Balzacq (Eds.), *Routledge handbook of security studies* (2nd ed., pp. 172–182). New York, NY: Routledge.
- Deibert, R., & Rohozinski, R. (2009, March 29). Tracking GhostNet: Investigating a cyber espionage network. *Information Warfare Monitor*, 17–45. Retrieved from <http://www.nartv.org/mirror/ghostnet.pdf>.
- Deibert, R., & Rohozinski, R. (2010). Risking security: The policies and paradoxes of cyberspace security. *International Political Sociology*, 4, 15–32. doi:10.1111/j.1749-5687.2009.00088.x
- DeNardis, L. (2014). *The global war for internet governance*. Cambridge, MA: Yale University Press.
- Dewar, R. S. (Ed.). (2018). *National cybersecurity and cyberdefense policy snapshots*. Zurich: Center for Security Studies. (CSS), ETH Zurich.
- Dillon, M., & Reid, J. (2009). *The liberal way of war: Killing to make life live*. London: Routledge.
- Dunn Cavelty, M. (2008). *Cyber-security and threat politics: US efforts to secure the information age*. London: Routledge.
- Dunn Cavelty, M. (2015). The normalization of cyber-international relations. In O. Thränert, & M. Zapfe (Eds.), *Strategic trends 2015: Key developments in global affairs* (pp. 81–98). Zurich: Center for Security Studies.
- Dunn Cavelty, M., & Egloff, F. J. (2019). The politics of cybersecurity: Balancing different roles of the state. *St Antony's International Review*, 15, 37–57.
- Dunn Cavelty, M., & Kristensen, K. S. (Eds.). (2008). *Securing the homeland: Critical infrastructure, risk, and (In)security*. London: Routledge.

- Egloff, F. J. (2019). Contested public attributions of cyber incidents and the role of academia. *Contemporary Security Policy*. Advance online publication. doi:10.1080/13523260.2019.1677324
- Egloff, F. J., & Wenger, A. (2019). Public attribution of cyber incidents. In F. Merz (Ed.), *CSS analyses in security policy*, 244 (pp. 1–4). Zurich: Center for Security Studies.
- Eriksson, J. (2001). Cyberplagues, IT, and security: Threat politics in the information age. *Journal of Contingencies and Crisis Management*, 9, 200–210. doi:10.1111/1468-5973.00171
- Eriksson, J., & Giacomello, G. (2006). The information revolution, security, and international relations: (IR)relevant theory? *International Political Science Review*, 27, 221–244. doi:10.1177/0192512106064462
- Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. *Survival*, 53, 23–40. doi:10.1080/00396338.2011.555586
- Finnemore, M., & Hollis, D. B. (2016). Constructing norms for global cybersecurity. *The American Journal of International Law*, 110, 425–479. doi:10.1017/S0002930000016894
- Fischerkeller, M. (2018). *Offense-defense theory, cyberspace, and the irrelevance of advantage*. Alexandria, VA: Institute for Defense Analysis.
- Fischerkeller, M. P., & Harknett, J. R. (2018). *Persistent engagement, agreed competition, cyberspace interaction dynamics, and escalation*. Alexandria, VA: Institute for Defense Analysis.
- Gartzke, E. (2013). The myth of cyberwar. Bringing war in cyberspace back down to earth. *International Security*, 38, 41–73. doi:10.1162/ISEC_a_00136
- Gartzke, E., & Lindsay, J. R. (2015). Weaving tangled webs: Offense, defense, and deception in cyberspace. *Journal of Strategic Studies*, 24, 316–348. doi:10.1080/09636412.2015.1038188
- Gartzke, E., & Lindsay, J. R. (2016). Coercion through cyberspace: The stability/instability paradox revisited. In K. Greenhill, & P. Krause (Eds.), *The power to hurt: Coercion in international politics* (pp. 179–203). Oxford: Oxford University Press.
- Georgieva, I. (2019). The unexpected norm-setters: Intelligence agencies in cyberspace. *Contemporary Security Policy*. doi:10.1080/13523260.2019.1677389
- Giles, K., & Hagestad, W. (2013). Divided by a common language: Cyber definitions in Chinese, Russian and English. In K. Podins, J. Stinissen, & M. Maybaum (Eds.), *Proceedings of the 5th international conference on cyber conflict* (pp. 1–17). Tallinn: CCD COE Publications.
- Gomez, M. A. (2019). Sound the alarm! Updating beliefs and degradative cyber operations. *European Journal of International Security*, 4, 190–208. doi:10.1017/eis.2019.2
- Graham, S. (1998). The end of geography or the explosion of place? Conceptualizing space, place and information technology. *Progress in Human Geography*, 22, 165–185. doi:10.1191/030913298671334137
- Grisby, A. (2017). The end of cyber norms. *Survival*, 59, 109–122. doi:10.1080/00396338.2017.1399730
- Hagmann, J., Hegemann, H., & Neal, A. W. (2019). The politicisation of security: Controversy, mobilisation. *Arena Shifting. European Review of International Studies*, 5, 3–29. doi:10.3224/eris.v5i3.01
- Hansen, L. (2006). *Security as practice: Discourse analysis and the bosnian war*. London: Routledge.

- Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International Studies Quarterly*, 53, 1155–1175. doi:10.1111/j.1468-2478.2009.00572.x
- Herrera, G. (2003). Technology and international systems. *Millennium: Journal of International Studies*, 32, 559–593. doi:10.1177/03058298030320031001
- Hitchens, T., & Gallagher, N. W. (2019). Building confidence in the cybersphere: A path to multilateral progress. *Journal of Cyber Policy*, 4, 4–21. doi:10.1080/23738871.2019.1599032
- Hofmann, J. (2016). Multi-stakeholderism in Internet governance: Putting a fiction into practice. *Journal of Cyber Policy*, 1, 29–49. doi:10.1080/23738871.2016.1158303
- Hurel, L. M., & Lobato, L. C. (2018). Unpacking cyber norms: Private companies as norm entrepreneurs. *Journal of Cyber Policy*, 3, 61–76. doi:10.1080/23738871.2018.1467942
- Hurwitz, R. (2014). The play of states: Norms and security in cyberspace. *American Foreign Policy Interests*, 36, 322–331. doi:10.1080/10803920.2014.969180
- Huysmans, J. (2006). *The politics of insecurity. Fear, migration and asylum in the EU*. London: Routledge.
- Kello, L. (2013). The meaning of the cyber revolution: Perils to theory and statecraft. *International Security*, 38, 7–40. doi:10.1162/ISEC_a_00138
- Kello, L. (2017). *The virtual weapon and international order*. New Haven, CT: Yale University Press.
- Keohane, R. O., & Nye, J. S. (1998). Power and Interdependence in the information age. *Foreign Affairs*, 77, 81–94.
- Kitchin, R., Perkins, C., & Dodge, M. (2009). Thinking about maps. In M. Dodge, R. Kitchin, & C. Perkins (Eds.), *Rethinking maps – new frontiers in cartographic theory* (pp. 1–26). London: Routledge.
- Kostyuk, N., & Zhukov, Y. M. (2019). Invisible digital front: Can low-level cyber operations shape battlefield events? *Journal of Conflict Resolution*, 63, 317–347. doi:10.1177/0022002717737138
- Krahmann, E. (2003). Conceptualizing security governance. *Cooperation and Conflict*, 38, 5–26. doi:10.1177/0010836703038001001
- Latour, B. (1999). *Pandora's hope: Essays on the reality of science studies*. Cambridge, MA: Harvard University Press.
- Lawson, S. (2013). Beyond cyber-doom: Assessing the limits of hypothetical scenarios in the framing of cyber-threats. *Journal of Information Technology & Politics*, 10, 86–103. doi:10.1080/19331681.2012.759059
- Leese, M., & Hoijsink, M. (Eds.). (2019). *Technology and agency in international relations*. London: Routledge.
- Lewis, J. A. (2018). *Rethinking cyber security: Strategy, mass effects, and states*. Washington, DC: Center for Strategic and International Studies.
- Libicki, M. (2000). The Future of Information Security [Web page]. Retrieved from <https://fas.org/irp/threat/cyber/docs/infosec.htm>.
- Libicki, M. (2009). *Cyberdeterrence and cyberwar*. Santa Monica, CA: RAND Corporation.
- Liff, A. P. (2012). Cyberwar: A new “absolute weapon”? The proliferation of cyberwarfare capabilities and interstate war. *Journal of Strategic Studies*, 35, 401–428. doi:10.1080/01402390.2012.663252
- Lindsay, J. R. (2017). Restrained by design: The political economy of cybersecurity. *Digital Policy, Regulation and Governance*, 19, 493–514. doi:10.1108/DPRG-05-2017-0023

- Maness, R., & Valeriano, B. (2016). The impact of cyber conflict on international interactions. *Armed Forces & Society*, 42, 301–323. doi:10.1177/0095327X15572997
- Matthewman, S. (2011). *Technology and social theory*. Basingstoke: Palgrave Macmillan.
- Maurer, T. (2017). *Cyber mercenaries: The state, hackers and power*. Cambridge: Cambridge University Press.
- McCarthy, D. (Ed.). (2018). *Technology and world politics: And introduction*. London: Routledge.
- Mueller, M. L. (2010). *Networks and states: The global politics of internet governance*. Cambridge, MA: The MIT Press.
- Naughton, J. (2016). The evolution of the internet: From military experiment to general purpose technology. *Journal of Cyber Policy*, 1, 5–28. doi:10.1080/23738871.2016.1157619
- Nye, J. S. (2010). *Cyber power*. Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School.
- Nye, J. S. (2011). *The future of power* (Vol. 11). New York, NY: PublicAffairs.
- Papp, D. S., Alberts, D. S., & Tuyahov, A. (1997). Historical impacts of information technologies: An overview. In D. S. Alberts, & D. S. Papp (Eds.), *The information age: An anthology of its impacts and consequences* (pp. 13–35). Washington, DC: National Defense University.
- Peters, G., & Pierre, J. (1998). Governance without government? Rethinking public administration. *Journal of Public Administration Research and Theory*, 8, 223–243. doi:10.1093/oxfordjournals.jpart.a024379
- Peterson, D. (2013). Offensive cyber weapons: Construction, development, and employment. *Journal of Strategic Studies*, 36, 120–124. doi:10.1080/01402390.2012.742014
- Price, M. (2018). The global political of internet governance: A case study in closure and technological design. In D. McCarthy (Ed.), *Technology and world politics: And Introduction* (pp. 126–145). London: Routledge.
- Rattray, G. (2001). *Strategic warfare in cyberspace*. Cambridge, MA: The MIT Press.
- Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies*, 38, 4–37. doi:10.1080/01402390.2014.977382
- Rosecrance, R. (1999). *The rise of the virtual state: Wealth and power in the coming century*. New York, NY: Basic Books.
- Rosenau, J. N. (1998). Global affairs in an epochal transformation. In C. Henry, C. Ryan, & E. Peartree (Eds.), *Information revolution and international security* (pp. 33–57). Washington, DC: Center for Strategic and International Studies.
- Rothkopf, D. J. (1998). Cyberpolitik: The changing nature of power in the information age. *Journal of International Affairs*, 51, 325–360.
- Sabbah, C. (2018). Pressing pause: A new approach for international cybersecurity norm development. In T. Minárik, R. Jakschis, & L. Lindström (Eds.), *10th international conference on cyber conflict CyCon X: Maximising effects* (pp. 263–281). Tallinn: CCDCOE.
- Saco, D. (1999). Colonizing cyberspace: “National security” and the internet. In J. Weldes, M. Laffey, H. Gusterson, & R. Duvall (Eds.), *Cultures of insecurity: States, communities, and the production of danger* (pp. 261–292). Minneapolis, MI: University of Minnesota Press.
- Salamon, L. M. (2002). The tools approach and the new governance: Conclusion and implications. In L. M. Salamon (Ed.), *The tools of government: A guide to the new governance* (pp. 600–610). Oxford: Oxford University Press.

- Schwab, K. (2018). *Shaping the future of the fourth industrial revolution: A guide to building a better world*. New York, NY: Currency.
- Shepherd, L. J. (2008). *Gender, violence and security: Discourse as practice*. London: Zeb Books.
- Shires, J. (2018). Enacting expertise: Ritual and risk in cybersecurity. *Politics and Governance*, 6, 31–40. doi:10.17645/pag.v6i2.1329
- Shires, J. (2019). Cyber-noir: Cybersecurity and popular culture. *Contemporary Security Policy*. Advance online publication. doi:10.1080/13523260.2019.1670006
- Slayton, R. (2017). What is the cyber offense-defense balance? Conceptions, causes, and assessment. *International Security*, 41, 72–109. doi:10.1162/ISEC_a_00267
- Smeets, M. (2018). A matter of time: On the transitory nature of cyberweapons. *Journal of Strategic Studies*, 41, 6–32. doi:10.1080/01402390.2017.1288107
- Stevens, C. (2019). Assembling cybersecurity: The politics and materiality of technical malware reports and the case of Stuxnet. *Contemporary Security Policy*. Advance online publication. doi:10.1080/13523260.2019.1675258
- Stevens, T. (2016). *Cyber security and the politics of time*. Cambridge: Cambridge University Press.
- Tancer, L. M. (2019). 50 shades of hacking: How IT and cybersecurity industry actors perceive good, bad, and former hackers. *Contemporary Security Policy*. Advance online publication. doi:10.1080/13523260.2019.1669336
- Valeriano, B., & Maness, R. (2014). The dynamics of conflicts between rival antagonists, 2001–2011. *Journal of Peace Research*, 51, 347–360. doi:10.1177/0022343313518940
- Valeriano, B., & Maness, R. (2015). *Cyber war versus cyber realities: Cyber conflict in the international system*. Oxford: Oxford University Press.
- Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97–102. doi:10.1016/j.cose.2013.04.004
- Waever, O. (2010). Towards a political sociology of security studies. *Security Dialogue*, 41, 649–658. doi:10.1177/0967010610388213
- Weber, V. (2018). Linking cyber strategy with grand strategy: The case of the United States. *Journal of Cyber Policy*, 3, 236–257. doi:10.1080/23738871.2018.1511741
- Wilner, A. (2019). US cyber deterrence: Practice guiding theory. *Journal of Strategic Studies*. Advance online publication. doi:10.1080/01402390.2018.1563779