Stockholm Studies in
International Relations 2023:1

Stockholm University

Making Sense of Large-scale Cyber Incidents

International Cybersecurity Beyond Threat-based Security Perspectives

Sarah Backman

Doctoral Thesis in International Relations at Stockholm University, Sweden 2023

Making Sense of Large-scale Cyber Incidents

International Cybersecurity Beyond Threat-based Security Perspectives

Sarah Backman

Academic dissertation for the Degree of Doctor of Philosophy in International Relations at Stockholm University to be publicly defended on Friday 2 June 2023 at 13.00 in hörsal 11, hus F, Universitetsvägen 10 F.

Abstract

Large-scale cyber incidents have figured prominently in securitizing speech acts over the last decade. This thesis demonstrates how conceptualizations of cybersecurity as a public security problem connects to and shapes cybersecurity governance in national and international settings. It explores how theoretical lenses drawn from the securitization, riskification, crisis and socio-technical systems literatures can improve our understanding of the phenomena of large-scale cyber incidents, and how such incidents are interpreted by key actors. The thesis includes four articles comprising case studies which utilize in-depth interviews, text analysis and discourse analysis. The findings reveal a steady development towards an increasingly threat-based security logic in both national and international cyber policy settings. The case studies also highlight the volatile nature of malware proliferation, the tendency of collateral damage from directed cyberattacks, the transboundary characteristics of large-scale cyber incidents, and the central role of civil contingencies actors and the private sector in cybersecurity governance. The implications of these findings are discussed in relation to the increasing securitization and militarization of cyberspace. Overall, this thesis contributes to our understanding of how cybersecurity is constructed as a security problem in theory and practice, and it employs analytical approaches which facilitate the exploration of international cybersecurity along more than just traditional 'hard' security lines.

Keywords: *International cybersecurity, large-scale cyber incidents, securitization, cybersecurity governance.*

Stockholm 2023
http://urn.kb.se/resolve?urn=urn:nbn:se:su:diva-215733

ISBN 978-91-8014-262-5
ISBN 978-91-8014-263-2
ISSN 2003-1343

Department of Economic History and International Relations

Stockholm University, 106 91 Stockholm

MAKING SENSE OF LARGE-SCALE CYBER INCIDENTS

Sarah Backman

Stockholm
University

Making Sense of Large-scale Cyber Incidents

International Cybersecurity Beyond Threat-based Security Perspectives

Sarah Backman

ISBN print 978-91-8014-262-5
ISBN PDF 978-91-8014-263-2
ISSN 2003-1343

Printed in Sweden by Universitetsservice US-AB, Stockholm 2023

Dedicated to the
memory of my Dad,
Hans Backman

Acknowledgements

Writing a PhD thesis is an intellectual journey. Mine has been influenced by many people whom I have had the privilege to meet and learn from throughout the duration of this project. Although I cannot mention everyone here, I'm sincerely grateful for all of you who, in various ways, have helped me along the way and generously offered your knowledge, advice and encouragement. There are some whom I want to acknowledge especially.

First of all, I want to thank my main supervisor, Mark Rhinard, who has consistently been there to guide me through the hurdles of this journey, and always with good humor, wisdom and friendliness. Mark, thank you for encouraging me to push beyond my limitations and strive for constant improvement. Your knowledge, advice and support have been vital for this thesis project and for my development as a scholar. Likewise, this thesis would not have been possible without the support of Roger Holfeldt and Secana. Not only has Roger been an invaluable source of knowledge and advice in my efforts to understand and navigate the complex realms of cyber(security) over the course of the last decade, but he also gave me the opportunity to be an industrially employed PhD student and thus pursue this project. I'm also grateful for the support from my second supervisor, Arjen Boin, who has provided valuable comments and suggestions throughout the process of writing the thesis, and who introduced me to works and literature that have had a great impact on my thinking and research. Thanks also to Jan Hallenberg and Magnus Ekengren at the Swedish Defence University, who encouraged me to pursue a PhD in the first place.

The Department of Economic History and International Relations has provided a warm, welcoming and supportive research environment for my time as a PhD student. I would like to thank Lisa Dellmuth, Thomas Jonter, Karl Gustavsson, Mark Rhinard and Magnus Petersson for their excellent leadership. Thanks to the administrative staff at Ekohist: Jennifer Lundgren, Kelly Biddle, Ibrahim Mohamad & Johannes Hartvigsson for efficient support whenever needed. Thank you also to the brilliant and friendly PhD students I had the privilege to work with over the years, including Steffi Winkler-van Maarseveen, Kajsa Hammargård, Louise Bengtsson, Jonathan Stiglund, Ece Kural, Vitaly Fedchenko, Nina Krickel-Choi, Nick Olczak, Anna Hammarstedt, Akinbode Fasakin, Klara Melin, Zigne Edström, Yeonju Jung, Axel Nordenstam, Li Andersson, Jorge Ernesto Rodriguez Morales, Tanushree Rao and Suanne Mistel Segovia Tzompa.

I would also like to thank the skilled discussants who provided constructive feedback and insightful comments on my manuscript at the different stages of its development: Reidar Staupe-Delgado, George Christou and Karl Gustafsson.

In 2019, I had the opportunity to do a visiting studentship at Cambridge University with the Department of Politics and International Studies. Thanks to Geoffrey Edwards for excellent supervision during my time there, and to Pembroke College for hosting me. My time in Cambridge was both inspiring and uplifting.

I am deeply grateful to the interviewees of this project. Thank you for taking time from your busy schedules to contribute to my research, and generously sharing your experiences, knowledge, and insights with me.

Thanks also to Erik Ryd, Johan Turell, Richard Widh, Ammi Alverås, Robert Jonsson, Robert Malmgren, Per Fjellgren, Markus Dansarie, Daniel Vikström and Alan Sewell for our discussions and debates on cyber(security) issues, which have always been (and continues to be) both fun and fruitful.

My friends outside of work has kept my energy and spirits up during the process of writing, not least by creating spaces of acceptance, adventure, and creativity outside the realms of academic achievement. I'm grateful to have you in my life.

Finally, I want to thank the ones closest to me. I’ve been lucky to grow up in a household where reading and debating was encouraged. My Dad always made sure that my sisters and I had books, and he was always interested in what we had to say. His unwavering love and belief in me have carried me through this project, even (maybe especially) after his passing. To my Mom: thank you for being my constant rock, for always supporting my dreams and making me believe that things were possible. It has made all the difference. To my sisters, Anna and Elin: you are the best siblings one could wish for. You make me a better person. Lastly, I want to thank my partner, Matt. Thank you for your steadfast love and support, and for always being happy to discuss and explore ideas with me. It’s a privilege to have you as a partner.

Swedish Summary

Storskaliga cyberincidenter har varit framträdande i säkerhetiserande talakter under det senaste decenniet. Denna avhandling visar hur konceptualiseringar av cybersäkerhet formar governance kring cybersäkerhetsområdet i nationella och internationella kontexter. Den utforskar hur teoretiska perspektiv från litteraturerna kring säkerhetisering, riskifiering, kris och socio-tekniska system kan användas för att öka förståelsen för fenomenet storskaliga cyberincidenter och hur dessa tolkas av centrala aktörer. Avhandlingen inkluderar fyra artiklar vilka involverar fallstudier och baseras på djupintervjuer, textanalys och diskursanalys. Resultaten visar en stadig utveckling mot en alltmer hotbaserad säkerhetslogik i både nationella och internationella cyberpolicy-kontexter. Fallstudierna belyser också svårigheten i att kontrollera malware-spridning samt oväntade följdeffekter från riktade cyberattacker, storskaliga cyberincidenters gränsöverskridande karaktärsdrag och den centrala roll civila aktörer och den privata sektorn har i cybersäkerhets-governance. Implikationer av dessa resultat diskuteras i relation till den pågående säkerhetiseringen och militariseringen av cyberspace. Övergripande bidrar avhandlingen till förståelsen kring hur cybersäkerhet konstrueras som ett säkerhetsproblem i teori och praktik, och tillämpar analytiska approacher som bidrar till utforskandet av internationell cybersäkerhet bortom traditionella säkerhetsperspektiv.

Contents

1. Introduction and research questions

In 2023, it has been 27 years since John Perry Barlow's famous "A Declaration of the Independence of Cyberspace" reflected the utopian, anarchic vision of the internet shared by many of its founders and pioneers (Barlow 1996). Although this view still echoes in some internet governance structures and communities, modern cyberspace is vastly different from what it once was. In 30 years, the internet has grown from a small, experimental research project to become an indispensable and fundamental underpinning of societies globally and a pillar of the global economy. This development has been accompanied by increasing state control and governance ambitions (Ellis & Mohan 2019). Over time, cyberspace has become subject to international competition and contestation, power projection, cooperation and conflict (Jarmon & Yannakogeorgos 2018, Van Puyvelde & Brantly 2019).

In parallel with this evolution, recent decades have seen the establishment of cybersecurity as a sub-field of international security studies. Structured by a predominance of strategic studies and traditional security perspectives, the field has developed a rich literature largely focused on threat-based approaches (i.e. military security, antagonists, intent of threat actors and the material dispositions of threats) and on transferring classical security concepts such as war, power, escalation, coercion and deterrence to cyberspace (see, for example, Arquilla & Ronfeldt 1993, Halpin et al. 2006, Libicki 2009, Nye 2010, Kello 2013 and Kello 2017).

More recently, a non-traditionalist and constructivist strand of international cybersecurity studies has emerged, within which this thesis is positioned. A central contribution of this literature has been to demonstrate how cyber is increasingly being constructed and treated as a "hard" security issue through processes of securitization and militarization, which has meant shifting cybersecurity from a regular political issue to a matter of national security. In this way, exceptional measures outside of "normal" politics are legitimized, and the issue is moved closer to the realms of military and intelligence agencies (Hansen & Nissenbaum 2009, Dunn Cavelty 2012, Christou 2019, Claessen 2020, Dunn Cavelty & Wenger 2020, Dwyer et al 2022).

Indeed, the past decade has seen cybersecurity become a national security priority for most modern states. The North Atlantic Treaty Organization

(NATO) has identified cyberspace as the fifth domain of warfare, alongside sea, air, land and space. More than 40 states have now publicly established a cyber command (Smeets 2022:1) and democratic states show an increased willingness to launch offensive capabilities in cyberspace – human, technical and virtual tools to destroy, disrupt and/or exploit the computer networks of an adversary (Burton & Christou 2021:1727).

From the perspective of non-traditionalist security scholars,[1] the narrowness of the classical security agenda in international cybersecurity research is considered analytically, politically and normatively problematic. However, while the non-traditionalist literature has been successful at identifying securitization processes, it has thus far not been as successful at broadening the cybersecurity research agenda beyond the threat-based focus of traditionalist approaches. As a result, the field of international cybersecurity studies has continued to focus on threats rather than risks, antagonists rather than sociotechnical system-based problems in cyberspace, and cyberwar(fare) rather than cyber crises (Burton & Lain 2020). Through this emphasis, it has itself been part of the securitization of cyberspace (Burton & Christou 2021).

This thesis addresses this problem by offering perspectives that support the widening and deepening of our understanding of international cybersecurity beyond threat-based approaches. This is achieved through a dual but interconnected focus. One aspect is focused on exploring how varying non-threat based theoretical lenses drawn from the risk, crisis and socio-technical systems literatures can improve our understanding of the phenomenon of large-scale cyber incidents[2]: events which have been used extensively to legitimize cyber securitization (Dunn Cavelty & Wenger 2020). The other explores how actors in national and international forums understand and conceptualize cyber as a public security problem and how these ideational approaches shape cybersecurity governance.

More specifically, the two central research questions of this thesis are:

- How can large-scale cyber incidents be understood beyond threat-based perspectives?
- How does the conceptualization of cyber as a public security problem shape how it is governed?

[1] The term ”Non-traditionalist” here refers to security scholars and literature on the constructivist – critical security studies spectrum.

[2] The term “Large scale cyber incidents” is defined in this thesis as cyber(attack) induced disruptions of key societal functions or critical infrastructure operations, which are considered serious, or “high-profile”, enough to generate broad responses beyond limited technical incident management. The definition is inclusive in terms of attack type and threat actor.

This research endeavour has importance and relevance for several reasons. One is that the international cybersecurity landscape is now in a process of fast change, on which we still have little empirical knowledge. While cyberspace is technically made up of code and hardware, it is also essentially socially constructed. This means that its ideational properties are constantly being negotiated and redefined, with consequences for its governance both nationally and internationally. In recent decades, cyberspace has been subject to intense international framing competition, as different actors compete to shape its conceptualization and governance (Radu et al. 2014, Deibert 2016). While this development has attracted an increased amount of attention from security scholars, we still know relatively little about how shifting definitions, understandings, ideas and framings of cyber as a security problem in public policy informs and connects with central cybersecurity governance developments, and what challenges arise as a result. This thesis provides theoretical and empirical findings to give us a better idea of how ideational aspects connects to governance in the cybersecurity issue area, supporting our ability to make sense of current and future developments in the cybersecurity approaches of states and international organizations.

Second, while large-scale cyber incidents (defined as cyber induced disruptions of key societal functions or critical infrastructure) are phenomena surrounded by fear and hype (Valeriano & Maness 2015, Lawson 2013), empirical studies of such events have been relatively scarce, especially in the field of security studies. Moreover, when these events are discussed in the literature, they are often approached from strategic-military perspectives, for example, as the potential consequence of "cyber war". This is puzzling, given that cyberwar (which is not the same as the use of digital means or the internet *in* war) is rare (Valeriano & Maness 2015), while large-scale cyber incidents have become relatively common in the past decade. We still have little empirical knowledge of the dynamics of large-scale cyber incidents from non-antagonist focused perspectives, or how they are perceived, managed and responded to in national and international settings. There have also been few attempts to theorize such events. This thesis contributes to both research ventures. Both are important not only for the empirical understanding required to make sense of these events and their consequences in the international cybersecurity landscape, but also to examine the empirical basis for some of the assumptions made regarding large-scale incidents upon which the cyber sector has been securitized (Burton & Lain 2020).

A central argument of this thesis is that the threat-based perspectives that currently structure and dominate both academic cybersecurity studies and public policy involve security imaginaries – or "collectively held meaning structures that enable the interpretation of social reality in specific realms"

(Gjesvik & Szulecki 2022:2) – that lead to assumptions concerning the international cybersecurity landscape and large-scale cyber incidents – assumptions that need to be deconstructed and empirically investigated.

This kappa/cloak-chapter provides an overall framing of the thesis project, through discussions on theory, methods, results and findings. This introductory section pinpoints the gaps in the research and the aims of the thesis. Section 2 outlines the content and contributions of the individual articles. Section 3 takes a closer look at the state of the art when it comes to international cybersecurity studies and where the project fits into current central debates. Section 4 discusses the theoretical approach of the thesis as a whole and the theoretical frameworks used in the individual articles. Section 5 details the methodology and materials used in the project, and is followed by a discussion on ethics and reflexivity in section 6. Section 7 expands on the main findings and results of the thesis. Finally, section 8 offers some concluding remarks and identifies future avenues of research.

The four contributing articles included in the thesis are as follows:

I. Backman, S. (2022). Risk- vs. threat-based cybersecurity: the case of the EU. *European Security.* 32:1, 85-10. https://doi.org/10.1080/09662839.2022.2069464

II. Backman, S., Rhinard, M. (2018). The European Union's capacities for managing crises. *Journal of Contingencies and Crisis Management.* 26: 261–271. https://doi.org/10.1111/1468-5973.12190

III. Backman, S. (2020). Conceptualizing cyber crises. *Journal of Contingencies and Crisis Management.* 29: 429– 438. https://doi.org/10.1111/1468-5973.12347

IV. Backman, S. (2023). Normal cyber accidents. Under review with *Journal of Cyber Policy.*

2. Research articles and individual contributions

Article I, Risk- vs. Threat-based Cybersecurity: The case of the EU
Cybersecurity is a concept that is currently being defined, shaped and redefined as a public policy problem in various contexts and arenas, with implications for its governance. Despite an increasing scholarly interest in studying the European Union (EU) as a cybersecurity actor, relatively few studies have so far focused on exploring this ongoing process in the context of the EU. Furthermore, while previous research has indicated that ambitious EU cybersecurity initiatives have been accompanied by governance challenges and member state contestation, the specifics of this contestation have so far been underexplored. By distinguishing between risk and threat-based logics in the development of the EU cybersecurity discourse over time, this study highlights a shift towards an increasingly threat-based security logic (securitization) in the EU cybersecurity approach over time. Based on in-depth interviews and analyses of key negotiation documents, the study identifies specific areas of member state contestation accompanying this shift. Contestation was particularly pronounced in areas such as information sharing obligations and increased supranational involvement in key cyber crisis management tasks. The article concludes with a discussion of the findings in relation to the development of the EU as a security actor in the wider international cybersecurity landscape.

Article II, The European Union's capacities for managing crises
Article 2 reveals patterns of institutionalization of crisis management/civil contingencies capacities across different parts of the EU political system. The article maps the institutionalization of cyber crisis management capacities at the EU-level in parallel with other transboundary sectors and finds similar patterns across the sectors. These include increasing entrepreneurship and consolidation of new EU-level crisis management initiatives over time, especially for detecting incidents and analysing/sharing information in relation to transboundary crises. The article highlights the connection between cybersecurity and civil contingencies governance at the EU level between 2010-2017.

Article III, Conceptualizing cyber crises

Article 3 investigates how large-scale cyber incidents are interpreted and governed in national administration settings. Through the comparative analysis of two cases of large-scale cyber incidents, in Estonia in 2007 and the United Kingdom in 2017, the study investigates whether the time gap and the difference in cyberattack type between the cases (untargeted ransomware vs. targeted distributed denial-of-service, DDoS) correlate with variations in governance and response features in the national settings of the cases. The analysis identifies some variation between the cases in terms of incident features but finds that both cases were responded to as transboundary incidents with technical aspects. This was also reflected in the actors and frameworks central to the response efforts (civilian technical incident response teams/Computer Emergency Response Teams (CERTs) and generic crisis management structures).

Article IV, Normal cyber accidents

Narratives warning of a scenario in which cyber operations/directed cyberattacks induce deliberate catastrophic disruptions of critical infrastructure have figured prominently in public discourses on cybersecurity for the past 20 years. The empirical reality, however, shows that several of the most serious large-scale cyber incidents affecting critical infrastructure to date have been the result of collateral damage rather than directed cyberattacks. This article suggests that this tendency is associated with the existence of normal accident (NA) dynamics (a combination of interactive complexity and tight coupling) found in the multiple layers of socio-technical systems that underpin critical infrastructure operations. Since the existence of NA dynamics in a system makes it exceedingly difficult to analyse the potential net-effects of disrupting certain components in that system, the article argues that the ability to contain the effects of an offensive cyber operation targeting a NA system should be questioned. This has implications in the context of the “offensive cyber” turn among democratic states.

3. State of the art: international cybersecurity studies

In the past decade, cybersecurity research in security studies and international relations has grown in parallel with the increasing importance of the internet globally, resulting in an emerging field of international cybersecurity studies. While the contours of this field can be distinguished, it is notoriously fragmented (Green 2015) and policy-oriented (Dunn Cavelty 2015, Stevens 2018), which is reflected in the abundant number of contributions in cyber-/technology-specific journals compared to the few theoretically rigorous contributions focused on cybersecurity in high-ranking security studies or IR journals thus far. The complex and interdisciplinary nature of cyberspace, as a multi-layered physical, logical and technical infrastructure that is also to a large degree socially constructed, has contributed to the conceptual diffusion and confusion among practitioners and scholars alike (Shires 2019, Green 2015). Consequently, members of different communities often talk across each other with limited mutual understanding (Van Puyvelde & Brantly 2019). Despite this disparity, a few central questions can be said to have structured the field and the debates therein. Two of the most influential are: What is the source of (in)security in cyber space?; and How, if at all, can the traditional concepts and theories of security studies be translated or transferred to describe what is happening in cyberspace?

From a theoretical perspective, traditionalist security scholars have focused on how classical security concepts such as coercion, deterrence (see, for example Libicki 2009) and power (see, for example, Nye 2010) apply to cyberspace. The threat-form that has triggered the biggest body of literature within the traditionalist camp is cyberwar and cyberwarfare, a subject that, since the publication of “Cyberwar is Coming!” (Arquilla & Ronfeldt 1993), has been the theme of a great number of academic and non-academic publications. In fact, cyberwar, information warfare (IW) and netwar are terms that have been widely used by military observers since the 1990s (Halpin et al. 2006). With the advent of the explicit use of offensive cyber capabilities (OCC) and operations (OCOs) by democratic states, authors from traditionalist security perspectives have increasingly focused on how offensive cyber can be used, under what conditions and to what ends (Halpin et al. 2006, Lin 2010, Smeets &

Lin 2018). Authors from traditionalist security perspectives commonly agree that OCC and OCOs can be useful for states, but disagree on how and under what conditions. It is often stressed that the development of OCC and the ability to conduct OCOs are necessary for deterrence and posture purposes in the face of the growing cyberthreats from states such as China, Russia, Iran and North Korea, which are continually developing and launching offensive cyberoperations to achieve various strategic and operational objectives. When it comes to conducting OCOs, some argue that it does not raise any moral concerns due to the precision of these operations (Jenkins 2016), while others recognize that collateral damage and a mismatch between intent and the actual damage caused by cyberattacks has been a common pattern of offensive cyber operations historically (Smeets & Lin 2018:104–105).

Traditionalist understandings of security in the international cyber landscape have been increasingly contested and contrasted in the past decade. Key ideas of the traditionalist perspective, such as the translatability of the classical deterrence concept to cyberspace and the “offence as defence” approach have been extensively criticized as ill-suited to contemporary cybersecurity challenges and leading to a more militarized cyberspace (Burton & Lain 2020:450), and the concept of cyberwar has been criticized as vague and overexpanded to the point of being analytically useless (Moore 2022).

A major point of dispute within international cybersecurity studies has concerned the prospects of cyberwar having catastrophic consequences. Scholars from the constructivist and critical strands of international cybersecurity studies have highlighted how narratives of an impending catastrophic event do not reflect the empirical reality of cyber conflict thus far, which instead tends to fall under the umbrella of intelligence activities or limited, minor operations more akin to sabotage than bombing (Burton & Christou 2021:1732).

Recognizing the importance of language, including metaphor, analogy and narrative, in how problems are framed and responded to, constructivist and critical cybersecurity scholars have been specifically interested in studying the public narratives and discourses around cybersecurity. Among the key findings of this research endeavour is the tendency to use military terms and battlefield analogies to describe events in cyberspace. The term “cyberattack” has been used to describe anything from online protests to criminal fraud, and the spreading of rumours to sabotage (Singer & Friedman 2013:68). At the same time, the term has regularly been connected in leader speech acts to hypothetical catastrophic scenarios of cyberwar, including analogies such as “Cyber 9/11” or “Cyber Pearl Harbor”.

This combination of using military labels for just about anything that happens in cyberspace and rhetoric that invokes images of impending “cyber doom" (as a result of cyberwarfare) has been a persistent element of cybersecurity discourse, especially in the United States (Lawson 2019). The label "cyberwar" has been placed on events which, if they happened in the physical space, would not be labelled as such; for instance, the Sony hack in 2014 (Moore 2022). From the perspective of the Copenhagen school of securitization, these are examples of "speech acts", or narratives aimed at constructing cyberattacks as an existential threat to the referent object (the state/its citizens), which aims to legitimize extraordinary measures and means to manage them beyond "normal politics" and normal public insight. From this viewpoint, "cyber doom" narratives are strategic narratives, or rhetorical devices used to package and frame a security issue for strategic benefit.

The securitization of cyberspace and its consequences have perhaps been the most prominent subject of study in the constructivist strand of cybersecurity studies. Since Hansen & Nissenbaum's influential article "Digital Disaster, Cyber Security and the Copenhagen School" (2009), a relatively large number of studies and dissertations on cybersecurity have used frameworks derived from securitization theory (Buzan, Wæver, and De Wilde 1998) to establish how different actors in cyberspace have tried to move cybersecurity from a regular political issue to a matter of national security.

Hansen & Nissenbaum outline three forms of securitization connected to the cyber issue area. The first, *hypersecuritization*, refers to the tendency for speech acts concerning cyber to invoke images of future catastrophic events in the absence of any incident of that magnitude, reflecting a reliance on the future to legitimize current exceptional measures (Hansen & Nissenbaum 2009:1164). The second, *everyday security practices*, highlights the way in which securitizing actors refer to the security or safety of the individual citizen to achieve acceptance for current exceptional measures (for instance, the individual's reliance on the functionalities of critical infrastructures). The third, *technification*, refers to the privileged position of technical experts and the reliance on expert discourse in cybersecurity. While assuming a politically and normatively neutral "technical" agenda, technical experts can act as securitizing actors in various ways that serve the interests of security communities while distinguishing themselves from the ‘‘politicking’’ of politicians and non-technical experts (Hansen & Nissenbaum 2009:1167).

Beyond focusing on how cyberspace is securitized, scholars have also focused on the practical implications of this securitization, such as the increased prominence of military and intelligence agency-led national cybersecurity centres, overclassification of threats in cyberspace (Burton & Lain 2020), and the involvement of military and intelligence agencies in cybersecurity even when police-, justice- or crime-based approaches might be more suitable (Dunn Cavelty 2015:92). Authors have also highlighted the fact that multiple communities profit from the securitization of cyberspace, not least the private cybersecurity sector, the military/industrial complex and even the academic community (Singer & Freidman 2014, Burton & Christou 2021:1731).

These debates on the securitization of cyberspace have generated an increasing, although still rather nascent, interest in cyber de-securitization. While commonly acknowledged to be a normatively desired outcome among students of cyber securitization, the nature and process of cyber de-securitization are far less explored in comparison with securitization – echoing the tendency of securitization research more broadly. Waever largely sees de-securitization as a counter process to securitization. Since securitization is about exceptional politics, de-securitization is about returning an issue to the realm of normal/unexceptional politics (Waever 1993). However, different views exist within the scholarly community on what constitutes de-securitization and how it can be achieved. While some argue that it is possible to actively de-securitize through speech acts, or that the process can at least be initiated through speech (Vuori 2010), others argue that de-securitization mainly happens through a "fading away" of the particular issue in the securitization repertoire (lack of speech) (Behnke 2006). To the extent that this thesis refers to de-securitization, it aligns with Lene Hansen's definition as "the shifting of issues out of emergency mode and into the normal bargaining processes of the public sphere", which includes a move from the securitized to the politicized. This means that the issue is still dealt with by the state and public governance, unlike non-politicized which means that the issue is taken out of public policy altogether (Hansen 2012:531).

Securitization perspectives have often been criticized for their tendency to consider security strictly within state and national security narratives. Applied to cybersecurity, this criticism is particularly relevant given the prevalence and importance of non-state actors – not least the private sector – in both internet and cybersecurity governance at all levels (Liebetrau 2019: 30). This thesis focuses primarily on states, which is indeed a limiting factor, but it does not see them as unitary actors. It assumes that different actors within the state can contribute to the securitization or de-securitization of cyberspace to varying degrees. For instance, this thesis presumes that an intelligence agency approach to national cybersecurity would be securitizing by default (institutionalized); while a civil contingency approach to national cybersecurity focused on societal resilience to cyberattacks (and other causes of digitally induced disruptions) is not necessarily de-securitizing, nor is it necessarily securitizing the issue. A civil contingency approach might also contribute to a de-securitizing approach in the sense of supporting a move towards a condition in which the issue of national cybersecurity is not dominantly associated with exceptionality, antagonist-centrism, and secrecy, but rather predominantly a regular governance issue subject to "normal" public insight.

Despite increasing contestation, traditionalist and threat-based understandings of the international cybersecurity landscape still holds a predominant position in international cybersecurity studies and informs cybersecurity policy at both national and international levels (Burton & Christou 2021, Burton & Lain 2020). Through the study of the construction of cyber as a public security problem and the phenomena of large-scale cyber incidents through varying non-threat based theoretical perspectives, this thesis aims to contribute to the expansion of perspectives on international cybersecurity beyond traditional “hard” security lines, and to empirically examine some of the assumptions upon which cyber has been securitized. While the thesis does not include a detailed agenda for cyber de-securitization, it aligns with the scholarly ambition to avoid a further reproduction of securitizing notions, assumptions and focus areas while studying international and national cybersecurity.

4. Theoretical considerations and frameworks

This thesis positions itself in the field of International Relations and, more specifically, its sub-field of Security Studies. It rests broadly within the constructivist research orientation of security studies and pursues four individual research studies which, taken together, broaden and deepen our understanding of international cybersecurity beyond threat-based approaches. The aim of this section is not to outline an overarching theoretical framework for the thesis as a whole. Rather, it sets out to provide clarity on the perspectives and analytical assumptions that underpin the theoretical frameworks and literatures used in the individual articles, and what they contribute in relation to the overarching aim of the thesis.

Section 4.1 expands on the overall theoretical orientation of the thesis, its constructivist understanding of security and how this is reflected in the thesis. It also discusses the theoretical journey of the thesis project and the decision to pursue an "interdisciplinary approach" in the sense of deploying a variety of theoretical frameworks and literatures to achieve the overall aim. Section 4.2 reflects on some relevant literatures that have been considered while writing the thesis, but not explicitly used in the individual articles.
Sections 4.3, 4.4 and 4.5 focus on the theoretical frameworks and literatures deployed in the individual articles: securitization and risk(ification), crisis management and sociotechnical perspectives/normal accident theory. Beyond introducing these perspectives and providing an overview of how key concepts were interpreted and implemented in the individual studies, these sections also reflect on the rationale behind their deployment and the key contributions.

4.1 Theoretical orientation and considerations

While this thesis is interdisciplinary in the sense of deploying different theoretical frameworks in its respective individual studies, the thesis overall takes a constructivist approach to the study of security. This means, among other things, that it seeks to depart from traditional understandings of security reflected in objectivist and neo-realist approaches to the study of cyber. While acknowledging the role of states in the international security environment, the constructivist approach of this thesis emphasizes that states are not unitary or fixed entities – and that the meaning and understanding of cybersecurity is constantly being intersubjectively shaped, defined and redefined by groups in both national and international forums. This is reflected in the thesis' interest in intersubjective understandings and conceptualizations, and temporal change. In positioning itself within the constructivist tradition of International Relations, this thesis adopts an understanding of national and international security that does not disregard the role of power, interests and competition, for instance, but highlights their constructed and social character (Adler 2012).

Due to their different theoretical approaches and associated literatures, the studies included in this thesis are situated in different parts of the constructivist and interpretivist spectrum. For instance, securitization-theory (article 1) is more closely related to the scholarly traditions of critical security studies, in contrast to the normal accidents theory applied in article 4, which is rooted in socio-technical theoretical perspectives. However, the constructivist understanding of security is a common theme in all four articles, each of which in its various ways sheds light on how cybersecurity and large-scale cyber incidents are interpreted and conceptualized by key actors.

The decision to deploy theoretical frameworks and insights from different strands of literature calls for a discussion on the theoretical journey of this thesis, which is reflected in the development of the individual articles. Initially, it was the observation that the phenomenon of large-scale cyber incidents affecting critical infrastructure was surprisingly unexplored in the growing literature on international cybersecurity that gave rise to my own scholarly curiosity. This was not only in the sense that there were few in-depth academic (peer reviewed) case studies exploring these events from an empirical point of view, and from a non-threat-based perspective in the sense of focusing on effects, consequences and responses rather than threats, threat-perceptions and attack-dynamics, but also that these events were under-theorized. The literature on international cybersecurity often dealt with these phenomena in terms of ideas, either (as in the strategic studies literature) as the potential source of future "cyber doom" connected to cyberwarfare, or (as reflected in the critical leaning debates) investigating the construction and consequences of these ideas produced by practitioners and academia.

There is thus a lacunae in the literature regarding the response to and governance of actual cases of large-scale cyber incidents. Recognizing that the connection between civil contingencies/crisis management and large-scale cyber incident governance and response had scarcely been investigated in the literature on international cybersecurity, this became central to the first two articles in the thesis. The value of further exploring non-threat based approaches, cybersecurity governance and large-scale cyber incidents as a way to investigate the empirical basis for key assumptions regarding cybersecurity governance and large-scale cyber incidents (in terms, for example, of sources of danger and central actors) became increasingly evident as I delved deeper into the empirics; and as the scholarly debate regarding the securitization and militarization of cyberspace developed in subsequent years. Thus, one of the articles that followed focused on adding a perspective of risk(ification) to the securitization of cyber at the EU level, acknowledging the existence of parallel cybersecurity logics, one of which is not threat-based. The final article builds on the empirical observations made in article 3 and applies a socio-technical perspective to explore the tendency for collateral damage in cyberattacks affecting critical infrastructure, placing it in the context of the militarization of cyberspace.

The overarching motivation for this pluralism in theoretical approaches – that incorporates both crisis and risk as well as socio-technical systems perspectives – has been to provide a variety of perspectives that, each in different ways, supports the widening and deepening of our understanding of international cybersecurity beyond the threat-based focus that often underpins classical security studies approaches. This aligns with the growing scholarly interest in exploring cybersecurity's many conceptual and empirical manifestations beyond the "theoretical sterility" and "hectic empiricism" which has so far characterized the field of international cybersecurity (Stevens 2018). As Van Puvelde & Brantly (2019) highlight, an interdisciplinary approach might also be especially appropriate when studying international cybersecurity, which is a particularly multi-layered and complex issue area. However, it is worth emphasizing that as a result, the papers in this thesis, although interconnected in different ways, pose their own research questions in relation to certain and to some extent different angles of the same empirical context. Thus, the articles may, at an individual level, relate more to one of the two main research questions of the thesis.

4.2 Theoretical context and related literatures

This section briefly reflects on the literatures that were considered in the process of writing the thesis, and which in various ways are related to the approaches adopted in the thesis, but have not been explicitly used in the articles. This includes the international cybersecurity and internet governance literatures, as well as the security governance literature more broadly – especially the component focused on ideational aspects.

A central assumption of this thesis is that there is a connection between understandings and conceptualizations of cyber as a public security problem and its governance, and that a lack of insight into this dynamic leaves us with an incomplete understanding of cybersecurity governance outcomes. This assumption has a close affiliation with insights from the ideational component of the governance literature, which argues that policy dynamics surrounding an issue (including subsequent contestation and cooperation) will be substantially influenced by the understandings, representations and framings of that issue (Daviter 2011, Rochefort & Cobb 1994, Campbell 2002). Students of policy framing are generally concerned with the ways framing influences how issues are processed by the political system, and how framing (and framing contests) are related to policy positions and decisions. Rein & Schön (1996) argue that frames can be seen from four compatible perspectives: as a scaffolding (an inner structure), as a boundary that sets off phenomena from their contexts, as a cognitive/appreciative schema of interpretation or as a generic diagnostic/prescriptive story (Rein & Schön 1996:88). This thesis primarily relates to the concept of frames as cognitive/appreciative schema of interpretation, or as generic diagnostic/prescriptive stories. Although the field has traditionally studied framing from the notion that definitions are important in the initial phase of policy processes or cycles, an increasing number of contributions depart from this view by arguing that definitions – or framings – are entangled in action itself (de Vreese 2012). This thesis subscribes to both approaches in its respective articles. However, the overarching starting point of the articles is one that subscribes to the idea that how we conceive and frame policy questions shapes how they are acted on (e.g. Hall 1993).

My interest in international cybersecurity governance naturally led me down the path of the wider internet governance literature as well as the more specific cybersecurity governance literature. There are considerable overlaps between the two. Contributions within the internet governance literature have tended to focus on the changed conditions for governance created by cyberspace, and the characteristics of current governance structures (Mueller 2010, Brown & Marsden 2013, Scholte 2017) and cyber norms (Iasiello 2016), as well as contributions focused on the nascent international cyber regime complex (Raymond 2016, Pawlak 2019). Arguing that internet governance tends to be characterized by "..trans-scalarity, trans-sectorality, diffusion, fluidity, overlapping mandates, ambiguous hierarchies and a post-sovereign absence of a single and consistent supreme authority" (Scholte 2017:182), scholars within this literature commonly highlight that the internet puts pressure on the traditional governance structures of the nation state in several distinct ways (Mueller 2010:4).

While contributions within the cybersecurity governance literature have been diverse, ranging from studies on network governance as applied to cybersecurity (Dunn-Cavelty & Suter 2009), to the influence of cyber-incidents on governance outcomes (Shires 2019) and the impact of context on cybersecurity governance challenges (Ellis & Mohan 2019), similar themes to the internet governance literature reoccur in this literature. In particular, the literatures both tend to focus on the ways in which the particular characteristics of cyberspace affect security governance and cooperation between key actors. These include but are not limited to the tendency for cyberspace to be simultaneously transboundary and geographically bound, and to transcend other important dichotomies for governance such as private/public, civil/military and operational/strategic. Similar scholarly interest has been extended to studying the emerging cybersecurity governance practices of the European Union, resulting in studies that, for instance, shed light on the creation of public–private transnational governance in the European internet economy (Christou & Simpson 2006:57), the characteristics of the EU as a cybersecurity actor (Carrapico & Barrinha 2017, Christou 2016, Sliwinski 2014) and the EU's role in shaping the global cyber regime complex (Christou & Simpson 2006, Pawlak 2019). Despite an emerging focus within this literature on studying the connection between problem perception/framing and governance of cybersecurity, notably Christou (2016) and Carrapico & Ferrand (2020), this has remained relatively uncharted territory, especially when it comes to crisis governance (Boeke 2017).

Moving on from a discussion of the governance literatures and insights that have been consulted in the process of designing this thesis, the following sections expand on the specific literatures and theoretical frameworks used in the individual articles. While these theoretical approaches are distinct from one another, they fit into a broader theoretical universe which shares certain common traits. They all subscribe to an understanding of security as something intersubjectively socially constructed, and they are all interested in how these processes relates to and affects governance. This is perhaps clearest in the securitization and riskification literatures. But it can also be identified broadly in the crisis management literature, as well as in the socio-technical literature's focus on the interaction between human cognition and complex technology, and the organizational settings that are put in place as a result.

4.3 Securitization and riskification: article 1

Like the framing literature discussed above, the securitization and riskification literatures are interested in the way an issue is presented or given saliency, and the policy consequences of this process. Some scholars argue that securitization should be viewed as a work of framing in the sense of "...an intersubjective practice of meaning making that triggers a particular security-oriented mindset and shapes the perception of both the nature of the problem and actions undertaken to deal with it" (Stepka 2022).

With their roots in speech act theory, both securitization and riskification theory have a discursive conception of security, meaning that the definition of security is dependent on its successful construction in discourse. Securitization as described by Buzan et al. (1998) is at its core a more extreme form of politicization. When an issue is securitized, it is presented as an existential threat to a referent object, which justifies actions outside of the ordinary or of normal political procedures (Buzan et al. 1998: 24). From this perspective, the general concept of security is drawn from its constitution within national security discourse, emphasizing the confronting – and construction – of threats and enemies, which grants the ability to adopt emergency measures and exceptional politics (Buzan & Hansen 2009: 213-214).

While the securitization perspective has been widely popular and influential within security studies, the Copenhagen School has also been criticized, particularly by approaches that advocate a more radical expansion of the concept of security. Another category of criticism has highlighted its lack of refinement in regard to different logics of security (Judge and Maltby 2017: 182), including the lack of acknowledgement of risks in relation to threats in the securitization process (Aradau et al. 2008:149).

Rather than arguing for a more deliberate and refined inclusion and acknowledgement of risk in securitization theory (see for example Trombetta 2008), I agree with Olaf Corry (2012) that risk politics (riskification) should be analysed and understood as separate from threat politics (securitization). This approach implies that risk politics involves its own dangers and advantages: "Though at times interwoven, making an issue a question of risk is not the same as securitization nor even necessarily a precursor to it" (Corry 2012: 236). From this perspective, riskification can be seen as a social process with similarities to the securitization process, but concerned with risks in both the discursive phase (speech acts) and the non-discursive phase (policy implementation and collective approval of proposed measures). A key difference here is that risk-security is essentially focused on the conditions of possibility for harm, as opposed to direct causes of harm (threat-security) (Corry 2012: 238). While the notion of riskification has also been criticized, prominently on the basis that it, like securitization, is fixated on discourse (Petersen 2012: 710), its added value arguably lies in making possible the identification of a different mentality of governing, in a process that without this perspective could be (mistakenly) labelled securitization. Thus, it maintains the integrity of the concept of securitization while allowing for a more refined understanding of the politics surrounding danger. Despite an increasing interest in looking at cybersecurity from risk perspectives, the relationship between threat- and risk-based security logics has so far been largely unexplored in the issue area of international cybersecurity. This is surprising given that international cybersecurity is an especially multi-layered and complex policy field with a tendency to transcend traditional dichotomies of governance. Article 1 helps to bridge this gap by investigating how the relative prevalence of risk- vs threat-based security logics in EU cybersecurity policy has changed over time and how this connects to governance outcomes.

4.4 Crisis management governance: articles 2 and 3

In the wake of the turn towards broadening and deepening the field of international security (Buzan & Hansen 2009:187), students of international security and governance paid increasing attention to non-threat-based security perspectives such as "all hazards", crisis and disaster management (Bossong & Hegemann 2015, Boin et al. 2017). The trend within security studies to pay increasing attention to perspectives of crisis and disaster coincided with empirical developments, in which international crises gained more political attention following high-profile events, not least in recent times, as we have experienced major crises such as Covid-19, climate change induced wildfires, and food and fuel-shortages as a result of Russia's war on Ukraine. In this context, the European Union (EU) has built up frameworks and mechanisms for responding to crises, disasters and structural risks that cross both geographical and functional boundaries.

Providing support for member states in terms of civilian crisis management has proved one of the most successful ways in which the EU can act in the realm of security. Referencing the need to confront transboundary challenges and threats through a comprehensive approach that bridges silos, the EU has continuously moved to collapse the traditional divide between internal and external security governance (Shepherd 2021, Bossong & Rhinard 2021). Traditionally, internal security challenges were seen as primarily concerning criminal activity within a state, and managed mainly through civilian law enforcement, while external security was seen concerning challenges and threats from outside the state's borders and managed by deterrence and defence, and/or repelled by military force (Shepherd 2021: 2). Bossong and Hegemann suggest that the emerging practices, policies and processes of civilian crisis and disaster management can be conceptualized within the security literature as "civil security governance", a concept which "...may help to capture the emerging protection-oriented policy space, which extends beyond the EU's CFSP and Area of Freedom, Security and Justice (AFSJ) and is not adequately covered by more traditional terms like internal security" (Bossong & Hegeman 2015:3).

This thesis subscribes to the importance of incorporating crisis and all-hazards management perspectives, which allow for non-antagonist threats and risks to be studied, into the notion of international security. Articles 2 and 3 adopt analytical frameworks drawn from the literature on transboundary crises within the wider crisis management and contingencies literature, and position these in the context of cyber crisis governance in national administration settings and the EU. What characterizes a crisis in a traditional sense is an event that threatens core values or life-sustaining systems, which requires an urgent response under conditions of deep uncertainty (Boin & Rhinard 2008; Rosenthal et al. 2001). What sets the transboundary crisis apart from a "traditional" crisis is, simply put, its tendency not to be limited by geographical, political, sectoral, economic, social or legal boundaries (Boin et al. 2014, Boin 2019, Jordana & Triviño-Salazar 2020). More specifically, a transboundary crisis can be defined as a crisis that transcends political boundaries, such as geographical borders, jurisdictions or levels of governance, functional boundaries, such as sectoral, policy and industry domains, and temporal boundaries of definitions (Ansell et al. 2010, Rose & Kustra 2013).

4.5 Sociotechnical perspectives and normal accidents theory: article 4

The sociotechnical systems/safety literature can be considered one of the cornerstones of the crisis management literature, although it has often been siloed from debates in security studies, including on cybersecurity. In article 4, I attempt to understand the proliferating tendencies of large-scale cyber incidents connected to critical infrastructure as observed in the empirics of earlier articles by applying a socio-technical perspective to developing dangers and cascading accidents. To do this, I built and expanded on the idea of normal accidents coined by Charles Perrow in 1984.

The normal accidents concept stems from a simple idea: that the combination of a complex interactive system and tight coupling between system components will inevitably lead to "accidents" in high-risk socio-technical systems, such as catastrophic failures causing disruption to operations. This condition exists because of several development steps.

The first is linked to technological progress. Modern technological invention, innovation and expansion is constantly multiplying and expanding high-risk technologies, such as industrial control systems (ICS) for critical infrastructure operations, nuclear technologies and space technology/satellites. These technologies are high-risk because we rely on their operation for our safety or daily lives, and their failure would have extensive disruptive effects or even threaten lives.

The second is linked to our need to control these rapidly developing technologies. To make them manageable, we create complex systems or inject them into complex systems. These systems could be technical or systems in an organizational sense (organizations of organizations). We build complexity into the systems by creating interactive-ness between the components of the system or between systems. The components could be made up, for example, of code, parts, procedures or operators.

The third is linked to tight coupling. When two or more failures of components happen in an interactive way, the result can be both unexpected and unpredictable – even for the designers of the system (Perrow 1999:4). This interactive complexity would not be as dangerous were it not for an additional system characteristic: tight coupling. Perrow defines tight coupling as a condition in which "..processes happen very fast and can't be turned off, the failed parts cannot be isolated from other parts, or there is no other way to keep the production going safely" (Perrow 1999:4). The result is that there is "no slack" in the system. Recovery becomes difficult and the initial disturbance can proliferate quickly and irreversibly. As the permutation and combination of interacting components increases, an error in any of those components, or combination of components, could have a catastrophic net effect on the functioning of the overall system – if adequate separation and segregation are not in place. According to Perrow, neither technological fixes nor better organization will entirely do away this dynamic, since this will only tend to increase the interactive complexity of the system. The only viable option to reduce the effects of the NA dynamic is to minimize tight coupling, for instance, by increasing redundancy and decreasing centralization.

Although increasingly popular among scholars, the seemingly deterministic argument of NA was challenged, among others, by a group of Berkeley researchers who coined the term "High Reliability Organizations" to describe organizations that, despite possessing systems that have both interactive complexity and tight coupling, still manage to keep catastrophic accidents to almost zero. The critics of NA also argued that Perrow was too focused on technology, downplaying or underestimating the role of the human, organizational and sociocultural factors involved in technological disasters (Le Coze 2021:4). Arguably, these perspectives are not mutually exclusive, and more recent academic contributions on both HRO and NA in particular commonly acknowledge their compatibility when applying a sociotechnical systems perspective to HROs (Rijpma 1997 Brown 2018, Le Coze 2015). Thus, more modern understandings and applications of NA incorporate to a greater degree an acknowledgement of the role of organizational and system design in compensating for human fallibility and technological failures.

Even though the idea of normal accidents was primarily developed in a time before the internet, I suggest that a slightly modified version of Perrow's NA approach can be applied to explore and explain cyber-induced failures in the large-scale socio-technical systems underlying the operation of critical infrastructure today. The main modification consists of a broader scope of the NA dynamic, and a greater focus on the macro-layer. Whereas Perrow originally referred to NA dynamics in relatively small and closed systems, such as the management of a nuclear facility or an aircraft, this thesis (in article 4) applies the NA perspective to regional and global dynamics such as international supply chains. One of the major takeaways is that this approach, in contrast to most of the contributions within international cybersecurity studies, theorizes large-scale cyber incidents from the perspective of the unintended-ness and unexpected-ness that stem from socio-technical system characteristics. In other words, it focuses on the systems attacked, and steers away from antagonist-centrism.

5. Methods and materials

This section outlines the methodological considerations and the methods used in the articles for the thesis. The purpose of the section is not to set out a common research design for the whole project, since each paper contains its own research design. This section instead outlines discussions on the overall methodological choices, with regard to ontology, reflexivity (reflections on my role as a researcher within the project), materials and case selection, as well as various ethical considerations.

5.1 Methodological approach

The previous section notes the social scientific orientation of this thesis as constructivist in nature. This section elaborates briefly on what this means for the thesis in terms of its central assumptions and approaches to scientific inquiry.

Constructivism is a broad strand of ontological thinking that is influenced by philosophy, social theory and sociology, by for example the works of Weber and Durkheim. Various currents of thought have developed under its umbrella, but common to all constructivist thinking is the proposition that people are social beings, and that social relations make us – but we also make social relations. In other words, structure affects agents and the other way around, simultaneously (Onuf 2013:7). Constructivists generally hold the view that international reality is constructed by building blocks that are ideational and material, and that ideational factors have both normative and instrumental dimensions (Ruggie 1998: 879). Furthermore, constructivists agree that social beings lend significance to the world through ideas and agreement that something exists, which includes a belief in the existence of (potentially) multiple, intersubjectively, constructed "truths" about social, political, cultural and other human events (Schwartz-Shea & Janow 2011). Based on the assumption that we are constantly remaking our world, constructivists often focus on understanding change (Müller 2013:622). While constructivism is not a method, it provides a set of assumptions that guides analytical focus and key methodological choices.

While there are some core features of constructivist research that reflect its view of scientific inquiry, it is worth noting that constructivism comprises a spectrum that ranges from positivist and rationalist-leaning approaches to interpretivist and radical reflectionist, critical-leaning approaches. This thesis contains articles that vary in terms of their position on this spectrum, but overall subscribe to a mainstream interpretivist constructivist approach in terms of ontology and epistemology. From this perspective, social reality is best accessed through qualitative methods focused on social constructions such as shared meanings, language and practice (Bevir & Rhodes 2015). This approach has guided the overall methodological choices of this thesis, including the decision to conduct qualitative, small N and primarily interview-based case studies with an emphasis on exploring and understanding rather than aspiring to provide causal explanations. While the thesis largely focuses on constructions and understandings of (cyber)security and large-scale cyber incidents involving key actors, it also assumes that this understanding cannot be divorced from context in terms of constructed structural conditions and considerations.

5.2 Case selection

A case study can be broadly defined as an attempt to understand and interpret a spatially and temporally bounded set of events, or as an intensive empirical inquiry investigating a specific phenomenon within its context (McNabb 2010:237). While the rationale behind case selection for the individual articles in this thesis ultimately depended on their specific respective aims and objectives, the cases were broadly selected on the basis of their "class of event" (Yin 2003, George & Bennett 2005) or, in other words, what they are "an instance of" (Levy 2008:2). The cases were furthermore selected based on their significance as instances of the respective class of event (McNabb 2010:281).

Two main classes of event, albeit in various ways interconnected and overlapping, guided the case selection for the articles: instances of international cybersecurity conceptualization and governance (articles 1 and 2), and instances of large-scale cyber incidents affecting critical infrastructure operations (articles 3 and 4). For the first two articles, focused on international cybersecurity conceptualization and governance, the EU was chosen as the object of study. The motivations for this choice were that the EU has had a relatively long history of engaging with the issue area of international cybersecurity – and the prospect of large-scale cyber incidents – and that there is data available to illustrate the development of the EU when it comes to conceptualization of cyber and governance trends over time, including contestations between member states and the EU as a supranational entity. For articles

3 and 4, the cases were selected on the basis that they fit the definition of large-scale cyber incidents as understood in this thesis (cyber induced disruptions affecting critical infrastructure operations) and because they were considered serious, or “high-profile”, enough to generate broad responses beyond limited technical incident management.

Qualitative studies with a small number of cases have several key strengths, but they are also prone to some limitations and risks, from which this thesis is not exempt. For instance, single or small-N case studies are more prone to the risk of selection bias than large-N case studies, something which is managed through conscious case selection and the selection of cases on the characteristics of the independent rather than the dependent variable (Atkinson & Delamont 2010, Halperin & Heath 2020:243). Moreover, while single and small-N case studies tend to have high internal validity due to the richness of the data and analysis focused on a single case or a few cases, the low number of cases can also affect the extent to which generalizability across the wider class of events can be claimed.

5.3 Data collection, materials and data analysis

Throughout its individual articles, this thesis has mainly employed three qualitative research methods: interviewing, textual analysis and (to a smaller extent) discourse analysis.

While the most important data source for this thesis was the interviews, a combination of data collection methods was important to provide the necessary depth and range of data to respond to the aim of the thesis. The primary and secondary documents were also essential to complement and validate the interview data in each of the studies. The primary documents (strategy documents, legal documents, official reports, decision-documents and position documents) were accessed through open source/official websites. The secondary sources mainly consisted of different kinds of reports and reviews from media and companies, such as reports on the timeline of events or consequences of a large-scale cyber incident.

5.3.1 Interviewing and fieldwork

The fieldwork undertaken for this thesis occurred before the Covid-19 pandemic of 2021–2022 and included travel to Estonia, the United Kingdom and Japan to conduct interviews with key senior practitioners in national cybersecurity organizations. During and after Covid-19, interviews were primarily performed online via Zoom. These interviews were with practitioners from the US, the UK, Sweden, Romania and Switzerland, as well as EU practitioners from the European Agency for Information Security (ENISA), and the European Cybercrime Centre (EC3). Of the 37 interviews conducted throughout the period of the thesis, 28 were in-depth interviews of between 30- and 90-minutes duration.

In addition to the formal interviews, the fieldwork included informal discussions with practitioners both within and without the set of official interviewees for this thesis. These were also an important source of information and insight concerning the overall events and surrounding factors. Interviewees were mainly selected due to their insight on or involvement in the cases in the respective articles. The goal of the interviewee selection strategy was to include both internal and external perspectives on each case, in terms of both involvement in the case of the study and geographic position. Most of the interviewees are affiliated with public organizations (such as CERTs or national/international cybersecurity agencies) while a minority are affiliated with private cybersecurity companies.

Interviews were conducted in a semi-structured manner, maintaining a set of overarching questions and themes to guide the interview while at the same time allowing the interview to be flexible, resemble a conversation and allowing the interviewees to focus and expand on themes essential to them. The interview data analysis strategy entailed three main steps: data reduction, coding and analysis (Halperin & Heath 2020, Curini & Franzese 2020). The first step entailed a process of transcribing the interview recordings into written form. The second step involved organizing the interview data according to the theory-informed themes, categories and motifs of the respective articles. The final step entailed analysis, drawing conclusions on the basis of the organized interview data and cross-checking the emerging findings.

5.3.2 Textual analysis and discourse analysis

Apart from interviewing, the qualitative analysis of the texts, primarily in the form of central documents and reports, was the most important source of data for the thesis. Most of the articles contain a combination of textual analysis and interviewing. This form of triangulation can be especially valuable when it comes to validating and substantiating findings from qualitative document analyses (Wesley 2014:146). Qualitative document analysis requires immersion in and familiarity with the texts in focus and in-depth accounts of findings. The text analysis strategy entailed several stages of study of the key documents, where the first was broader and holistic and the subsequent stage involved broad categorization or classification of data. The final stage involved in-depth analysis and potential revision of the categorization.

One article in this thesis (article 1) utilized discourse analysis, which is an interpretive form of analysis that explores the way in which speech and discourses give meaning and legitimacy to actors, institutions and practices. From this perspective, textual analysis can detect and lay out discourse, but this must also be understood in relation to its contexts. Discourse analysis has a close association with (qualitative) content analysis, which involves the systematic analysis of textual information (Halperin & Heath 2020). In article 1, a minor content analysis was carried out using the qualitative content analysis software tool NVIVO. This process entailed developing a coding table and injecting key documents into the software tool before analysing the documents for the relative frequency of select coded words while controlling for versions of the words that could affect the results (Weber 1990).

6. Ethical issues

Ethical concerns are part of the everyday practice of doing research. In the course of conducting the studies included in this thesis, several ethical implications had to be addressed. Guillemin & Gillam (2004) suggest that there are at least two major dimensions of ethics in qualitative research: (a) procedural ethics, involving formal procedures and applications for conducting research involving humans; and (b) "ethics in practice" (Guillemin & Gillam 2004:263). This section discusses both dimensions in relation to my research and fieldwork.

6.1 Procedural ethics

Procedural ethics relate to the more technical considerations of a study, such as informed consent and data protection (Kapiszewski et al 2015:226). In line with standard ethical guidelines, I informed all the interviewees about the study's aims, the questionnaire, their role in the study, why they had been asked to participate, plans for subsequent publication and data protection. This information was also sent to the interviewees in writing in the standard form provided by Stockholm University for participants in research projects. All the interviewees were asked for full consent and permission to record the interview. Due to the often-sensitive nature of the interviewees' identities, all have been anonymized. After conducting the interviews, the interviewees were informed that they could have a copy of the recorded interview if they wished, and that they would have an opportunity to read their quotes before publication.

6.2 Ethics is practise

Ethics in practice relates to the relationship between the researcher and the people interviewed, including pre-established norms and ideas that might affect the study outcome. Although a contested concept, the people I interviewed for this thesis can generally be described as "elites" in the sense that they have close proximity to power (senior positions within their organizations) and/or a particular expertise on the subject of interest. Most of my interviewees hold positions in high-level public institutional structures for managing cybersecurity, such as EU agencies, National Cybersecurity Centres or national CERTs. Rice (2010) identifies that interviewing elites presents researchers with a number of practical challenges associated with the question of power. One main challenge is gaining access to interviewees in the first place. This was indeed perhaps the most difficult stage of the interviewing process for this thesis. Interview opportunities were given almost exclusively as a result of my personal connections in the cybersecurity field. I had to be careful not to bring my involvement in the field as a consultant into the interview situation, in terms of both interaction and the interview questions. However, my practical experience in the field has also given me a solid basis of understanding, which was naturally helpful when conducting the interviews. Another issue that I had to consider was the potentially influential factor of the organizational affiliations of the interviewees (Rice 2010:74). I approached the risk that this aspect might skew the results by trying to find several interviewees from different organizations and countries, to gain external perspectives on the phenomenon/case of interest.

6.3 Reflexivity

Reflexivity concerns reflections on my own roles as a researcher in and observer of the field, and the limitations these impose. One such reflection included the notion of the west/euro-centrism of my studies and perspectives, something still exceedingly common even in critical-leaning perspectives on international cybersecurity (Dwyer 2022). Another concerned my position as a scholar working in the field of international cybersecurity. As Coles-Kemp (2022) argues, cybersecurity scholars must acknowledge and be aware of how we are served by the hype around cybersecurity and the power that comes with working within a hyped field, including socio-economic resources and influence. Indeed, as highlighted by Burton & Christou (2021), cybersecurity scholars are among those who have benefited from the securitization of cyberspace. Moreover, the particular power that cybersecurity as an academic pursuit typically accrues comes from its links with industry and government and its usefulness to those entities (Coles-Kemp 2022).

As cybersecurity scholars, it is important that we confront our own roles in this power dynamic. For myself, this has been especially important considering that my career originated in the cybersecurity industrial complex as a consultant primarily involved in government civil cybersecurity projects. Such reflections have included notions on my privilege given my background in a field which is, in practice, closely connected to intelligence-agency culture and secrecy. Without my social and professional networks, which stem from my involvement in the field as a practitioner, I would probably have had difficulty getting access to the interviewees who were the most important source of data for this thesis. I have had access to national cybersecurity conferences and other spaces that provide limited access to those from outside this community. My aim throughout the process of writing the thesis has been to acknowledge the ways in which my background in the field might have influenced my views on the objects and subjects of study, and to strive for transparency, awareness and critical reflection in relation to my background as well as my current position as a researcher.

7. Main findings and contributions

This section will expand and reflect on the main findings and contributions of the thesis.

In general, the findings reveal a disparity between the catastrophic scenarios depicted in speech acts used to secure cyberspace and the current empirical reality of cyber incidents affecting critical infrastructure. We have not yet witnessed a "Cyber 9/11" or a significant disaster caused by cyberwarfare. This suggests that the securitization of cyberspace continues to rely heavily on the fear of potential future events to legitimize current securitization and associated exceptional measures.

For article 1, I developed an analytical framework based on the work of Corry (2012) on threat- vs risk-based security logics, adapted to cybersecurity (see table 7.1). While not mutually exclusive, the separation of security logics allows us to differentiate processes of securitization from processes of riskification. Article 1 showed that, since 2013, the EU has evolved its cybersecurity approach primarily from a risk-based conceptualization to an increasingly threat-based approach - more focused on antagonist threats and the need to defend against, or deter, “threat actors” in cyberspace. The data indicates a similar shift at the EU member state level.

Table 7.1. Analytical framework, risk- vs threat-based cybersecurity, article 1

Analytical categories of cybersecurity discourse in public policy	Threat-based cybersecurity logic	Risk-based cybersecurity logic
Problem emphasis	• Focused on identifiable and acute cyber threats • Focused on agency, capability and intent of antagonists	• Focused on long term or future risks and impacts to societies stemming from cyberspace

	• Focused on the need to defend against or deter external “threatening others” in cyberspace	• Not focused on specific “threatening actors” or antagonists in cyberspace • Focused on digital dependency and system vulnerabilities
Related response/ policy prescriptions	• Active response to defend against or deter acute cyber threats stemming from antagonists • Management of cyber threats leaning towards exceptional politics or militarization	• Long-term societal engineering to reduce system vulnerabilities • Management and governance of causes of harm in cyberspace without going into the realm of emergency, or exceptionality

A more threat-based cybersecurity logic in EU-policy contexts entails increased ambitions for pan-European cybersecurity cooperation to “defend and deter” against cyber threat actors and a more pronounced role for the EU in cybersecurity and large-scale cyber incident management. Nevertheless, a more threat-based cybersecurity logic at the member state level (securitization) is accompanied by an increase in the influence of traditional security actors and a greater sense of secrecy in operational cybersecurity matters. A parallel transition to a more threat-based approach to cybersecurity at both the supranational and state levels may not necessarily improve international cybersecurity cooperation. Rather, as indicated by the data, this development is not only associated with increased supranational cybersecurity ambitions, but also resistance from member states when it comes to mandatory pan-European information sharing, and even, to some extent, to voluntary information sharing initiatives.

The focus of Articles 2, 3, and 4 was on large-scale cyber incidents affecting critical infrastructure and the governance structures established to manage them in national and international contexts. The studies found that, in practice, these incidents are typically governed and responded to as multi-layered transboundary incidents, rather than security events in a traditional or military sense - even when there is the suspected involvement of a state-sponsored actor. Large-scale cyber incident response tends to feature actors such as Computer Emergency Response Teams (CERTs), organizations from the affected critical infrastructure sector, digital service providers and private cybersecurity firms/contractors, as well as generic (primarily national, but sometimes also international) crisis management structures and actors. While traditional security actors such as military or intelligence agencies can play a role, such as providing threat intelligence and/or supporting attribution efforts, this role tends to be supportive, rather than a leading one. Generic transboundary crisis management capacities, such as monitoring, sectoral situation awareness, capacity to quickly deploy expert teams (cyber incident response), clear bureaucratic coordination procedures, pre-established public/private relationships and platforms, formal scaling procedures for generic national crisis management efforts and public communication/meaning making, were regularly emphasized in the data as key capabilities.

The argument for the need to securitize in response to the prospect of large-scale cyber incidents disrupting critical infrastructure is thus essentially connected to assumptions about the effectiveness of intelligence and military actors at monitoring for and preventing these events – primarily through threat intelligence and/or deterrence (for instance, preventing threat actors from launching attacks against critical infrastructure due to fear of retaliation). The ability to transfer the deterrence concept neatly to cyberspace is contested in the literature, as discussed in earlier sections. Even if we consider that deterrence may be effective at preventing intentional disruptions of critical infrastructure by threat actors, it may not be as effective at preventing unintentional disruption due to collateral damage from directed attacks, or proliferating malware. Moreover, this approach comes with a flipside, since the increased influence of intelligence practices that comes with securitization and militarization of an issue, will tend to decrease the prospects for enhanced trust and information sharing between key stakeholders, including between private and public sector actors.

Several of the most serious large-scale cyber incidents affecting critical infrastructure to date have been the result of collateral damage/unintended consequences, and/or broadly proliferating malware, rather than directed offensive cyber operations. In article 4, I built on sociotechnical systems theory to develop an analytical framework (see table 7.2) for understanding how initial disturbances in system components of critical infrastructure may cascade in unexpected ways, and with unexpected consequences. I argue that the existence of Normal Accidents dynamics (the combination of interactive complexity and tight coupling), in multiple layers of critical infrastructure operations, makes it exceedingly difficult to foresee, or estimate, how disruptions or alterations of individual components in a system, or several systems, might interact and cause incidents.

Table 7.2 Analytical framework for NA-dynamics in critical infrastructure operations, article 4

Layers of critical infrastructure operations	Examples of normal accident dynamics in systems of critical infrastructure operations	Interactive complexity	Tight coupling
Macro	• Supply chain interdependencies	Complex global ecology of supply chain actors (including vendors) and inter-organizational dependencies	Dependency on delivery of supplies/services to keep system running/inability to operate without supply/service delivery
Organization	• Centralization of services in combination with interdependencies of interactive components in the organization • Lack of distinction between critical and non-critical system components	Integration between organizational components and functions Lack of comprehensive understanding of the system (subsystems and their interfaces)	Lack of organizational slack/structural flexibility, or redundancy
Technology	• Legacy code • Legacy hardware • Legacy systems	Layered legacy code and combinations of old and new hardware	Dependence on legacy code layers, and legacy hardware, to keep systems operational

The proliferating tendencies of malware in combination with NA-dynamics in critical infrastructure systems have implications for at least two threat-based assumptions regarding the international cybersecurity landscape. The first concerns the idea of the centrality of actor intent. The findings of this thesis suggest that the proliferation pathways, seriousness of impact, and political interpretation of malware deployment, tend to be both more volatile, and unpredictable, than is sometimes suggested. Thus, the intent of threat actors may not have a clear link to the proliferation, impact, and political consequences of cyberattacks or cyber operations.

The second concerns the "offensive turn" in the cyber policies of democratic states, or the increasingly legitimized idea of the use of offensive cyber tools and operations as a way to assert power, deter foes and project strategic influence in cyberspace. These practices assume the ability to correctly assess the impact and consequences of the use of offensive tools and methods. According to NA-theory, it may be almost impossible to consistently do this when a system with NA-characteristics is affected, because of the possible ways in which failures in individual components of that system could interact and cause unexpected consequences. Moreover, the difficulty of assessing how an offensive action will be interpreted by the opponent will add to the challenge of analyzing outcomes. The same offensive action may be interpreted differently by different states, due to varying conceptual and legal interpretations of cyberattacks, and different thresholds for counterattacks. NA-dynamics may also be "hidden" in systems, meaning that systems with these characteristics could be targeted, or affected by mistake. If offensive cyber operations become a more common feature of the international cyber landscape, we are, therefore, likely to see an increase in collateral damage incidents/unintended consequences from cyberattacks, worldwide.

The empirical reality of cyber incidents affecting critical infrastructure so far suggests that the likelihood of catastrophic critical infrastructure disruptions due to cyberwarfare has probably been exaggerated. What is likely to have been understated, in academia and in practice, is the danger posed by a more militarized and securitized cyberspace globally. Increasing use of offensive tools and methods in cyberspace by both democratic and non-democratic states is likely to contribute to malware proliferation, increased stockpiling of vulnerabilities by states, and more instances of unintended effects and collateral damage from offensive cyber operations. In combination with a further destabilized international cybersecurity landscape involving increased fear and suspicion between states in cyberspace, and weak international cybersecurity norms, this will result in a more dangerous, and less secure, future cyberspace, in which the risk of escalatory scenarios increases.

8. Concluding remarks and further research

In the context of a swiftly changing international cybersecurity landscape, this thesis has sought to provide theoretical and empirical findings to give us a better idea of how conceptualizations of cybersecurity as a public security problem shape how it is governed, and to achieve an improved understanding of the phenomenon of large-scale cyber incidents. Through the application of various non-threat based theoretical lenses, it has addressed and questioned some of the assumptions that result from a predominantly threat-based cybersecurity focus in public policy and academia. Moreover, the thesis has employed analytical approaches which facilitate the exploration of international cybersecurity along more than just traditional 'hard' security lines.

The next decade will be critical for the future of cyberspace. There are still several possible trajectories of development in terms of international cooperation on cybersecurity and governance of the dangers that stem from cyberspace. The idea that suspicion, secrecy, and conflict might constitute the foundation for future cyber interactions at the inter-state level is troubling. Nonetheless, this future becomes increasingly plausible as the continuation of securitization and militarization of cyberspace globally leads to path-dependencies that will further structure, and consolidate, triggered security dilemmas and cyber arms races. Attempts to de-securitize cyberspace and focus the conditions for cyber peace, rather than cyber conflict (Burton & Christou 2021), will be key to preventing this outcome.

However, the potential pathways of cyber de-securitization are still extensively underexplored in the literature. This will continue to be an important aim of future research within international cybersecurity studies, along with attempts to employ theoretical perspectives beyond narrow traditional security approaches. Another potential subject for further exploration is the connection between institutional arrangements, (cyber)security understandings (meaning-making), and governance outcomes. While many of the most powerful states in the cyber realm have organized their national cybersecurity agencies under the umbrella of intelligence/defense agencies, some have located their National Cybersecurity Centres, or equivalent, within other institutional arrangements. These variations provide opportunities for comparative case studies.

Finally, the continued focus on identifying and investigating central representations (and the imaginaries they draw on) of dangers in the international cyber landscape (not least large-scale cyber incidents) will continue to be an important task for students of international cybersecurity. This will not only further the academic debates surrounding the securitization of cyberspace, but also have practical implications, by shedding light on the implicit assumptions that underpin key decisions, and cyber policy choices, in both national and international contexts.

References

Adler, E (2012). “Constructivism in International Relations”. In Carlsnaes.(ed.) Handbook of International Relations: Sources, Contributions and Debates. London: Sage.

Ansell, C., Boin, A., & Keller, A. (2010). Managing transboundary crises: Identifying the building blocks of an effective response system. *Journal of Contingencies and Crisis Management*, 18(4), 195–207. https://doi.org/10.1111/j.1468-5973.2010.00620.x.

Aradau, C., Lobo-Guerrero, L., & Van Munster Rens, R. (2008). Security, technologies of risk, and the political: Guest editors’ introduction. *Security Dialogue* 39(2–3), 147–154. https://doi.org/10.1177/0967010608089159.

Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is coming! *Comparative Strategy*, 12(2), 141–165.

Atkinson, P., & Delamont, S. (2010). *SAGE Qualitative Research Methods*. SAGE Publications, Inc., https://dx.doi.org/10.4135/9780857028211.

Barlow, J. (1996). A Declaration of the Independence of Cyberspace. Electronic Frontier Foundation. URL: https://www.eff.org/cyberspace-independence (accessed 2022-01-01).

Bevir, M., & Rhodes, R.A.W. (eds) (2015). *Routledge Handbook of Interpretive Political Science*. New York: Routledge.

Behnke, A. (2006). No way out: desecuritization, emancipation and the eternal return of the political — a reply to Aradau. J Int Relat Dev 9, 62–69.

Bijl-Brouwer, M. van der. (2019). Problem framing expertise in public and social innovation. The Journal of Design, Economics, and Innovation, 5(1), 29–43.

Boeke, S. (2018). National cyber crisis management: Different European approaches. *Governance*, 31(3), 449-464.

Boin, A. (2019). The transboundary crisis: Why we are unprepared and the road ahead. *Journal of Contingencies and Crisis Management*. 27, 94– 99. https://doi.org/10.1111/1468-5973.12241.

Boin, A., & Rhinard, M. (2008). Managing Transboundary Crises: What Role for the European Union?. International Studies Review. 10. 1 - 26. 10.1111/j.1468-2486.2008.00745.x.

Boin, A., Hart, P.T., Stern, E.K., & Sundelius, B., (2017). *The Politics of Crisis Management: Public Leadership Under Pressure* (Second edn), New York: Cambridge University Press.

Boin, A., Rhinard, M., & Ekengren, M. (2014). Managing transboundary crises: The emergence of European Union capacity. *Journal of Contingencies and Crisis Management*, 22(3), 131–142. https://doi.org/10.1111/1468-5973.12052.

Bossong, R. & Hegemann, H. (eds) (2015). *European Civil Security Governance Diversity and Cooperation in Crisis and Disaster Management.* Basingstoke: Palgrave Macmillan. [Electronic resource].

Bossong, R. & Rhinard, M. (2021). The internal and external security nexus in Europe. in Haar, R.N. (red.) (2021). The making of European security policy: between institutional dynamics and global challenges. Abingdon, Oxon: Routledge

Brown (2018). *Keeping the Lights On: A Comparison of Normal Accidents and High Reliability Organizations*. IEEE Technology and Society Magazine.

Brown, I., & Marsden, C. T. (2013). Regulating code: Good governance and better regulation in the information age. MIT Press.

Burton, J., & Christou, G. (2021). Bridging the gap between cyberwar and cyberpeace. *International Affairs*, 97(6), 1727–1747. https://doi.org/10.1093/ia/iiab172.

Burton, J., & Lain, C. (2020). Desecuritising cybersecurity: towards a societal approach. *Journal of Cyber Policy*, 5(3), 449–470. https://doi.org/10.1080/23738871.2020.1856903.

Buzan, B., & Hansen, L. (2009). The evolution of international security studies. Cambridge University Press.

Buzan, B., Wæver, O., & Wilde, J. D. (1998). *Security: A New Framework for Analysis*. Boulder, Colorado: Lynne Rienner.

Carrapico, H., and Barrinha, A. (2017) The EU as a Coherent (Cyber)Security Actor*?. JCMS: Journal of Common Market Studies,* 55: 1254– 1272. doi: 10.1111/jcms.12575.

Carrapico, H., & Farrand, B. (2020) Discursive continuity and change in the time of Covid-19: the case of EU cybersecurity policy*, Journal of European Integration,* 42:8.

Campbell, J. (2002). Ideas, politics and public policy. *Annual Review of Sociology*. 28, 21–38.

Christou, G. (2019). The collective securitisation of cyberspace in the European Union. *West European Politics*, 42(2), 278–301. https://doi.org/10.1080/01402382.2018.1510195.

Christou, G. & Simpson, S. (2006). The Internet and Public-Private Governance in the European Union. *Journal of Public Policy*, 26(1), 43-61.

Christou, G. (2016). Cyber security in the European Union: resilience and adaptability in governance policy. Houndmills, Basingstoke Hampshire: Palgrave Macmillan.

Claessen, E. (2020). Reshaping the internet: The impact of the securitisation of internet infrastructure on approaches to internet governance, the case of Russia and the EU. *Journal of Cyber Policy*, 5(1), 140–157. https://doi.org/10.1080/23738871.2020.1728356.

Corry, O. (2012). Securitisation and "riskification": Second-order security and the politics of climate change. *Millennium: Journal of International Studies*, 40(2), 235–258. https://doi.org/10.1177/0305829811419444.

Curini, L. & Franzese, R. (2020). *The SAGE Handbook of Research Methods in Political Science and International Relations* [Electronic resource].

Daviter, F. (2011). *Policy Framing in the European Union*. Basingstoke: Palgrave Macmillan.

de Vreese, C. H. (2012). New avenues for framing research. *American Behavioral Scientist*, 56(3), 365–375. https://doi.org/10.1177/0002764211426331.

Deibert, R. (2016). Cyber-security. In Dunn Cavelty, M., & Balzacq, T. (ed.) *Routledge Handbook of Security Studies*. (Second edn.) Abingdon, Oxon.: Routledge.

Dunn Cavelty, M (2012). The militarisation of cyberspace: Why less may be better. In *Proceedings of the 4th International Conference on Cyber Conflict*. Brussels: NATO.

Dunn Cavelty, M. (2015). Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. *Science and Engineering Ethics*, 20(3), 701–715. https://doi.org/10.1007/s11948-014-9551-y.

Dunn Cavelty, M., & Wenger, A. (2020). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*, 41(1), 5–32. https://doi.org/10.1080/13523260.2019.1678855.

Dunn-Cavelty, M. & Suter, M. (2009). Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection. *International Journal of Critical Infrastructure Protection,* 2:4, pp. 179-187.

Dwyer, A. C., Stevens, C., Muller, L. P., Cavelty, M. D., Coles-Kemp, L., & Thornton, P. (2022). What can a critical cybersecurity do? *International Political Sociology*, 16(3). https://doi.org/10.1093/ips/olac013.

Ellis, R., & Mohan, V. (ed.). (2019). *Rewired: Cybersecurity Governance. The Past, Present, and Future of Cybersecurity*. Wiley.

George, Alexander L., & Andrew Bennett (2005). *Case Studies and Theory Development in Social Sciences*. Cambridge, Mass.: MIT Press.

Gjesvik & Szulecki (2022). Interpreting cyber-energy-security events: Experts, social imaginaries, and policy discourses around the 2016 Ukraine blackout, *European Security*, doi:10.1080/09662839.2022.2082838.

Green, J.A. (ed.) (2015). *Cyber Warfare: A Multidisciplinary Analysis* (1st edn). Routledge.

Guillemin, M., & Gillam, L. (2004). Ethics, reflexivity, and “Ethically important moments” in research. *Qualitative Inquiry*, 10(2), 261–280. https://doi.org/10.1177/1077800403262360.

Halperin, S., & Heath, O. (2020). *Political Research: Methods and Practical Skills* (Second edn) Oxford: Oxford University Press.

Halpin, E., Trevorrow, P., Webb, D., & Wright, S. (2006). *Cyberwar, Netwar and the Revolution in Military Affairs*. (Basingstoke, Hants, UK: Palgrave MacMillan.

Hansen, L. (2012). Reconstructing de-securitization: The normative-political in the Copenhagen School and directions for how to apply it. *Review of International Studies* 38(3), 525–546.

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, Cyber security, and the Copenhagen school. *International Studies Quarterly*, 53(4), 1155–1175. http://www.jstor.org/stable/27735139.

Hall, P. A. (1993). Policy Paradigms, Social Learning, and the State: The Case of Economic Policymaking in Britain. Comparative Politics, 25(3), 275–296. https://doi.org/10.2307/422246

Iasiello, E. (2016). What Happens If Cyber Norms Are Agreed To?. *Georgetown Journal of international affairs*, 30-37.

Jarmon, J., & Yannakogeorgos, P. (2018). *The Cyber Threat and Globalization: The Impact on US National and International Security*. Rowman Littlefield.

Jenkins, R. (2016). *Cyberwarfare as Ideal War* ,in Allhoff, Henschke, and Strawser (eds): Binary Bullets: The Ethics of Cyberwarfare, New York.

Jordana, J., & Triviño-Salazar, J. C. (2020). EU agencies' involvement in transboundary crisis response: Supporting efforts or leading coordination? *Public Administration*, 98(2), 515–529. https://doi.org/10.1111/padm.12652.

Judge, A., & Maltby, T. (2017). European Energy Union? Caught between securitisation and 'riskification.' *European Journal of International Security*, 2(2), 179–202. https://doi.org/10.1017/eis.2017.3.

Kapiszewski, D., MacLean, L.M., & Read, B.L. (2015). *Field Research in Political Science: Practices and Principles*. Cambridge: Cambridge University Press.

Kello, L. (2013). The meaning of the cyber revolution: Perils to theory and statecraft. *International Security*, 38(2), 7–40. https://doi.org/10.1162/ISEC_a_00138.

Kello, L. (2017). *The Virtual Weapon and International Order*. Yale 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(1).

Lawson, S. T. (2021). *Cybersecurity Discourse in the United States: Cyber-Doom Rhetoric and Beyond*. Routledge.

Le Coze, J-C (2015). 1984–2014. Normal accidents:. Was Charles Perrow right for the wrong reasons?. *Journal of Contingencies and Crisis Management*, 23(4).

Le Coze, J. (2021). Post normal accident. [Elektronisk resurs] : revisiting Perrow's classic. (1st Edition). Boca Raton: CRC Press.

Levy, J. S. (2008). Case studies: Types, designs, and logics of inference. *Conflict Management and Peace Science*, 25(1), 1–18. https://doi.org/10.1080/07388940701860318.

Libicki, M.C. (2009) *Cyberdeterrence and Cyberwar*. Santa Monica. https://www.rand.org/pubs/monographs/MG877.html. Also available in print form.

Lin, H. S. (2010). Offensive Cyber Operations and the Use of Force *Journal of National Security Law & Policy* 4(1). https://heinonline.org/HOL/License.

Moore, D. (2022). Offensive cyber operations: understanding intangible warfare. London: Hurst & Company.

McNabb, D.E. (2010). Research Methods for Political Science: Quantitative and Qualitative Methods (2nd ed.). Routledge. https://doi.org/10.4324/9781315701141

Müller (2013) Security Cooperation in Handbook of international relations in (ed) Carlsnaes, Risse & Simmons

Mueller, M. (2010). Networks and States: The Global Politics of Internet Governance. Cambridge, Massachusetts; London, England:

Nye, J. S. (2010). Cyber power. http://belfercenter.org.

Onuf, N.G. (2013). Making sense, making worlds: constructivism in social theory and international relations. London: Routledge

Pawlak, P. (2019) The EU’s Role in Shaping the Cyber Regime Complex. *European Foreign Affairs Review*, 24: 2, pp. 167-186,

Perrow, C. (1984). Normal accidents: living with high-risk technologies. New York: Basic Books.

Perrow, C. (1999). Normal accidents: living with high-risk technologies. ([Rev. ed.]). Princeton, NJ: Princeton University Press.

Petersen, K. L. (2012). Risk analysis: A field within security studies? *European Journal of International Relations*, 18(4), 693–717. https://doi.org/10.1177/1354066111409770.

Raymond, M. (2016). Engaging security and intelligence practitioners in the emerging cyber regime complex. *The Cyber Defense Review, 1*(2)*,* 81-94.

Radu, R., Chenou, J.-M., & Weber, R. H. (2014). *The Evolution of Global Internet Governance: Principles and Policies in the Making*. Springer.

Rein, M. & Schön, D. (1996). Frame-critical policy analysis and frame-reflective policy practice. *Knowledge and Policy*, 9, 85–104.

Rice, G. (2010). Reflections on interviewing elites. *Area*, 42(1), 70–75.

Rijpma, J.A. (1997). Complexity, tight-coupling and reliability: Connecting normal accidents theory and high reliability theory. *Journal of Contingencies and Crisis Management*, 5, 15–23. https://doi.org/10.1111/1468-5973.00033.

Rochefort, D. A., & Cobb, R. W. (eds) (1994). *The Politics of Problem Definition: Shaping the Policy Agenda*. Lawrence, Kan.: University Press of Kansas.

Rose, A., & Kustra, T. (2013). Economic considerations in designing emergency management institutions and policies for transboundary disasters. *Public Management Review*, 15, 10.

Rosenthal, U., Boin, R.A., & Comfort, L. K. (eds) (2001). *Managing Crises: Threats, Dilemmas, Opportunities*. Springfield, Ill.: Charles C Thomas.

Ruggie, J. (1998). What Makes the World Hang Together? Neo-Utilitarianism and the Social Constructivist Challenge. International Organization, 52(4), 855-885.

Schwartz-Shea, P., & Yanow, D. (2011). *Interpretive Research Design: Concepts and Processes* (1st edn). Routledge. https://doi.org/10.4324/9780203854907.

Scholte, J. (2017). Polycentrism and Democracy in Internet Governance. In The Net and the Nation State: Multidisciplinary Perspectives on Internet Governance (ed. Kohl, U), 165-184, Cambridge, Cambridge University Press

Shepherd, A. J. (2021.). *The EU Security Continuum; Blurring Internal and External Security*. Routledge.

Shires, J. (2019). Cybersecurity Governance in the GCC, in Ellis, R. & Mohan, V. (eds). *Rewired: Cybersecurity Governance*. Wiley.

Singer, P. W & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York: Oxford University Press.

Smeets, M.W.E. (2022). No shortcuts: why states struggle to develop a military cyber-force. New York, NY: Oxford University Press.

Smeets, M., & Lin, H. S. (2018). Offensive cyber capabilities: To what ends? *International Conference on Cyber Conflict (CYCON)*, Tallin, 29 May to 1 June, 55–71. https://doi.org/10.23919/CYCON.2018.8405010.

Stepka, M. (2022). Identifying Security Logics in the EU Policy Discourse. Springer International Publishing.

Stevens, T. (2018). Global cybersecurity: New directions in theory and methods. *Politics and Governance* 6(2), 1–4). https://doi.org/10.17645/pag.v6i2.1569.

Sliwinski, K. (2014) Moving beyond the European Union's Weakness as a Cyber-Security Agent, *Contemporary Security Policy*, 35:3, 468-486

Trombetta, M. (2008). Environmental security and climate change: analysing the discourse, *Cambridge Review of International Affairs,* 21:4, 585-602, DOI: 10.1080/09557570802452920

Valeriano, B. & Maness, R.C. (2015). *Cyber War Versus Cyber Realities: Cyber Conflict in The International System*. New York: Oxford University Press.

Van Puyvelde, D., & Brantly, A. F. (2019). *Cybersecurity: Politics, Governance and Conflict in Cyberspace*. Cambridge, UK: Polity Press.

Vuori, J. A. (2010). Religion bites: Falungong, securitization/desecuritization in the People’s Republic of China. In Securitization Theory (pp. 200-225). Routledge.

Wæver, O. (1993). Securitization and desecuritization. Copenhagen: Centre for Peace and Conflict Research.

Weber, R .P. (1990). Basic content analysis [electronic resource]. (2nd edn) Newbury Park, SAGE.

Wesley, J (2014). The qualitative analysis of political documents. In Kaal, B., Maks, I., & van Elfrinkhof, A. (eds)., *From Text to Political Positions: Text Analysis Across Disciplines*. John Benjamins Publishing Co.

Yin, R. K. (2003). *Case Study Research: Design and Methods* (3rd edn) Thousand Oaks: Sage Publications.