1 Introduction

Cyber security between socio-technological uncertainty and political fragmentation

Myriam Dunn Cavelty and Andreas Wenger

In the past decade, cyber security has consolidated its position as one of the top national security issues of the 21st century: The dynamic interaction between technological vulnerabilities and the possibilities of their political misuse creates a problem space with little stability. Due to enduring uncertainties about the scope and tempo of ongoing socio-technological transformations, an increasing willingness to use disruptive cyber tools in the context of great power rivalry, and significant fragmentation of authority and accountability on different levels, managing cyber insecurities continues to be a most challenging governance issue in contemporary politics.

Cyber security is challenging because it is a so-called “wicked problem”. Cyber security is “transboundary in nature, occur[s] at multiple levels across sectors, between institutions, and will impact all actors, both public and private, in complex, interconnected, and often highly politicised ways” (Carr and Lesniewska 2020: 392). Wicked problems avoid straightforward definitions and are impossible to solve in simple or final ways because they are composed of many interdependent factors that are often in flux (Rittel and Weber 1973). In addition, involved stakeholders have divergent values, goals, and motivations when it comes to the issue, making it difficult to find solutions that satisfy everyone to a sufficient degree.

As a politically relevant problem, cyber security evolves at the intersection between fast-paced technological development, the political and strategic use of these tools by state and non-state actors, and the various attempts by the state and its bureaucracies, society, and the private sector to define appropriate responsibilities, legal boundaries, and acceptable rules of behavior for this space. Our edited volume sheds light on socio-technical uncertainties and political responses. In 16 chapters, we highlight different facets of this problem space, showing how cyber security challenges states, private actors, and civil society in multiple ways because of dynamic, unforeseeable changes arising from the complex interactions between technical and social systems that have mounting political significance.

Socio-technical uncertainties in complex systems

Cyberspace is a complex socio-technical system. Three points are important in this context: First, cyberspace is brought into being by technologies that are made by humans. What might seem like a somewhat banal statement at first has considerable consequences that are not in the least banal consequences for how to conceptualize cyber security. The intentions, norms, and values of technological developers find their way into the artifacts during the design stage, while existing power structures influence the desirability of specific aspects or forms of technology (Matthewman 2011; Krause 2019). Hence, technologies are to be treated as inseparable from politics and vice versa, which necessitates analytical approaches that are sensitive to how technologies are shaped by political contexts and in turn enable specific political actions in the security domain. Just as importantly, economic forces influence many aspects of technical innovation and shape the availability of products and services to counter cyber risks (Lindsay 2017; Burkart and McCourt 2017). There is no thorough understanding of how economic and political factors interact in the literature yet.

Second, cyberspace is not independent but is closely intertwined with other systems such as the energy network – which in turn depends on communication infrastructure, creating co-dependencies. Important infrastructures and services and their respective interdependencies with digital infrastructures matter in the security discourse because they are crucial for the functioning of society – in fact, cyber security has reached the level of a key national security issue predominantly due to how the topic was interlinked with the critical infrastructure debate in the political process (Collier and Lakoff 2008). In addition, the cyber security discourse has changed considerably over the last 20 years: Cyber security is moving upward in the political agenda and expanding sideways as a problem area to a multitude of additional policy domains with advancing digitalization (Dunn Cavelty and Egloff 2019). As the currently last, important development, the cyber-incidents during the US elections in 2016 – attributed to the Russian government as well as semi-state actors – started a new chapter in the cyber security debate. The hack and leak operations highlighted the issue of strategic manipulation – also called influence operations – as a threat to democratic processes (Whyte 2020). While influence operations are far from new, the current technological environment affords different actors with new opportunities.

Third, cyberspace consists of multiple interactions between the underlying technology and its human users and operators. It is human interaction with technology – and the interaction between humans by means of technologies – that creates cyberspace in the first place. Furthermore, the growing complexity and nonlinear behavior of a complex system, like cyberspace, leads to a growing probability of unexpected disruptive events – from internal accidents to malicious attacks from both inside and outside the system (Hiermaier and Scharte 2019). Growing complexity offers new incentives and possibilities to threat actors to target people and assets in and through cyberspace. These varied interactions with technology introduce a specific type of uncertainty: It is an ontologically intrinsic

type of uncertainty linked to human decisions, making us “part of the problem, system and potential solutions” (Sword Daniels et al. 2018: 291).

Political responses and emergent governance arrangements

As a wicked problem, cyber security is notoriously hard to pin down and is contested politically on conceptual and practical grounds in both national and international arenas. This is little surprising, given that security is an essentially contested concept to begin with – one whose proper use “inevitably involves endless disputes about their proper uses on the part of their users” (Gallie 1956: 169). If we consider security politics as “interactions through which values are allocated authoritatively for a society” (Easton 1965: 21), it becomes clear that defining the parameters of any type of security is always about difficult political choices, because the identification of valuable objects in need of protection from particular threats assigns legitimate claims to protection to some security objects and political subjects, but not to others.

In line with this, the “security” in cyber security means fundamentally different things to different communities. On a basic level, the security of digital technologies is grounded in risk management practices developed by computer specialists to make computers and computer networks more secure. Yet, cyber security is more than information security: Rather than just seeking to protect information assets it also extends to humans and their interests (Von Solms and Van Niekerk 2013). Moreover, decisive for the elevation of the issue from a technical to a security political issue was the realization in the 1990s that a set of high-value assets, so-called critical infrastructures, whose disruption or destruction could have severe consequences for a nation, were getting increasingly dependent on digital technologies for a variety of functions (Dunn Cavelty 2008). The related threat discourse that emerged consists of two interlinked factors, linking technical systems to more traditional threat politics: An outward-looking focus that sees an increasing willingness of malicious actors to exploit the weaknesses inherent in our societies without hesitation or restraint. This is coupled with an inward-looking focus on system-inherent vulnerabilities in (computer) systems. Beyond the technical realm, cyber security has become a type of security that refers to offensive and defensive activities of state and non-state actors in cyberspace, serving the pursuit of wider security political goals through the exploitation of various related opportunities (Deibert and Rohozinski 2010).

That said, the right role of the state in cyber security matters remains politically contested because cyber security is *not only* about national security. The question is not whether there *is* a role for the state – but who should have what kind of role and responsibility in different governance arrangements that aim to enhance national and international security (Dunn Cavelty and Egloff 2019). Obviously, states alone cannot ensure an increase of cyber security, not least because many crucial networks are in private hands. 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 (Dunn Cavelty and Wenger 2020).

Fragmentation of political power can occur through decentralization when government tasks and authority are delegated downward (localization), upward (supranationalization), or sideways (privatization). It also takes place inside the government itself through ever-increasing functional differentiation of the administration. Increasingly, performing tasks requires highly specific expert knowledge. The increasing division of labor, a hallmark of modern societies, blurs the lines between the public and the private sectors. Many tasks that were previously performed by the state are now handled by specialized companies. This reshuffling of responsibility and power is ongoing and probably one of the defining features of cyber security politics.

The objective and structure of the book

The main objective of this book is to portray how technological developments interact with broader sociopolitical and socioeconomic dynamics that call for different national and international political responses. To that end, we bring together innovative, interdisciplinary conceptualizations of a changing threat landscape and explore how national and international governance solutions interact with this environment.

We understand the politics of cyber security as follows: As the interplay between *digital technologies*, their development, their use and misuse by human actors in conflictual economic, social, and political contexts, and the enduring *negotiation processes* between politically relevant actors about their roles and responsibilities in governing this problem space. There is an international security dimension, with state actors trying to shape and use cyberspace in accordance with their strategic goals – while at the same time attempting to stabilize the strategic environment through the development of behavioral norms (Dunn Cavelty and Wenger 2020). In addition, there is a domestic dimension, where states and their bureaucracies negotiate roles and responsibilities with civil society actors and the private sector. Our volume will combine national and international, state and non-state, technical, social, economic, and political perspectives, paying tribute to the complex environment in which cyber security is situated. The book has two main parts: the first focuses on the changing socio-technical environment and its implications for political action, while the second deals with the political responses.

Part I: The changing socio-technological environment and its impact on cyber threats

A first group of chapters focuses on the choice for and effects of cyber influence operations against the backdrop of domestic and international political fragmentation, heightened geopolitical tensions, and international disagreements about accepted political behavior in cyberspace. Though the use of disinformation in

conflictual contexts is not a novel phenomenon, it has emerged as a new focal point in contemporary cyber security politics. One of the key questions that the scholarly community should strive to answer is why cyber influence operations have become so interesting of late, what actual impact they have and how we can best study said impact, and what can be done against potentially destabilizing effects. Three chapters in the book give partial answers to these questions.

Marie Baezner and Sean Cordey outline recent trends in cyber operations, showing how different actors in conflictual settings exploit conceptual and legal grey zones (Baezner and Cordey 2022). The chapter thus explores why cyber influence operations have become one of the more interesting tools for both state and non-state actors, even if purposeful strategic impact might be elusive. At the macro level, this trend is due to the overarching political fragmentation, intensification of international rivalries, costly and complex interdependences, relative imbalance in military power/capabilities, and socio-technological vulnerabilities. At the micro and operational-technical level, the relative availability and accessibility of cyber tools coupled with the flexibility, customizability, rapidity, scalability, and limited escalation potential of cyber operations is the main driver for their use. Supported by examples from a range of operations observed in the last few years, the chapter shows the reader that cyber operations, which include cyber influence operations, are efficient and effective tools for disruption and at the same time enhance and transform traditional grey zone activities, such as espionage and influence. It is rather likely therefore that we will see more of this kind of operations in the future. But what are their impacts?

In his chapter, Wolf Schünemann adds to our understanding of the phenomenon and its political impact (Schünemann 2022). Analyzing the existing literature about influence operations, he asks what the contributions and findings are in terms of theory, methods, and empirics and looks at whether there is good empirical evidence that disinformation has a destabilizing effect on democracies. With a three-layered distinction between a micro, a meso, and a macro level of analysis at which distortion and influence can be measured, the chapter includes three perspectives of importance for a solid threat assessment of disinformation campaigns. Moreover, with echo chambers and automation, Schünemann refers to phenomena that are widely associated with the structural transformation of the digital public sphere and are assumed to be facilitating factors for the spread of disinformation. The chapter finds, however, that just like with disinformation in general, their alleged effects are very difficult to prove – thereby adding to the overall uncertainty political actors find themselves in.

Noting that countermeasures need to be drafted carefully since our understanding of the overall challenge is incomplete at best, Schünemann passes the ball to the next chapter in the volume. Based on the notions of cultural violence and cultural peace, the chapter by Jasmin Haunschild, Marc-André Kaufhold, and Christian Reuter shows the potential for political fragmentation through social media, focusing on fake news and terrorist propaganda, and their amplified dissemination through social bots. They show that technology plays an ambiguous role, on the one hand being an amplifier and enabler of effects such as astroturfing

and smoke screening, but on the other hand also enhancing social bot detection. However, noting that technology is just one aspect in this issue area, the authors raise the important point that technical interventions cannot address the root causes that make people spread or believe disinformation in the first place. Their findings raise interesting questions about the definition of victims and perpetrators of online structural violence. They ask: “Are people who spread misinformation and propaganda perpetrators of societal fragmentation and structural violence, or victims of a society that has left them with low media literacy and the feeling of being alienated by the society they live in?” (Haunschild et al. 2022: 58). The more digital technologies become interwoven with society and its general functioning, the harder will it be to isolate them from the humans that use them.

The book then moves on to look at new technological developments and their current and future impact on cyber security politics. We look at three technological areas: artificial intelligence/machine learning, quantum computing, and the expansion of cyberspace into space. In his chapter on artificial intelligence and the offense–defense balance in cyber security, Matteo Bonfanti provides an overview over the debate about so-called artificial intelligence in cyber security (Bonfanti 2022). It clarifies the concept of artificial intelligence (AI) and shows in which security-related fields such tools are already used. However, Bonfanti makes clear that future projections are very hard because the actual usage of new technologies depend on too many factors that are highly uncertain. What seems clear, and reinforces the observation made in the previous chapter, is that despite the many uncertainties of how AI will be used in the future, it will benefit both the defense and the offense. Who will benefit more will depend on the capacity of cyber security stakeholders in the private and the public section to master and leverage AI technologies for specific purposes. This usage will be inevitably shaped by the models of governance which will emerge from the formal/informal, fragmented/coordinated, and often unbalanced interactions among public authorities, private organizations, and the civil society.

Following a similar path of reasoning, Jon R. Lindsay evaluates the implications of quantum computing on cyber security and security more generally (Lindsay 2022). The chapter shows that cryptology is shaped by a paradoxical dynamic of cooperation-enabled competition in line with an expanded play of intelligence and covert influence, with ambiguous implications for strategic stability. Using the advent of quantum computing as a thought experiment, the chapter tackles technologically deterministic projections that are rampant in the field of cyber security. In short, if it were true that technology determines politics, then radical changes in technical infrastructure should have important, potentially equally radical political consequences. Focusing on the contest between code makers and code breakers against the backdrop of political logical, strategic context, and organizational implementation, the chapter shows convincingly how such deterministic perspectives neglect the social factors that shape secrecy and intelligence regardless of the type of technology that is involved. Even though quantum computing is making this contest more complex, its political implications are far from predetermined.

In the subsequent chapter, Johan Eriksson and Giampiero Giacomello look at the expansion of cyber infrastructure into the atmosphere and beyond through balloons, satellites, and other bodies in space, spearheaded by private actors (Eriksson and Giacomello 2022). By using fragmentation, vulnerability, and uncertainty as central analytical concepts, the chapter focuses on what this technological change means for the threat landscape, governance, as well as power and accountability. A central point in Eriksson and Giacomello's chapter is how the multiplication of actors and different forms of public-private constellations lead to increasing fragmentation and to more uncertainties. Just like Bonfanti and Lindsay point out in their chapters, new technologies co-create ambiguities because they are embedded in social and political systems that shape the very development as well as the possibilities of use and misuse of these technologies.

Part II: Emerging political responses in a complex environment

Switching to political responses as part of these developments, the book first focuses on the link between an uncertain environment, the role of decision-making in cyber security politics, and academic ways to study them. The uncertainties policy makers face in creating strategies and assessing their effectiveness also become a fundamental challenge for scholars who aim to trace, understand, and explain dynamics in the cyber domain.

Miguel Gomez and Chris Whyte present an analysis of national responses to a cyber security incident in a series of war games involving participants from Taiwan, the Philippines, and the United States (Gomez and Whyte 2022). With the majority of real-world incidents contextualized by geostrategic rivalries involving salient issues and the rise of both cyber capabilities and the willingness to engage in this domain, a better understanding of strategic decision-making becomes all the more crucial. This chapter, in response, applies a pseudo-experimental design to the increasingly popular activity of war gaming to better understand the processes involved in responding to cyber security incidents. By focusing on cognitive heuristics in decision-making and its consequences, the chapter contributes to a "behavioral turn" in the literature. Through war games, the authors observe the value of distinct cross-national perspectives in explaining variation in outcomes across participants. Despite the broad similarities among the participants involved, it is clear that cultural, procedural, and political expectations unique to each national context shape preferences and corresponding actions. As a result, the authors argue for the existence of distinct approaches to cyber security which may or may not reflect prevailing strategic realities but are, instead, rooted in preexisting beliefs among decision-makers. In their chapter, the authors continue the trend of presenting cyber security as a sphere of action that can only be fully understood when we embed it in a much broader context.

Continuing in this vein, Amir Lupovici focuses on Israel's cyber deterrence strategy (Lupovici 2022). He suggests that the Israeli case is puzzling: Despite the prominence of deterrence in Israeli strategic thinking and despite the prominence of cyber technology in Israel, Israel started to incorporate cyberspace into

deterrence strategy late and to a limited extent only. How can this be explained? By combining discourse analysis, process tracing, and interviews, the chapter shows what role new constructions of cyber security and political trade-offs played in this evolution. Lupovici makes the point that the uncertainties in the cyber domain not only create difficulties for political actors, but that the same uncertainties also exacerbate scholars' ability to explore the practices, behavior, and strategies of involved actors. His remedy is to focus on the aforementioned embeddedness, namely, to ask, "how technological impetus is embedded in actors' narratives, strategic culture, and identities, and how adopting a certain strategy fits or challenges international norms" (Lupovici 2022: 130). This, so the author, provides new opportunities for studying topics that are defined by uncertainties, rapid changes, and fragmentation of authority. Overall, paying attention to the context of technological change can help us understand how policy makers develop new strategies but also adapt old strategies, such as deterrence, to new domains.

Moving on, we explore how three different states in different geopolitical settings attempt to tackle fragmentation of authority and accountability, outlining both differences and commonalities in their struggles. We show that the integration of cyber security policy into a coherent overall framework involves difficult trade-offs between security and privacy, and that outside influence and policy diffusion do not always translate into effective or legitimate policies.

Stefan Steiger looks at contestation in the formation of the German cyber security policy (Steiger 2022), focusing on the interactions between different actors in their attempts to establish stable and legitimate policies. The chapter analyzes the development of the German cyber security policy in four areas: law enforcement, intelligence services, military, and the protection of critical infrastructure. Drawing on role theory, the chapter proposes a two-level game to account for domestic and international influences on the development of cyber security policies. This approach facilitates a holistic look at the factors that shape cyber security policies. The chapter argues that in order to establish stable cyber security policies the administration's role (in this case "protector") has to be met by complementary counter roles from parliament, judiciary, non-state actors, and international partners. These role plays follow different patterns in the four areas that are studied because of the actors involved and the different kinds of insecurity that have to be addressed. The chapter shows that the government has expanded its protective role, but it also illustrates processes of contestation that limited domestic and international role taking and thereby shaped the cyber security policy.

Aaron Brantly's chapter focuses on Ukraine (Brantly 2022). Ukraine has struggled with the help of European and NATO allies to forge multiple organizational structures capable of facilitating national cyber and information security. The chapter offers a detailed analysis on the construction of national information resilience and cyber capability by a medium-sized state under duress and coercion from an adversary state. The result is an analysis of how the interaction of rapid socio-technological transformation in a highly fragmented political context translated into a hybrid approach to countering propaganda and disinformation, on the one hand, and a centralized approach to addressing cybersecurity

challenges, on the other. Overall, Brantly highlights the importance of bureaucratic politics and historical path-dependencies in the shaping of new approaches to cyber threats.

Similarly, Islam Jusufi demonstrates how cyber security is tackled in the Albanian context (Jusufi 2022). Just like Brantly, Jusufi describes the development of the policy approach as a push and pull between different internal and external forces, between cultural contexts and political change, between fears of big attacks and the realities of everyday cyber crime. Standing for other small states transitioning to liberal democracies, Albania can serve as an example for how uncertainties in the cyber realm give more power to non-state actors, especially in the private sector and how these shifts in power translate into the need for states to adapt their ideas of sovereignty and rule. When capacities are low, it seems that international organizations play a big and important role in exporting ideas around multistakeholder models and legitimacy that are then adopted to local contexts.

The last three chapters move inside and beyond the state. Understanding political behavior in cyberspace is difficult at times due to the opaqueness of cyber operations and the limited visibility and ambiguity of many of the involved actors, especially private actors and intelligence agencies. Jacqueline Eggenschwiler focuses on non-state actors in the development of cyber norms (Eggenschwiler 2022). Her chapter examines the contributions of corporate actors to cyber security norm development processes. Specifically, it summarizes and comments on the effectiveness of the norms-based cyber insecurity reduction measures undertaken by technology companies. As a result of political and ideological contentions among governments, and against the background of increasing numbers of threats emanating from cyberspace, corporate entities have started inserting their voices more vocally in debates about rules of the road for the digital domain. The chapter argues that while the norms-based activities carried out by technology firms have been effective in terms of output and outcome, their efforts have borne less fruit apropos decreasing systemic risks and levels of cyber insecurity, respectively. However, this does not mean that their efforts are fruitless: In an environment as malleable as the cyber environment, norm development is messy and often linked to practices.

A concrete set of practices is what Danny Steed looks at in his chapter (Steed 2022) when he examines the impact of cyber security on intelligence practices. He reveals two broad themes: first, that the specific actions and adaptation from intelligence communities are acutely reflective of broader socio-technological transformations presented by the wider information revolution. Secondly, that the actions taken by certain intelligence agencies carry significant political repercussions for the future of cyber security itself. In this vein the chapter shows that in numerous ways the actions taken by intelligence agencies to remain effective instruments of national security actively contributes to exacerbated political fragmentation and an arguable state of increased and increasing cyber *in*security. To Steed, “the impact of intelligence *upon* cyber security carries more significant consequences to political fragmentation and cyber security politics than the

impacts of cyberspace upon how the intelligence services conducts their affairs” (Steed 2022: 215).

It is such uneven, invisible power to shape the environment that makes cyber security such a difficult policy topic. In the last chapter, Brenden Kuerbis, Farzaneh Badiei, Karl Grindal, and Milton Mueller offer a view on how the strategic use of cyberspace could be made more governable by examining some of the current practice of cyber attribution, scientific developments in the field, and possibilities for its transnational institutionalization (Kuerbis et al. 2022). Looking at cases from 2016 to 2018, the authors find that new technical approaches reliant on observable artifacts occurring in private networks and behavioral differences of states are upping the need for institutionalizing neutral, transnational attribution where evidence can be assessed and independently reviewed. Most recently, a network of university, civil society, and industry-based researchers have sought to develop attribution capabilities that are considered scientific and credible by the broader community. Numerous challenges remain to this collective action. However, if successful, it could effectively counter state-sponsored or affiliated cyberattacks and the strategic use of attribution, therefore bringing more stability to cyberspace.

In the conclusion, Andreas Wenger and Myriam Dunn Cavelty (Wenger and Dunn Cavelty 2022) highlight four main issues emerging from the individual chapters of this book. The first major point is about the limited strategic utility of cyber operations. Rather than being noticeably escalatory or resulting in visible changes in the existing balance of power between great powers, they are mainly used as tools of subversion and mild sabotage. The second issue deals with the dynamic interrelationship between emerging technologies and the future of cyber security politics, highlighting the role of private actors, tech race dynamics as drivers of cyber threat perceptions as well as the role of institutional factors in shaping the influence that emerging technologies have on the balance between the offense and the defense. A third issue deals with the challenge of upholding strategic stability under multidimensional uncertainty, whereby the chapter discusses the micro-dynamics of decision-making that might drive escalation under uncertainty and ambiguity, the ambiguities of attribution as a precondition for a credible deterrence threat, and the growing role of intelligence in cyberspace. The fourth issue the chapter discusses is how to overcome fragmentation of authority and accountability.

Conclusion

Digital technologies are transforming many aspects of social and political life at a rapid pace while at the same time, they themselves are shaped by political decisions and governance arrangements that seek to balance opportunities and risks in an optimal way. This co-dependency and co-shaping of technology and politics plays a role in all the chapters in this volume. To study it, the authors are sensitive to the complex and non-determined workings of socio-technical systems and assemblages, rather than falling prey to technological determinism

that isolates technological artifacts from their societal, economic, and political contexts.

The fact that there is considerable uncertainty regarding the tempo and scope of 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 of technologies that will affect the patterns of cooperation and conflict in politics and society at the national and international levels. But social scientists also need to become increasingly apt at conversing with a variety of technical disciplines. At the very minimum, we need to familiarize ourselves through expert publications, better even, start a regular dialogue with colleagues in the technical sciences. Even though solutions for wicked problems are elusive, beginning to bridge the gap between different communities is a necessary start.

Bibliography

All links checked on August 20, 2021.

- Baezner, M. and Cordey, S. (2022). Cyber in the Grey Zone: Influence Operations and Other Conflict Trends. In: M. Dunn Cavelty and A. Wenger (eds). *Cyber Security: Socio-Technological Uncertainty and Political Fragmentation*. London: Routledge, pp. 17–31.
- Bonfanti, M. E. (2022). Artificial Intelligence and the Offence-Defence Balance in Cyber Security. In: M. Dunn Cavelty and A. Wenger (eds). *Cyber Security: Socio-Technological Uncertainty and Political Fragmentation*. London: Routledge, pp. 64–79.
- Brantly, A. (2022). Battling the Bear: Ukraine’s Approach to National Cyber and Information Security. In: M. Dunn Cavelty and A. Wenger (eds). *Cyber Security: Socio-Technological Uncertainty and Political Fragmentation*. London: Routledge, pp. 157–171.
- Burkart, P. and McCourt, T. (2017). The International Political Economy of the Hack: A Closer Look at Markets for Cybersecurity Software. *Popular Communication*, 15(1): 37–54.
- Carr, M. and Lesniewska, F. (2020). Internet of Things, Cybersecurity and Governing Wicked Problems: Learning from Climate Change Governance. *International Relations*, 34(3): 391–412.
- Collier, S. J. and Lakoff, A. (2008). The Vulnerability of Vital Systems: How “Critical Infrastructure” Became a Security Problem. In: M. Dunn and S. Kristensen (eds). *The Politics of Securing the Homeland: Critical Infrastructure, Risk and Securitisation*. London: Routledge, pp. 17–39.
- Deibert, R. and Rohozinski, R. (2010). Risking Security: The Policies and Paradoxes of Cyberspace Security. *International Political Sociology*, 4: 15–32.
- Dunn Cavelty, M. (2008). *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. London: Routledge.
- Dunn Cavelty, M. and 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. and Wenger, A. (2020). Cybersecurity Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science. *Contemporary Security Policy*, 41(1): 5–32.

- Easton, D. (1965). *A Systems Analysis of Political Life*. New York: John Wiley.
- Eggenschwiler, J. (2022). Big Tech's Push for Norms to Tackle Uncertainty in Cyberspace. In: M. Dunn Cavelty and A. Wenger (eds). *Cyber Security: Socio-Technological Uncertainty and Political Fragmentation*. London: Routledge, pp. 186–204.
- Eriksson, J. and Giacomello, G. (2022). Cyberspace in Space: Fragmentation, Vulnerability, and Uncertainty. In: M. Dunn Cavelty and A. Wenger (eds). *Cyber Security: Socio-Technological Uncertainty and Political Fragmentation*. London: Routledge, pp. 95–107.
- Gallie W. B. (1956). Essentially Contested Concepts. *Proceedings of the Aristotelian Society*, 56: 167–198.
- Gomez, M. A. and Whyte, C. (2022). Cyber Uncertainties: Observations from Cross-National Wargames. In: M. Dunn Cavelty and A. Wenger (eds). *Cyber Security: Socio-Technological Uncertainty and Political Fragmentation*. London: Routledge, pp. 111–127.
- Haunschild, J., Kaufhold, M.-A. and Reuter, C. (2022). Cultural Violence and Peace in Social Media: Technical and Social Interventions. In: M. Dunn Cavelty and A. Wenger (eds). *Cyber Security: Socio-Technological Uncertainty and Political Fragmentation*. London: Routledge, pp. 48–63.
- Hiermaier, S. and Scharte, B. (2019). Fault-Tolerant Systems. In: R. Neugebauer (ed.). *Digital Transformation*. Berlin: Springer, pp. 285–300.
- Jusufo, I. (2022). Uncertainty, International Obligations, Fragmentation and Sovereignty: Cyber Security in Albania. In: M. Dunn Cavelty and A. Wenger (eds). *Cyber Security: Socio-Technological Uncertainty and Political Fragmentation*. London: Routledge, pp. 172–185.
- Krause, K. (2019). Technologies of Violence. Myriam Dunn Cavelty and Jonas Hagmann in Conversation with Keith Krause. In: C. Kaltfofen et al. (eds). *Technologies of International Relations – Continuity and Change*. Basingstoke: Palgrave Macmillan, pp. 97–106.
- Kuerbis, B., Badiei, F., Grindal, K. and Mueller, M. (2022). Understanding Transnational Cyber Attribution: Moving from 'Whodunit' to Who Did it. In: M. Dunn Cavelty and A. Wenger (eds). *Cyber Security: Socio-Technological Uncertainty and Political Fragmentation*. London: Routledge, pp. 220–238.
- Lindsay, J. R. (2017). Restrained by Design: The Political Economy of Cybersecurity. *Digital Policy, Regulation and Governance*, 19: 493–514.
- Lindsay, J. R. (2022). Quantum Computer and Classical Politics: The Ambiguity of Cryptologic Advantage. In: M. Dunn Cavelty and A. Wenger (eds). *Cyber Security: Socio-Technological Uncertainty and Political Fragmentation*. London: Routledge, pp. 80–94.
- Lupovici, A. (2022). Uncertainty and the Study of Cyber Deterrence: The Case of Israel's Limited Reliance on Cyber Deterrence. In: M. Dunn Cavelty and A. Wenger (eds). *Cyber Security: Socio-Technological Uncertainty and Political Fragmentation*. London: Routledge, pp. 128–140.
- Matthewman, S. (2011). *Technology and Social Theory*. Basingstoke: Palgrave Macmillan.
- Rittel, H. W. and Webber, M. M. (1973). Dilemmas in a General Theory of Planning. *Policy Sciences*, 4(2): 155–169.
- Schünemann, W. (2022). A Threat to Democracies? An Overview of Approaches to Measuring the Effects of Disinformation. In: M. Dunn Cavelty and A. Wenger (eds). *Cyber Security: Socio-Technological Uncertainty and Political Fragmentation*. London: Routledge, pp. 32–47.

- Steed, D. (2022). Disrupting the Second Oldest Profession: The Impact of Cyber on Intelligence. In: M. Dunn Cavelty and A. Wenger (eds). *Cyber Security: Socio-Technological Uncertainty and Political Fragmentation*. London: Routledge, pp. 205–219.
- Steiger, S. (2022). Cyber Securities and Cyber Security Politics: Understanding Different Logics of German Cyber Security Policies. In: M. Dunn Cavelty and A. Wenger (eds). *Cyber Security: Socio-Technological Uncertainty and Political Fragmentation*. London: Routledge, pp. 141–156.
- Sword-Daniels V., Eriksen, C., Hudson-Doyle, E. E., Alaniz, R., Adler, C., Schenk, T., Vallance, S. (2018). Embodied Uncertainty: Living with Complexity and Natural Hazards. *Journal of Risk Research*, 21(3): 290–307.
- Von Solms, R. and Van Niekerk, J. (2013). From Information Security to Cyber Security. *Computers & Security*, 38: 97–102.
- Wenger, A. and Dunn Cavelty, M. (2022). Conclusion: The Ambiguity of Cyber Security Politics in the Context of Multi-dimensional Uncertainty. In: M. Dunn Cavelty and A. Wenger (eds). *Cyber Security: Socio-Technological Uncertainty and Political Fragmentation*. London: Routledge, pp. 239–266.
- Whyte, C. (2020). Cyber Conflict or Democracy “Hacked”? How Cyber Operations Enhance Information Warfare. *Journal of Cybersecurity*, 6(1): tyaa013. <https://doi.org/10.1093/cybsec/tyaa013>

Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>