Cyber securitization or cyberization of conflict?

– On the militarization of Cyber Security in Estonia

Marleen van Ooijen

4257944

Utrecht University

03-08-2020

A Thesis submitted to the Board of Examiners in partial fulfillment of the requirements of the degree of Master of Arts in Conflict Studies & Human Rights

Image Source: Abhilasha Dewan, retrieved from:

https://www.cigionline.org/articles/doing-battle-cyberspace-how-attack-estonia-changed-rules-game

Preamble

Submission date: 03-08-2029

Supervisor: Lieneke de Visser

Program Trajectory: Research and Thesis Writing (15 ECTS)

Word Count: 15.943 (Excluding references)

Keywords: Estonia, Securitization theory, Derrida, Post-Structuralism, Discourse Analysis, Cyber Security, Cyber Warfare.

Abstract

In 2007, Estonia became one of the first countries to face severe cyber-attacks, which it represented as being Web War I. This discourse of cyberwar has been contested by scholars and professionals: in reality the event was nothing close to a war and therefore there also did not have to be military retaliation from NATO. By studying the event using Copenhagen School Securitization theory, it seems like it constitutes a failed or partially successful securitizing move i.e. an attempt at assigning an issue the identity of existential threat in order to legitimize extraordinary measures. This thesis, arguing from a post-structuralist position, views securitization as a gradual, long term process in constituted out of both discursive (speech act) and non-discursive -practices (extraordinary measures). The central question that the thesis seeks to answer is: *How has a securitizing discourse on cyber threats legitimized the militarization of cyberspace in Estonia after the country experienced cyber-attacks in 2007?* By making use of discourse analysis, this thesis argues that the discourse of cyberwar – or the militarization of cyber security – was shaped through its repetition over a longer time that make the immaterial/ virtual visible. The military securitizing practices reinforced and disseminated the idea of the cyber-threat and cyberwar narrative, but were also only possible because they were legitimized through this securitizing narrative. Simultaneously, these practices imbued the securitizing narrative with the material and thereby stabilized the discourse. Instead of treating securitization according to a sequential causality, it is a co-constitutive process in which the ideational and material interact and complement each other.

Table of contents

Acknowledgements

In turbulent times like the year 2020, in which we experienced a global pandemic, writing a MA thesis can be a though journey. I started this process in Latvia for my internship at NATO StratCom COE, which I had to abruptly leave due to closing borders through living at my birth-home and finally moving into a new house. Such a time can be stressful, and I had to learn how to adapt and adjust myself to work under changing circumstances. The process as such has taught me a great deal about myself, about always persisting and finding fresh motivation to keep on working. In writing the thesis, I developed my analytical research skills and learned a great deal about cyber security and conflict.

I would not have been able to achieve all this without the great support I received, be it physical or virtual at times. First of all, I would like to thank my supervisor Drs. Lieneke de Visser for the great advice and support both in terms of my research but also for support during my internship. She helped me by fueling my enthusiasm while also reminding me to stay focused. I would further like to thank the full CCS staff for the lessons I learned during their courses, and specifically Dr. Chris van der Borgh for the support regarding the repatriation process. Thirdly, I would like to thank my classmates Naomi Thielman and Esther Meyer that I could always count on this year, as well as all the classmates that I spend hours in the library with and made the research process much more fun. I would also specifically like to thank my friend Emma Prins, resident of Estonia, who inspired me to look into this topic and ensured me that I remained close to empirical realities in the country. I would further like to thank NATO StratCom COE, and the colleagues I met there (be it for a short time) for granting me access to their organization and world. This helped me to develop literacy and comprehension to the field of military cyber- and information security. Finally, I would like to thank my family, roommates and friends for their unconditional support and patience.

Abbreviations

NATO: North Atlantic Treaty Organization

NATO CCDCOE: NATO Cooperative Cyber Defense Center of Excellence.

NATO StratCom COE: NATO Strategic Communications Center of Excellence.

CoS: Copenhagen School (of Security Studies)

PARIS School: Political Anthropological Research for International Sociology.

EU: European Union

DDoS: Distributed Denial of Service

Chapter 1: Introduction

Did you feel like that yourself? [like you were at the frontline of the information war?] – Yes, I think so.[1]

What will the future of warfare look like? This question does not only belong to science fiction, but has been a topic of both scholarly- and public enquiry. One of the most abstract new types of warfare is 'cyber warfare'. Strategic military thinkers have speculated how new digital technologies would affect warfare and power relations. In such a 'cyberwar', physical weapons and borders would be replaced- or complemented by digital weapons that reach deep into societies and critical infrastructures. Yet, empirical scholars have argued that there have been no examples of cyber-attacks with a level of lethality and damage to fit the classical definitions of 'war'.[2] Still, people talk about cyberwar as something that already exists, something that countries should prepare for and something that is invisible or even secretive but nevertheless experienced and felt.

The quote at the start of this chapter illustrates a broader trend in how 'cyberwar' is discussed.[3] In this discussion, popular concepts used are 'information war', i.e. practices like sending fake information and propaganda, or 'cyber war', referring to practices like hacking or temporarily disabling digital services.[4] Mundane activities, previously considered a technical issue for computer experts, are talked about in terms of military practice, national security and conflict. This new interpretation given to the security of digital technologies is often studied by looking at the case of Estonia.[5] In 2007, the country experienced cyber-attacks that it later branded to be 'Web War I'. Stating this to be the first digital state-to-state attack, the Estonian government attributed the attacks to its neighbor, Russia. This narrative of 'Web War I' was widely taken over by the international press and fueled academic and policy discussions as well as a fear of cyber threats. Ever since, cyberwar as a new, realistic danger increasingly became a policy object on the agenda of (inter)national cyber security.[6]

The process by which an issue comes to be recognized as a threat to the survival of a 'referent object', in this case the Estonian state, is analyzed using the theoretical framework of Securitization

---

[1] Translated from Dutch: Director (Mea Dols de Jong): *'(Floor Boon) zei: het voelde alsof ik aan het front van de informatieoorlog ben.'* […] Moderator (Bart Krull): *'Voelde je dat zelf ook toen je daar was? Dat gevoel dat je daarnet beschrijft, van Floor Boon?'.* Director: *'(korte stilte) ja, dat denk ik wel.'* Discussion during 'Tegenlicht Meetup: Aan het front van de informatieoorlog', de Zwijger, Amsterdam 20-5-2020. Retrieved from: https://dezwijger.nl/programma/aan-het-front-van-de-informatieoorlog

[2] Columba Peoples & Nick Vaughan-Williams (2014) *Critical security studies: An introduction*. Routledge, 207; Jan-Frederik Kremer & Benedikt Müller (Eds.). (2013). *Cyberspace and international relations: Theory, prospects and challenges*. Springer Science & Business Media.

[3] On Tuesday the 9th of March 2020, Dutch documentary makers filmed at a NATO conference on social media. The theme and title of this documentary was: 'The future of warfare', and covered the battle against disinformation and 'trolls' in the Baltic States. The documentary followed different 'combatants', from NATO troops to 'fake news-debunkers' in civil society. The Director argued that she became fascinated with the idea of how to visualize an 'invisible war'.

[4] For example: Nick Dyer-Witheford and Svitlana Maviyenkoier (2019) *Cyberwar and revolution: Digital subterfuge in Global Capitalism*. University of Minnesota Pres: 4; Huib Modderkolk (2019) *Het is oorlog maar niemand die het ziet.* Podium B.V. uitgeverij; Peter Pomerantsev (2019) *This is not Propaganda: Adventures in the War against Reality.* PublicAffairs; John Arquilla & David Ronfeldt (1993). Cyberwar is coming!. *Comparative Strategy*, *12*(2), 141-165. Floor Boon (2019) 'In Litouwen is de Oorlog van de toekomst al begonnen'. *NRC*, 29 oct.

[5] Lene Hansen & Helen Nissenbaum (2009). 'Digital disaster, cyber security, and the Copenhagen School'. *International studies quarterly*, *53*(4); Robert Kaiser (2015) 'The birth of cyberwar'. *Political Geography*, *46;* Matthew Crandall & Collin Allan (2015) 'Small States and Big Ideas: Estonia's Battle for Cybersecurity Norms', *Contemporary Security Policy*, 36:2, 346-368.

[6] Kaiser, 'The birth of cyberwar', 18.

Theory. Hansen & Nissenbaum (2009) have applied this theory to the Estonian case to illustrate how there have been 'securitizing moves' to cyberspace.[7] They concluded that this process of 'cyber-securitization' is a distinct new type of dynamic or discourse, but has only been partially 'successful' in the case of Estonia.[8] International audiences did not accept the 'war' narrative fully, and therefore not all extraordinary measures were implemented. Moreover, Hansen and Nissenbaum predicted that the narrative of cyberwar would soon fade as it would not have enough impact to become the dominant interpretation. However, from a long-time-perspective, conceptions of (inter)national security have changed in the international- and domestic arena. A 2017-survey amongst Estonians found that cyber threats are still perceived as the largest security issue to the country.[9] Furthermore, cyber security has become a prominent part of policies- and practices of national security. It therefore feels unsatisfactory to conclude that 'securitization' has not been successful considering ideas of cyber security and security have changed over time.

This thesis analyses the Estonian case, using an updated version of securitization theory. It thereby aims to develop theory and by implication provide a more holistic image of the case itself. This thesis seeks to answer the following question: *How has a securitizing discourse on cyber threats legitimized the militarization of cyberspace in Estonia after the country experienced cyber-attacks in 2007?*

This thesis does not reject the approach and conclusions made by Hansen & Nissenbaum and other scholars, but seeks to advance both its theoretical- and empirical insights. The success of securitization should not be placed external to the speech act. Instead of looking at securitization as a static moment, it is viewed as a *process* in which a discourse of existential threat legitimizes changing material practices. Empirically, this means that it is not only the attacks and its representation that are the focus, but also the practices of cyber security that follow. The main argument is that the cyber-attacks, discursively represented as cyberwar, became a sign that is citable in future securitizing moves. This legitimized the increasing military involvement in cyber security, but also influenced conceptions of national security in the country. Through repetition, in the form of material practices, the discourse of cyberwar stabilized.[10]

Using a poststructuralist, discourse analytical method, securitization theory is amended to be able to include the possibility of gradual change in meaning attached to cyber security and to military practice. In this framework, both signifying *narratives* are considered to be part of this process as well as the material *practices* – i.e. extraordinary policy measures. In this process, not only the identity (meaning) of cyber security (threat) is formed, but also the identity of the referent object (the Estonian state) and the securitizing actors and audiences (cyber security experts or policy members). It is not only a case of the securitization of cyberspace, but also a cyberization of national (military) security.[11] The first chapter lays out the framework of poststructuralist securitization theory, referred to as 'performative securitization'. It will argue that the original theory is too static, as it is focused on a single moment and on external and fixed criteria for success. The new framework views securitization as a gradual and intersubjective process, as an accumulation of texts (including practices) that identify something as an existential threat.[12] This thesis thereby seeks to highlight the discursive struggle by which military cyber security practices are legitimized. Secondly, the thesis will provide a brief outline of the methodology

[7] Hansen & Nissenbaum, 'Digital disaster'.
[8] Ibid, 1171-1172.
[9] VIljar Veebel and Illimar Ploom, (2016). 'Estonian perceptions of security: not only about Russia and the refugees'. *Journal on Baltic Security, 2*(2), 55.
[10] Kaiser, 'The birth of cyberwar', 14.
[11] Tim Stevens (2016). *Cyber security and the politics of time*. Cambridge University Press, 29.
[12] Julie Wilhelmsen, (2016). *Russia's securitization of Chechnya: how war became acceptable*. Taylor & Francis, 24.

used and a chapter providing background information on Estonia and the attacks. Thirdly, the analytical chapters will show how broader discourses on cyber security and Estonian identity have been shaped prior to 2007, which serves as a structuring device for the analysis of securitizing moves made after the attacks. Understanding securitization as both a process of exceptionality and of quick change, the first analytical chapter focuses on the attacks as a triggering event. The last chapter looks at the gradual change to practices of security in the country. Finally, this thesis will argue cyber security and cyberwar have become stabilized as a security policy objective.[13] The attacks as a security imaginary have shaped identities of the security field, Estonia as a cybersecurity expert and norm setter and cyberspace as an existential threat.

[13] Kaiser, 'The Birth of Cyber War', 18.

Chapter 2: Securitization theory, post-Copenhagen School

This thesis makes use of Securitization Theory, developed by the Copenhagen School (CoS) of security studies. This theory revolutionized thinking in security studies, by both deepening and widening the concept of security. Barry Buzan (1991) proposed to study how the meaning of security was constructed,[14] whereas Waever (1993) widened the study of security to sectors outside the field of military security.[15] Securitization theory provides a framework for studying how the logic of security is applied to 'new' issues, and how this legitimizes certain 'extraordinary measures'. This chapter sets out the basic framework of securitization theory and its main critiques. These critiques form the basis of the argument for the framework of 'performative securitization', which structures this thesis. It will argue that the 'speech act' should be replaced with post-structuralist 'discourse'.

The classic securitization theory framework

Securitization theory focuses on the process by which an issue becomes socially constructed and recognized as a security threat.[16] Securitization, in its classical version, is a 'speech act': by labeling something as a security issue it becomes one.[17] The developers of this theory, Buzan, de Wilde and Waever (1998) based it upon John L. Austin's speech act theory, in which language is viewed as performative. Each speech act can convey three types of acts: saying something *meaningful* (locutionary act), doing *in* saying something (illocutionary act) and the effects produced *through* acting in saying something (perlocutionary effect).[18] The performativity of language, following Austin, is also dependent upon appropriate circumstances.[19] These contextual requirements for success of the speech act, or felicity conditions, include a 'specific linguistic framing and a particular intersubjective context'.[20] These ideas have been adopted by the Copenhagen School.

Securitization theory poses that a securitizing actor makes a securitizing move, in which someone frames an issue as an existential threat to the survival of a referent object. This then has to be accepted as such by a relevant audience. If successful, this logic of security takes an issue out of the political arena and legitimizes extraordinary measures.[21] A referent object can be the state, as in national security, but also individuals, critical infrastructures or the environment. Securitizing moves must follow internal felicity conditions: rules and conventions of a speech act and its consequences, or in other words a logic- or grammar of security.[22] This logic of security constructs a story that includes an existential threat, a sense of urgency and a way out.[23] Similar to the speech act, external conditions must be met for securitization to happen. The theory includes external facilitating factors that can constrain

[14] Barry Buzan (1991). New patterns of global security in the twenty-first century. *International Affairs*, *67*(3), 431-451.

[15] Ole Wæver (1993). *Securitization and desecuritization* (p. 48). Copenhagen: Centre for Peace and Conflict Research.

[16] Frank A. Stengel (2019). Securitization as Discursive (Re) Articulation: Explaining the Relative Effectiveness of Threat Construction. *New Political Science*, *41*(2), 295; Matt McDonald (2008). Securitization and the Construction of Security. *European journal of international relations*, *14*(4), 581; Sara Léonard (2010) 'EU border security and migration into the European Union: FRONTEX and securitisation through practices', *European Security*, 19:2, 235.

[17] Ole Wæver (2003) *Securitisation: Taking stock of a research programme in Security Studies.* Unpublished manuscript, 13.

[18] Thierry Balzacq (2005). 'The three faces of securitization: Political agency, audience and context'. *European journal of international relations*, *11*(2), 175.

[19] Marina Sbisà (2002). Speech acts in context. *Language & Communication*, *22*(4), 422.

[20] John. L. Austin (1962) *How to Do Things with Words.* Oxford: Clarendon Press, 14-15.

[21] Barry Buzan, Ole Wæver & Jaap de Wilde (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers, 25.

[22] Juha Vuori (2016) 'Constructivism and securitization studies'. In *Routledge Handbook of Security Studies* (pp. 64-74). Routledge, 65.

[23] Stengel, 'Securitization as Discursive (Re) Articulation', 296.

or enable audience acceptance of the move, including the social position of the actor and - audience and the nature of the threat.[24]

Securitization theory opened the field of security studies to include issues outside of the traditional military and national security threats. Following Waever, new sectors have been added to which the logic of security has been applied: the 'environmental-, economical-, societal- and political-sector'.[25] Later, scholars have argued cyber security to be a separate sector within the theory.[26] Distinct to this sector is the networked character of computer systems, which crosses boundaries and distinctions often seen as crucial in security studies.[27] Not only does cyberspace transcend traditional territorial boundaries, cyber security discourse moves across distinctions between 'individual and collective security, between public authorities and private institutions and between economic and political-military security'.[28] Although it is not formally part of the framework, scholars have used the term militarization to refer to extreme strands of securitization, focused on the role of the military as a countermeasure.[29] It is a discourse in which 'security is linked more closely to military practices instead of other, non-military means'.[30] Militarization refers to how a threat is constructed as relevant to military security but also how military practices are applied to a new issue. In other words, it is a specific focus within securitization theory.

Critique to the Copenhagen School

The Copenhagen School securitization theory has been influential but has also been criticized and refined.[31] These critiques focus on the development of concepts and the relationships between factors. The main discussion is between an internalist and externalist reading of the theory, rooted in discussions about speech act theory. Speech act theory is argued to be incoherent: it implies simultaneously 'the autonomous productive power of a text', as well as being reliant upon external factors such as the authority of an actor.[32] Securitization, similarly, is both performative in itself, and an intersubjective process formed out of interaction between securitizing actors and audiences. The latter is the focus of the externalist, or sociological approach to securitization theory.[33] These scholars argue that the CoS version of the theory neglects the intersubjective nature of the theory, as it does not theorize how to establish whether the audience has accepted a securitizing move. [34] Finally, the theory is seen as vague on the conceptualization of 'extraordinary', and if that is established the question if securitization can

[24] Vuori, 'Constructivism and securitization studies', 65; Stengel, 'Securitization as Discursive (Re) Articulation', 296.
[25] Wæver, *Securitization and desecuritization.*
[26] Hansen & Nissenbaum, 'Digital Disaster'.
[27] For example, boundaries of states and between individual and collective security, in Hansen & Nissenbaum 'Digital Disaster'.
[28] Hansen & Nissenbaum, 'Digital disaster', 1161.
[29] Mirva Salminen and Mika Kerttunen (2020) 'The becoming of cyber-military capabilities' *Routledge Handbook of International Cybersecurity*, Routledge, 96.
[30] Thorsten Bonacker (2018). 'The militarization of security. A systems theory perspective'. *Critical Military Studies*, 3.
[31] Matt McDonald (2008). Securitization and the Construction of Security. *European journal of international relations*, *14*(4), 563-587; Holger Stritzel (2007). Towards a theory of securitization: Copenhagen and beyond. *European journal of international relations*, *13*(3), 357-383.
[32] Stritzel, 'Towards a theory of securitization', 365.
[33] Thierry Balzacq, Sarah Léonard & Jan Ruzicka (2016). 'Securitization'revisited: Theory and cases. *International Relations*, *30*(4), 494-531; Stritzel 'Towards a theory of securitization'.
[34] Thierry Balzacq, 'The three faces of Securitization'; Thierry Balzacq, 'Understanding Securitization Theory'; Philipp Klüfers,(2014). Security repertoires: Towards a sociopragmatist framing of securitization processes. *Critical Studies on Security*, *2*(3), 278-292; Colin McInnes & Simon Rushton (2013). 'HIV/AIDS and securitization theory'. *European Journal of International Relations*, *19*(1), 115-138.; Holger Stritzel (2014). 'Securitization Theory and the Copenhagen school', *Security in Translation* (pp. 11-37). Palgrave Macmillan, London.

exist without these sort of measures?[35] In the case of 'human security', there is no call for measures that are undemocratic, military or that require extraordinary means.[36] Neglecting this as a form of securitization, as the Copenhagen School would imply, is criticized. The framework is thereby too 'static', treating the logic of security and the types of measures that follow as fixed entities. In order to theorize these external factors and -context, the anthropological 'PARIS-school' proposed to supplement securitization theory with a focus on practices.[37]

The 'PARIS-school' provides a reactive theory to the construction of security. Instead of theorizing security to be something of survival and urgency, these scholars consider security to be a routine process, produced and reproduced in everyday practices. Bigo (2002) argued that security is defined by 'mundane bureaucratic decisions and practices that create a sense of insecurity and unease'.[38] This logic of routine diverges from the CoS in its internal logic of threat construction. Instead of an intentional speech act, an intentional moment of exceptionality and public legitimation, security threats can be constructed gradually. [39] Importantly, this theory inverts the logic of the CoS where practices (extraordinary measures) follow speech acts, and where these are solely institutionalized urgency. Instead, to study securitization is 'to focus on the creation of networks of professionals of (in)security, the systems of meaning they generate and the productive power of their practices'.[40] In other words: meaning is created through practice, and not the other way around. With this focus on the daily performances of security professionals and on observing the power relations in the 'field', these scholars 'solve' the conceptual weakness of the original theory. The PARIS-school, however, is also criticized for its flat view of the process, as it does not differentiate between political- and security practices.[41]

A securitizing discourse

The two approaches are often treated as irreconcilable which Bourbeau (2014) considers to be empirically and theoretically unsatisfactory.[42] The sociological approach cannot escape a reference to discourse and narrative, and the speech act approach is in itself not able to explain routinization and non-exceptionality. This thesis thereby focuses on the common ground between the two approaches. Security is perceived as performative: either as a discursive- or non-discursive enactment of meaning.[43] In this way, securitization can be viewed as an interactive process of both exception and of routinization. It focuses both on speech acts, and how understandings are 'locked in' through mechanisms of reproduction. [44] In a post-structural reading of securitization, inspired by Derrida and Butler, the speech act is replaced by discourse.

---

[35] For example in Lise Philipsen, (2018). 'Performative securitization: from conditions of success to conditions of possibility'. *Journal of International Relations and Development*, 2; Thierry Balzacq (2005). The three faces of securitization: Political agency, audience and context. *European journal of international relations*, *11*(2), 171-201; Thierry Balzacq, (Ed.). (2010). *Understanding securitisation theory: How security problems emerge and dissolve*. Routledge; Holger Stritzel,(2014). *Security in translation: Securitization theory and the localization of threat*. Springer.

[36] Philipsen, 'Performative securitization', 6.

[37] Didier Bigo & Emma McCluskey (2018). 'What Is a PARIS Approach to (In) securitization? Political Anthropological Research for International Sociology'. *The Oxford handbook of international security*, 116.

[38] Didier Bigo (2001). 'Migration and security.' *Controlling a new migration world*, 111; Philippe Bourbeau, (2017). Migration, exceptionalist security discourses, and practices. In *Handbook on Migration and Security*. Edward Elgar Publishing, 108.

[39] Philippe Bourbeau, (2014). 'Moving forward together: Logics of the securitization process'. *Millennium*, 43 (1); Elsa Vigneau, (2019). 'Securitization theory and the relationship between discourse and context: A study of securitized migration in the Canadian press, 1998-2015'. *Revue europeenne des migrations internationales*, *35*(1), 193.

[40] Collective, C. A. S. E. (2006). Critical approaches to security in Europe: A networked manifesto. *Security dialogue*, *37*(4), 468.

[41] Bourbeau, 'Moving forward together', 112.

[42] Bourbeau, 'Moving forward together', 114.

[43] Stengel, 'Securitization as Discursive (Re) Articulation', 14.

[44] Bourbeau, 'Moving forward together', 112-113.

In a critique to Austin, Derrida posed that external conditions cannot account for the 'success' of a speech act, because that presupposes that context is determinable.[45] Instead, meaning is only to be found within the text itself: 'Il n'y a hors de text'.[46] Instead of treating the meaning (i.e. identity or ideas) and the material as separate, discourse encompasses social practices and the social field. Context in this sense is something internal to discourse, it is constituted out of sedimented discursive practices. Central to this understanding is Derrida's concept of iterability, which implies that a text is citable. It can travel to new contexts, and is changed through citation.[47] Following Derrida, the logic (convention/meaning) of security is changeable: securitization is a *process* of generating meaning. Each securitizing move adds something to the meaning of security, while simultaneously being consistent with past practices.[48] The performative is not a snapshot, a singular act, but is 'derivative of broader social practices that must be cited in order to be intelligible'. Thereby the speech act is historicized and placed within its established (linguistic and non-linguistic) conventions.[49]

Butler adds that speech acts have 'the power to constitute new meaning and create new patterns of significance in social relations'.[50] Because external context is always changing, she argued that we cannot know what circumstances empower the securitizing actor.[51] This means that authority should not be taken a prerequisite for securitizing moves. There is also the possibility to claim authority through speech acts.[52] This implies that audiences are not passive, but potential securitizing actors.[53] Securitization processes are strongly iterative and interactive struggles for authority and legitimacy.[54] Therefore, the Derridean view of the performative goes beyond the securitizing actor and its intentions. It is less focused on the 'who' of securitization and more on the relationship between the utterance and internal (discursive) context. It is through repetitions that securitization becomes effective.[55] Attention is placed on how meaning is produced, by looking at the agency at power at play in speech acts.[56]Abandoning external success factors opens the theory up to looking at routine, 'failed securitization' (incompetent acts) and to lose the elite bias, as proposed by the PARIS-school.

A post-structuralist framework of Securitization

Securitization, in this thesis, is viewed as a security performance.[57] It includes both signifying practices (speech act or moment of exception) and material practices (security practice or routine).[58] Securitization is seen as a gradual, intersubjective process that is 'produced over time in multiple texts that represent something as a threat'.[59] The core of this process is a securitizing narrative - embedded in- and interacting with existing discursive structures- that materializes in emergency measures.[60] These emergency measures complement- and are intertwined with signifying practices. Material practices are

[45] Philipsen, 'Performative securitization', 7-8.
[46] Derrida stated: 'There is no outside-text', this means that although there is an 'external' reality, it is also imbued with meaning and therefore part of the discourse. Derrida, Jacques, Spivak, Gayatri Chakravorty (1997). *Of Grammatology*. Baltimore: Johns Hopkins University Press., 158-159
[47] Philipsen, 'Performative securitization', 7.
[48] R. Guy Emerson (2016) 'Limits to a cyber-threat', *Contemporary Politics*, 9.
[49] Emerson, 'Limits to a cyber-threat', 9.
[50] Stritzel, 'Towards a theory of securitization', 361.
[51] Adam Côté (2016). Agents without agency: Assessing the role of the audience in securitization theory. *Security Dialogue, 47*(6), 548
[52] Butler in Philipsen, 'Performative securitization'.
[53] Philipsen, 'Performative Securitization', 11.
[54] Philipsen, 'Performative Securitization', 11.
[55] Stengel, 'Securitization as Discursive (Re) Articulation', 10.
[56] Philipsen, 'Performative securitization', 17.
[57] Bourbeau, 'Moving forward together', 106-107.
[58] Bourbeau, 'Moving forward together', 113.
[59] Julie Wilhelmsen (2016). 'How does war become a legitimate undertaking? Re-engaging the post-structuralist foundation of securitization theory'. *Cooperation and Conflict,* 7.
[60] Wilhelmsen, 'How does war become a legitimate undertaking?, 7.

part of the securitizing discourse as well as its outcome. They are enabled through a legitimizing securitizing narrative, but they also convey the threat identity. Finally, securitization processes have effects for the referent object by (re)producing actors, audiences and communities.[61] It is a process instead of a moment, and it is through 'positive reinforcements' that securitization remains the dominant discourse: a securitizing attempt thereby consists of a *series* of utterances.[62] Securitization can be viewed as a discursive battle, in which different actors negotiate and struggle over the meaning of security as well as over how it should be carried out.[63]

The first component of a securitization process is that of representation: a securitizing actor represents an issue as an existential threat to a referent object. This component concerns the internal logic and consistency of the security argument made.[64] The practice of securitization is here the signifying practice of giving something the identity of an existential threat.[65] Such a securitizing narrative is stronger when it follows a specific analytical template. In the poststructuralist reading this firstly exists out of an existential threat, a description of the nature of the threat. Secondly, this includes a point of no return or urgency', a description of what will happen to the referent object if no security action is taken. Finally, it includes a way out, the identification of policies, practices or emergency measures necessary to tackle the threat.

The second component of securitization is concerned with the inter-unit relations and breaking free of rules. This component concerns the external factors of actor/audience relationships and the facilitating conditions.[66] In post-structuralist terms, these factors are seen as internal: the discourse or securitizing argument creates boundaries between actor and audience, and between the threat and threatened. The identity of a referent object is thereby (re)produced by the securitizing discourse and not an objective, pre-existing fact.[67] The securitizing move produces boundaries for acceptable action, and thereby also produces an actor by 'demarcating a sphere where such an actor can legitimately produce those policies. The identity of the referent object is likewise (re)produced through securitizing moves by constructing a binary opposition between a threat and a threatened. This establishes a relation of power where the threatened, or referent object, will be privileged. Securitizing moves thereby (re)produce identities and power relations (or authority).

The last component, the possibility of emergency measures, focuses on the actual material expressions of the signifying practices. It is not the claim that signifying practices cause certain policies, but they both open up- and constrain the range of possible and legitimate policies or practices.[68] This means that it is necessary to assess the 'enactment of a securitizing narrative in specific policies and material practices directed towards that/those represented as existential threat'. This implies linking two aspects: the signifying representations in the narrative (the way out/ policy proposals) and the implementation of this in practices (policies). Policies are never a given response to an external reality, but are co-constituted by ideas or identities.[69] Following Adler and Pouliot, practices are 'patterned actions that are embedded in particular organized contexts and as such are articulated to specific types of action and are socially developed through learning and training'.[70] Action is behavior imbued with meaning. Practices translate abstractions into physical and sensory modalities that make something more

[61] Wilhelmsen, 'How does war become a legitimate undertaking?, 6.
[62] Wilhelmsen, 'How does war become a legitimate undertaking?, 6; Sara Léonard & Christian Kaunert (2019). 'A new securitization framework' (Chapter 1). *Refugees, security and the European Union*. Routledge, 29.
[63] Philipsen, 'Performative securitization'.
[64] Wilhelmsen, *Russia's securitization of Chechnya,* 25-26.
[65] Wilhelmsen, *Russia's securitization of Chechnya,* 36.
[66] Stritzel, 'Towards a theory of securitization', 362-365; Wilhelmsen, *Russia's securitization of Chechnya*.
[67] Wilhelmsen, *Russia's securitization of Chechnya*, 40-41.
[68] Wilhelmsen, *Russia's securitization of Chechnya,* 25.
[69] Lene Hansen (2013). *Security as practice: discourse analysis and the Bosnian war*. Routledge, 43.
[70] Emmanuel Adler & Vincent Pouliot (Eds.). (2011). *International practices* (Vol. 119). Cambridge University Press, 6.

intelligible.[71] The focus is placed on changes in- or beginnings of such patterned actions.[72] Instead of focusing on the routinization, securitization directs the attention to how practices are changed or established. Securitizing practices, or emergency measures, are those practices that are usually used to tackle issues that are widely to be 'considered security threats', (i.e. traditional military practices). Securitizing practices can further be viewed as practices that are extraordinary. This does not necessarily mean it is 'above politics, or to involve emergency, exceptionalism or illegality'.[73] Rather, an extraordinary character needs to be assessed in its specific context. In other words: it has not been applied to a specific policy issue before. [74]

Following this framework, a set of sub-questions can structure the analysis of the securitizing discourse. The first question looks at how the securitizing argument is constructed. This exists out of the identification of a threat, the threat level (urgency, existentialism) it is given, and what solutions are proposed (a way out). The second question focuses on the identities of actors, referent objects and power relations that are (re)produced in the process of securitization. This includes looking at how it constructs the Estonian identity (referent object) and the actors that are authorized to react to the threat (policy makers, security professionals). Finally, the materializations of discourse in the form of emergency measures or those security practices or policies that seek to deal with the threat are analyzed. It is then interesting to see how these either (re)produce the securitizing argument or diverge from it. Each of these components should be placed within its discursive context to be able to identify how it builds upon convention, but also how it adds to this context and in that process possibly changes existing discourses. This requires identifying the basic- or existing dominant discourses in a society, prior to the 2007 attacks, and looking how securitizing moves refer to these discourses. Relevant discursive terrains include an international discourse on cyberspace/ security (the threat), the national discourse on the Estonian state/identity (referent object) and the institutional context (actors/ power relations).[75] This discursive context forms the condition of possibility that constrains and enables (discursive and non-discursive) action.

[71] Stevens, *Cyber security and the politics of time*, 18.
[72] Wilhelmsen, *Russia's securitization of Chechnya.*
[73] Léonard & Kaunert, 'A new securitization framework', 29.
[74] Léonard & Kaunert, 'A new securitization framework', 29.
[75] Emerson, 'Limits to a Cyber Threat', 9.

Chapter 3: Methodology

Securitization theory is discourse analysis – Barry Buzan[76]

This thesis positions itself as a post-structuralist, internalist approach to securitization theory. [77] By implication, it views security as a particular discourse that is performative. Securitization processes provide templates or frameworks for uncovering how relations between language and social structures are co-constitutive. The method used to uncover this is discourse analysis. This chapter will shortly discuss the underlying assumptions of the research, how the method of discourse analysis is used to structure the analysis and the research goals and strategies. Following, it will argue for the choice of selection of material and for the focus on the case of Estonia after the 2007 cyber-attacks.

Research objectives

This thesis aims to contribute to the empirical and theoretical debate on the construction of the cyber threat in Estonia. It aims to contribute to understanding the way in which an act (DDoS attacks) - that has historically been treated as a technical issue of computer security - came to be seen and treated as a threat to national security. In reaction to previous research, this thesis argues that cyber security has successfully been transformed into an issue of national security in Estonia, and has changed the meaning of security. Different from earlier studies, that either focus on policy change[78] or on (securitizing) narratives[79], this thesis aims to focus on practice and narrative equally. This thesis argues that the construction of the cyber threat and the transformation of the cyber security field should be studied from an extended time frame as opposed to a certain moment in time. The theoretical objective of this thesis is to contribute to the debate and critiques to securitization theory, by focusing on the common ground between the sociological PARIS-approach and the traditional Copenhagen School.[80] The performative securitization approach is textual, but provides answers to the theoretical problem of linking securitizing move to extraordinary measure and that of audience acceptance.

Assumptions and method

In seeking to understand how cyberspace came to be seen as an existential security threat in Estonia this thesis takes an interpretive stance towards research. Using a qualitative approach, the focus is placed on an in-depth case study and the construction of meaning.[81] In doing so, the thesis takes a stance in an ontological, methodological and theoretical debate surrounding securitization theory. The internalist, post-structuralist approach to securitization theory understands security as a discourse in which language is assumed to be constitutive of social reality.[82] Different from the Austinian speech act, discourses encompass the social field and the social practices that are in the traditional securitization theory perceived as results of securitizing attempts. A securitizing discourse opens up- and constrains the range of feasible policies, practices and actions, but does not determine action. The assumption is only that a securitizing representation enables the legitimate undertaking of an action. Although such an action is possible without such a threat representation, that would not have made sense.[83]

Discourse analysis is both an ontological theory and a method. As a method, it involves the

[76] Buzan, New patterns of global security in the twenty-first century.
[77] Balzacq, 'The three faces of securitization'; Stritzel, 'Towards a theory of securitization'
[78] Myriam Dunn Cavelty (2008). 'Cyber-terror—looming threat or phantom menace? The framing of the US cyber-threat debate'. *Journal of Information Technology & Politics*, *4*(1), 19-36.;
[79] Hansen & Nissenbaum, 'Digital disaster'.
[80] Bourbeau, 'Moving forward together'.
[81] Charles C. Ragin & Lisa M. Amoroso (2019). *Constructing social research: The unity and diversity of method*. Pine Forge Press, 121.
[82] Wilhelmsen, *Russia's securitization of Chechnya.* 23.
[83] Wilhelmsen, *Russia's securitization of Chechnya,* 29.

identification of key texts in which a specific rhetorical structure is located that can indicate the securitization move. Discourses are understood as social relations represented in texts, and in which language used in these texts is used to construct meaning and representation.[84] Discourses are 'made in a process of social practical interaction and are always textually interconnected. Discourse analysis aims to establish the meaning of texts shaped by distinct contexts'. [85] A text does not only reflect and describe an external reality, it *does* things and thereby has political implications. Although most discourse analyses focuses on written or spoken language, language does not have to be verbal.[86] Non-verbal language includes body language for the individual, but for a collective it could be movement of full troops.[87] Any text is situated in a larger web of texts that it references to, and should therefore be situated and studied in relation to other texts.[88] A (policy) discourse constructs problems, objects and subjects, and articulates policies to address those. It structures identities (meaning), and legitimizes and enables action.[89] Policy, or practice, and identity are co-constitutive: it is only through the discursive enactment or performance that identity comes into being, but this identity is simultaneously the legitimization and the reason for the existence of this policy or practice.[90]

As such, discourse analysis incorporates both material and ideational factors of discourses without privileging one over the other, since ideational constructions are both enacted through and reproduced by a set of material structures.[91] As an iterable process, meaning needs to be reproduced and repeated in order to stay dominant over other interpretations. A post-structuralist approach to securitization thus focuses on signifying practices, but also how these 'find an expression in material practices (emergency measures) and how these, in turn, serve to constitute and confirm the identity constructions in the securitizing narrative'.[92]

In empirical terms, poststructuralist discourse analysis focuses on how social facts are brought together to constitute events.[93] Key events are those situations where important facts are manifested in debates: moments of contestation or identity change. An analysis of the debates around such key events provides a methodological tool to structure data collection. [94] By invoking an issue with the concept of national security, it is a particularly radical form of identity construction. It operates around a distinct rhetorical and discursive force providing a sense of urgency and responsibility to those speaking within it.[95] Studying the formation of identity/ meaning, one can look at the boundaries that are drawn on a spatial, temporal and ethical dimension. The spatial dimension implies that identity is always relationally constituted to an Other.[96] Identity can further be temporal, based on themes of 'development, transformation, continuity, change, repetition or stasis'.[97] Finally, identity constructions are based on ethics, morality and responsibility where the Self bears (non)responsibility towards the Other.[98] This dynamics of boundary drawing and components of identity can be captured with the concept of social imaginary.[99] This is a way in which people 'imagine their social existence, how they fit together with

[84] Vivienne Jabri,(1996). *Discourses on violence: Conflict analysis reconsidered*. Manchester University Press, 94-95.
[85] Thierry Balzacq (Ed.). (2010). *Understanding securitisation theory: How security problems emerge and dissolve*. Routledge, 40.
[86] Norman Fairclough (2001) 'Critical discourse analysis as a method in social scientific research'. *Methods of critical discourse analysis*, *5*(11), 122.
[87] Lene Hansen (2013). *Security as practice: discourse analysis and the Bosnian war*. Routledge, 21
[88] Marianne W. Jørgensen & Louise J. Phillips (2002). *Discourse analysis as theory and method*. Sage, 26.
[89] Hansen, *Security as practice*, 19.
[90] Idem.
[91] Ibid, 20.
[92] Wilhelmsen, 'How does war become a legitimate undertaking?', 9.
[93] Hansen, *Security as practice*, 28.
[94] Idem.
[95] Ibid, 30.
[96] Ibid, 42.
[97] Hansen, *Security as practice*, 42.
[98] Ibid, 45.
[99] Charles Taylor (2004), *Modern social imaginaries*. Duke University Press, 23.

others, how things go on between them and their fellows, the expectations that are normally met, and the deeper normative notions and images that underlie these expectations'.[100] It thereby refers to a spatiality – describing relations between Self and Other – as well as temporality (expectations and underlying notions and images) and ethical or normative ideas. These imaginaries can be represented, following Schröder and Schmidt (2001), through narratives, performances and inscriptions.[101] Joelien Pretorius (2008) adds that a '*security* imaginary is that part of a social imaginary 'specific to a society's common understanding and expectations about security and [which] makes practices related to security possible'.[102] These different dimensions of identity construction and difference provide a lens to understand the links between identity and policy. Questions to be answered are: how are selves and others constituted in policy discourse, how radical is the difference and how is this constituted through the articulation of spatial, temporal and ethical identity.[103] Basic discourses, those texts identified as being representative for a wider reading, are built on 'explicit articulations of key representations of identity'. These representations must then be placed in a historical conceptual context. Finally, texts must be related to potential contesting discourses and analyze how these propose different policy measures.[104]

It is the aim of this thesis to study how a securitizing discourse re-articulates and changes meaning (identity, logic of security) and practice (emergency measures/ policies). This continuity is studied by placing the texts within its discursive context, whereas change is studied by identifying how boundaries are drawn and re-drawn. In the case of identity/meaning, this means looking at boundaries of spatial, temporal and ethical identity. Practices, following the framework, are intertwined with signifying practices and are central to the construction, constitution and maintenance of the linguistic identity they enact.[105] Although analytically treated as apart from signifying practices in this thesis, material practices are to be studied using similar methods using texts and quotes.[106] It is studied by focusing on how boundaries are drawn for acceptable action, how these legitimize and materialize in policies and practices and in turn how these practices transmit and stabilize the securitizing discourse.[107] The boundaries for acceptable action reflect the scaling of representations of threat.[108] Constructions of threats can be placed on a scale of varying degrees of danger and difference, leading to equally radical measures.[109]

Research design

The choice for a method of discourse analysis structures the research questions, the empirical data to collect and the focus of the case study. This thesis makes use of an intertextual model focused on official policy discourse of those actors with central roles in the policy process. It links these official texts, such as speeches, debate, interviews or articles, to those texts that directly influence this discourse. This model focuses on the extent of links made to oppositional discourses and critique within texts and whether it is deemed necessary to counter those texts.[110] The thesis focuses on a single 'Self', examining the 'Estonian state' and its relation to cyber security policy.[111] The temporal perspective chosen is a

[100] Taylor, *Modern social imaginaries*, 23.
[101] Bettina Schmidt & Ingo Schröder (2001). *Anthropology of violence and conflict*. Psychology Press: 9.
[102] Emphasis in original; Joelien Pretorius (2008). 'The security imaginary: Explaining military isomorphism'. *Security Dialogue, 39*(1), 112; Stevens, *Cyber security and the politics of time*, 36.
[103] Hansen, *Security as practice*, 45.
[104] Ibid, 48.
[105] Wilhelmsen, *Russia's securitization of Chechnya*, 151.
[106] Idem.
[107] Patrick T. Jackson (2006). *Civilizing the enemy: German reconstruction and the invention of the West*. University of Michigan Press, 16.
[108] Wilhelmsen, *Russia's securitization of Chechnya*, 25.
[109] Ibid, 26.
[110] Hansen, *Security as practice*, 66; another possibility is to focus on oppositional political parties or on popular culture.
[111] Ibid, 68.

historical analysis, seeking to both capture moments of 'intensification' (change) and of more gradual evolution.[112] Thereby this thesis makes use of second-order observations and interviews that have been conducted and included in academic literature. The broader time frame and focus make documentary analysis a well suited and feasible method. As the purpose is to focus on the full process of securitization by focusing on the performativity of the speech acts, documents provide a good overview of the historical development of discourse. As it is not the intention of this thesis to capture the 'intensity' of discourse and securitizing moves, but rather to look at development, it is not necessary to capture all securitizing moves or texts in a quantitative analysis.

Chapter outline and structure of analysis

Securitization as an iterable process of (re)production is studied by looking at the interaction between signification and enactment. This thesis analyses how securitizing discourse has evolved over time by focusing on continuity and change in the ideational and material practices surrounding cyber security in Estonia. The analysis thereby takes a chronological order. The first chapter provides background information on the 2007 cyber-attacks and elaborates on the institutional context in the country. Following, the second chapter discusses the broader discourses, or the discursive context prior to the 2007 attacks, by looking at discourses on the Estonian identity and the (global) discourses on cyberspace, -security and –war. These discourses serve as a structuring device for the following two chapters. The first focuses on how the cyber-attacks have been interpreted and used in a securitizing discourse that legitimizes new and existing practices. The second focuses on how cyber security has evolved in Estonia by looking at the policies, practices and debates after 2007. Throughout these last two chapters, the following sub-questions are answered:

1) *How has cyberspace and -security been represented by the Estonian state after the 2007 cyber-attacks?*
    a. *What boundaries between the 'Self' and 'Other' are drawn in terms of spatial, temporal and ethical dimensions?*
    b. *What level of urgency (existentialism) has been assigned to the issue?*
    c. *What boundaries for acceptable action are drawn in these representations, enabling and constraining policies and practices?*
2) *How has this representation materialized in policies, institutions and actions?*
    a. *How are existing security practices legitimized and changed through securitizing moves?*
    b. *How do security practices confirm and enact the identity constructions drawn up in the securitizing narratives?*

[112] Ibid, 70.

Chapter 4: A Discursive context: Discourses of Estonian identity and cyber security

"The internet is presented as a human right of every Estonian in an ultimate 'wired' nation and digital society characterized by 'transparency, efficiency and cyber-security'.[113]

The representation of the 2007 cyber-attacks as a threat to national security is embedded and structured by its discursive context. This chapter identifies two basic discourses: on the national level a discourse on the Estonian identity and national security, on the international level a discourse on cyberwarfare and cyber security. As has been explained, (national) security discourses are intertwined with discourses of national community and historical forms of political community.[114] In both of these discourses, boundaries are drawn between a 'Self' and an 'Other'. In the case of Estonian identity, this mainly is between a 'Western Self' against the 'Eastern/Russian Other'. In the case of cyber security, the most radical boundary is between the roles 'malicious hacker' and the 'cyber security expert'. These two discourses serve as structuring devices for the analytical chapters that follow below.

Discourses of Estonian identity.

After Estonia became independent from the Soviet Union in 1991, the country underwent rapid and radical institutional changes. This was accompanied by a reinvention of the Estonian national identity: it imagined itself as a Western, neo-liberal democracy and aimed to distance distanced itself from its former occupant. This was part of a deliberate strategy of rewriting its past, and nation branding.[115] In 2001, it hired a British consulting firm to 'convey to the world its legitimacy as a European nation and its openness to world capital'.[116] This firm stated its objective to be to 'help Estonia overcome the 'accident of history' that placed the country in the East rather than the West in the mind of its interlocutors'.[117]Estonia was the first former-Soviet country to reform its economy and institutions, and the first to start negotiations with the EU and NATO. The country democratized, basing its constitution on Western models and values: it gave political supremacy to the *Riigikogu* (State Assembly), a single-chamber parliament.[118] The country imagined itself as a Western/ Nordic, and modern country as opposed to its Soviet, communist past. Estonia thereby drew boundaries between Self and Other in terms of spatial, temporal and ethical identities.

The new Estonian state thereby established a spatial identity, differentiating itself from its physical neighbor Russia.[119] The establishment of an ethnic Estonian identity has also been strongly articulated in opposition to local Russian-speakers.[120] About 25% of inhabitants of Estonia are ethnic Russians that moved to the country during the Soviet period. In 1991, Estonian legislators had adopted a citizens act proclaiming that residents who had been citizens before 1940 had their rights restored meaning those who settled after became 'Aliens'. These people could not participate in elections and the government.[121] The Russian ethnic minority has been poorly integrated into Estonian society, both

[113] Daria Savchecnko (2019) 'E-Estonia Reprogrammed: Nation Branding and Children Coding (Chapter 8.) in Mario Biagioli & Vincent Antonin Lépinay (ed.) *From Russia with Coe: Programming Migrations in Post-Soviet Times.* Duke University Press, 214.
[114] Rob B.J. Walker (1990). 'Security, sovereignty, and the challenge of world politics'. *Alternatives, 15*(1): 5.
[115] Katrin Kello (2017) 'Identity and Othering in Past and Present: Representations of the Soviet Era in Estonian Post-Soviet Textbooks', *Journal of Social and Political Psychology* Vol. 4 (2), 665-693
[116] Savchecnko. 'E-Estonia Reprogrammed: Nation Branding and Children Coding' , 220.
[117] Melissa Aronczyk,(2013). *Branding the nation: The global business of national identity*. Oxford University Press, 140.
[118] Toivu U. Raun (1994). POST-SOVIET ESTONIA, 1991-1993. *Journal of Baltic Studies, 25*(1), 73.
[119] Kello 'Identity and Othering in Past and Present'.
[120] Ibid, 667.
[121] Nils Muiznieks, Juris Rozenvalds & Ieva Birka (2013) 'Ethnicity and social cohesion is post-Soviet Baltic States' *Patterns of Prejudice*. Vol. 47 (3), 291.

concerning cultural segregation and socio-economic terms. [122]

The Estonian identity has been imagined following narratives of: 'Estonia as a reconstituted state and society'; 'Estonia as European' and as a Nordic, Finnish country.[123] Security is a key element in the Estonian integration and sovereignty agenda. This is due to memories of oppression, but also to a narrative of 'Estonia as a small country, dependent on protection and cooperation. With only 1.2 million inhabitants, Estonia is one of the smallest countries of Europe. Membership of the European Union and NATO has been articulated as 'the ultimate expression and codification of Estonian identity and values, as well as a security guarantee'.[124]

In terms of temporal identity, discourses on Estonian identity make a strong connection to its Western past, while differentiating itself from its Soviet past. In popular discourse the Soviet past is regarded as a period of total rupture.[125] In comparison, other occupations, such as the Swedish between 1600 and 1800, are described positively. The narrative of the Estonian identity strongly draws upon continuity with the period before the Second World War. This temporality is also performed through the politics of memory, including the re-writing of history text books, the removal of statues and the creation of a national Independence Day.[126]

Estonia views itself as a modern and advanced country, and is known for its investments and heavy reliance of information technologies. The digitalization of the country has been a priority from the early 1990s, after its independence, which since has had a continuous cross-party support. A high level of public and private sector -services are provided digitally, with at its core the 'digital citizen', a label that can extend beyond the borders of the Estonian state.[127] The quick transformation was possible because the Soviet Period left the country's economic infrastructure collapsed but many young academics trained in ICT technologies – the only type of education that was possible in the Soviet Union.[128] The digitalization was further driven by ideas. First, its newly formed government pursued a Thatcher-inspired, free-market ideology, arguing that digitalization would provide the country with competitive economic advantages. [129] Further, the digital agenda was part of a broader political consensus based on joining the 'west' and seeking national security through membership of NATO and the EU.[130] From 1996, the country heavily invested in education through their 'Tiger Leap program', in cooperation with the private sector promoting entrepreneurship amongst young people.[131]

Discourses of cyber security

Discourses on cyber security or cyberwarfare have developed on both the national Estonian- and the global scale. In essence, cyber security connects practices of computer security and information and communication technologies (ICTs) to national security. Cyber as a concept can be seen as a discourse that is intertwined with politics. In order to understand narratives of and practices of cyber security, it is important to understand its conceptual history.[132]

---

[122] Oleksandra Seliverstova (2017) 'Consumer Citizenship and reproduction of Estonianness'. *Identity and Nation Building in Everyday Post-Socialist Life* (pp. 119-138). Routledge, 112.

[123] Gregory Feldman (2000). 'Shifting the perspective on identity discourse in Estonia'. *Journal of Baltic Studies*, *31*(4), 406-428. 406; Piia Taampuu, Külliki Seppel & Kadri Simm, (2019) 'Appropriation of the Nordic brand in the Estonian political discourse 1997-2017: consistencies and contestations' (Chapter 15) in *The Nordic Wave in Place Branding.* Edward Elgar Publishing, 191-206.

[124] Kuus, 'European integration in identity narratives in Estonia', 91-92.

[125] Oleksandra Seliverstova 'Consumer Citizenship and reproduction of Estonianness', 113.

[126] Feldman, 'Shifting the perspective on identity discourse in Estonia'.

[127] Rainer Kattel & Ines Mergel (2019) 'Estonia's Digital Transformation: Mission Mystique and the Hiding Hand' in Mallory E. Compton & Paul 't Hart (ed.) *Great Policy Successes.* Oxford University Press, Oxford, 155.

[128] Kattel & Mergel, 'Estonia's Digital Transformation', 155.

[129] Ibid, 146-148.

[130] Ibid, 145.

[131] Idem.

[132] Stevens, *Cyber security and the politics of time*, 14.

Cyber is often imagined in a spatialized way: as 'cyberspace' a term developed in science fiction novels. Cyberspace refers to 'a shared virtual hallucination', in which 'virtual' is something 'nonphysical' but fundamentally real of nature.[133] Cyberspace is both a physical construction, of networking information technology, but also a social construction, a system of social relations that connects people on a global scale.[134] In Western discourse, it is a value loaded space in which ideals of an ultimate 'liberal' or 'free' but also a globalized world are the norm. From the outset, cyberspace has been discussed as an inherently insecure and vulnerable construct.[135] It has therefore been intertwined with discourses of security.[136] Cyber security is not only the protection of critical infrastructures (technology and information), but also refers to threats conducted through cyber space.[137] In practice this includes looking for 'zero-days', or weak spots in coding and protecting against information operations.[138] These technical practices of computer security have been given the identity of an existential threat to the national state or global community.

Hansen & Nissenbaum define cyber security as 'computer security plus securitization'.[139] It broadly refers to practices that seek to secure states, individuals and private actors from threats ranging from computer viruses and cybercrime to categories of cyber-terror and –warfare.[140] Specific to the threat narrative around cyber security is that it transcends boundaries often seen as crucial in security studies. Not only does cyberspace transcend traditional territorial boundaries, cyber security discourse moves across distinctions between 'individual and collective security, between public authorities and private institutions and between economic and political-military security'.[141] The connection between cyberspace and discourses of war specifically makes cyber security the responsibility of the military and the state. The narrative of cyberwarfare developed before it was even technically possible in popular media, academic and policy circles. Strategic scholars have theorized the potential impact of computers on war and power relations from the 1990s and cyberspace has been treated as the 'fifth domain of warfare' in military circles. [142] ICT practices are connected to military concepts, ideas and narratives. Yet, a cyber weapon is simply software, which in practice works in a way opposed to the image of a weapon that can be directed at a target of choice with foreseeable effects.[143]

Cyber also contains temporal components. The temporality of cyber security imaginaries, theorized by Tim Stevens (2015), shapes narratives and practices of cyber security communities.[144] Cyber security is inherently temporal, as it aims to counter future and present insecurities, mobilizing imagined times of past and future as resources to legitimize present practices.[145] Discourses of cyber security are dominated by dystopian visions of the future: Cyber Doom scenarios. These forms of apocalyptic thinking construct historical events of cyber insecurity as signs of inevitable and imminent catastrophe that is bound to happen.[146] Discourses of cyber security make use of the past as a resource,

[133] David Barnard-Wills & Debi Ashenden (2012) 'Securing Virtual Space: Cyber War, Cyber Terror, and Risk'. *Space and Culture*, 15(2), 111.
[134] Barnard-Wills & Ashenden, 'Securing Virtual Space', 111.
[135] Ibid, 118.
[136] Ibid, 114.
[137] Stevens, *Cyber security and the politics of time*, 223.
[138] Jouni Flyktman, Aki-Mauri Huhtinen and Lars Koreman (2020) 'Information Operations (Chapter 13) in Routlegdge Handbook of International Cybersecurity. P. 177
[139] Hansen and Nissenbaum 'Digital Disaster', 1060.
[140] Myriam Dunn Cavelty (2020) 'Cybersecurity between hypersecuritization and technological routine' in Routledge handbook of international cybersecurity.' P. 16
[141] Hansen & Nissenbaum, 'Digital disaster', 1161.
[142] For example, John Arquilla & David Ronfeldt (1993). Cyberwar is coming!. *Comparative Strategy*, *12*(2), 141-165.
[143] Cavelty 'Cybersecurity between hypersecuritization and technological routine', 16.
[144] Stevens, *Cyber security and the politics of time*, 207.
[145] Ibid, 2.
[146] Ibid, 16; Barnard-Wills & Ashenden, 'Securing Virtual Space', 118.

using historical analogies such as 'electronic Pearl Harbor' or 'digital 9/11'.[147] The use of the past analogies and future disasters can be defined as a discourse of *hypersecuritization*.[148] This temporality also finds its expression in practices that Stevens calls 'inhabitation of the future'.[149] Inhabitation is meant both metaphorical, as a way of occupying future events through exercises and simulations as well as literally, by training young people for cyber security.[150]

Finally, cyber security discourse builds upon ethical identities. Cyber security or -defense as a practice has been constructed as something 'legitimate' as opposed to the 'malicious' practices of hackers.[151] There have for a long time been no strong international norms for cyberspace, both in legal and cultural terms. Prior to 2007, cyberwar had been discussed as a possibility but not as a realistic security threat.[152] In practice, there were no laws or policies defining when- and if cyber-attacks should be treated as an act of war. The insecurity of digital networks was seen as a technical problem instead of a political one. This can be defined as a discourse of *technification*: to construct an issue as reliant upon technical and expert knowledge, granting those experts a special epistemic authority.[153] Cyber security experts are still often perceived as apolitical and objective, granting them a privileged role in constructing the cyber threat image. [22]

[147] Stevens, *Cyber security and the politics of time*, 17.
[148] Hansen & Nissenbaum, 'Digital disaster', 1164.
[149] Stevens, *Cyber security and the politics of time*, 17.
[150] Ibid, 17.
[151] For example, James Shires explores this image and narrative as has been seen in popular culture and in expert communities in James Shires, (2020). 'Cyber-noir: Cybersecurity and popular culture'. *Contemporary Security Policy, 41*(1), 82-107.
[152] Kaiser, 'The Birth of Cyber War', 11.
[153] Hansen & Nissenbaum, 'Digital disaster', 1167- 1168.

Chapter 5: Securitizing moves following the 2007 attacks

"The attack is virtual, psychological and real – all at the same time".[154]

The 2007-attacks led to securitizing moves by the Estonian government that were not only directed at the international press, but also at the ethnic Estonian, domestic audience. These attacks are viewed as a key event, a moment of identity change. As one of the first of its kind, the attacks fueled (inter)national imaginaries of the cyber threat. This chapter will analyze how this securitizing narrative developed initially after the attacks. It will focus on how securitizing actors represented both Russia and cyber insecurity as a primary threat to the survival of the Estonian state, the Western world and to individual security. It will then look at the level of urgency assigned to the threat and finally how this established the boundaries for acceptable action.

The catalyzing event: the cyber-attacks to Estonia

On the night of 26 April 2007, the Estonian government moved the Bronze Soldier, a Soviet World War II memorial statue to the outskirts of Tallinn. The Russian ethnic minority in Estonia protested, backed up by the Russian government that called for the resignation of the Estonian government. Where the statue was a soviet symbol for the victory of the Red Army, to Estonians it was a symbol for the decades-long Soviet occupation. Protests turned into riots, resulting in one death, hundreds injured and many arrests. A day later, Estonia faced different kinds of cyberattacks that would last for weeks – the main type of attack being DDoS-attacks.[155] In such an attack a perpetrator seeks to make a network services unavailable by disrupting it through traffic flooding. Estonia pointed at Russia to be at least indirectly responsible for these attacks, based on network traffic of Russian language and due to political motivations. The Russian government denied any involvement but the attacks were accompanied by hostile political rhetoric by Russian officials, economic measures and refusal to cooperate with the Estonian investigation.[156] The event was branded to be the first country-to-country attack- and even war in cyberspace. Yet, the impact of the attacks was from a technical perspective only considered modest to low.[157]

The nature of the threat and referent object.

As discussed, the attacks have been branded 'Web War I' in the domestic and international press.[158] Yet, this narrative of cyberwar only emerged a while after the attacks since people first had to make sense of what happened. The first days of the cyber-attacks were marked by public confusion and uncertainty: the events were unexpected and unprecedented. There was little information available on the nature and origin of the attacks, and the media took a neutral tone towards the issue.[159] It was only after the events that this narrative shifted. On the 30th of April, Estonia's justice minister declared that investigations showed Russian involvement, be it indirectly.[160] With the detection of a spatial 'Other', the main

[154] Urmas Paet, (2007) 'Declaration of the Minister of Foreign Affairs of the Republic of Estonia'. *Republic of Estonia Website*. May 1st

[155] Stephen Herzog (2017). 'Ten years after the Estonian cyberattacks: Defense and adaptation in the age of digital insecurity' *Georgetown Journal of International Affairs*, 18(3), 68-69

[156] NATO STRATCOM COE (2019) '2007 cyber-attacks on Estonia' Thematic Report on Cyber operations, 53.

[157] Andreas Schmidt, 'The Estonian Cyber Attacks', 11.

[158] For example, Mark Landler and John Markoff (2007) 'In Estonia, what may be the first war in cyberspace.' *New York Times.* May 28; Joshua Davis (2007) 'Hackers Take Down the Most Wired Country in Europe'. *WIRED* aug. 21; BBC (2007) Estonia hit by 'Moscow cyber war'. BBC, May 17; Valentinas Mite (2007) 'Estonia: Attacks Seen As First Case Of 'Cyberwar'. *RFE/ RL.* May 30.

[159] Kari Alenius & M. Warren (2012). 'An Exceptional war That Ended in Victory for Estonia or an Ordinary e-Disturbance? Estonian Narratives of the Cyber-Attacks in 2007'. *The Institute Ecole Supérieure en Informatique Electronique et Automatique, Laval, France 5-6 July 2012*, 81.

[160] Alenius & Warren, 'An Exceptional war that ended in Victory for Estonia or an Ordinary e-Disturbance?', 81.

narrative started forming.[161] The discourse of cyberwar against the Russian enemy was accepted by ethnic Estonian audiences, as it resonated with the broader riot-context and discourses of national security and –identity.[162] The separate events of the riots and the cyber-attacks were discursively connected to create an imaginary of Estonia as a 'cyber frontier', a borderland between East and West, between ally and foe as well as a geographical referent for imagining virtual events.[163] While international actors initially repeated the cyberwar-narrative, they did not reproduce the enemy image as there was a lack of official evidence of Russian involvement.[164] The hypersecuritizing- 'war'-discourse later became more contested, due to a lack of physical, war-like consequences.[165] A temporal disruption of online banking services is difficult to be pictured as war, leading to statements like 'to be frank, in Estonia no one died'.[166] This did not mean that the idea of an impending cyber-threat was not taken seriously. Instead, the focus was placed on the vulnerability of cyberspace and on hackers as a threat, an anonymous entity for which the emphasis is placed on ethical boundaries rather than spatial ones.[167]

The construction of the militarized discourse of cyberwar therefore only emerged gradually and had limited efficacy.[168] Information infrastructures are ordinarily 'invisible', but come into visible focus when they become inoperable.[169] As an event, the attacks illustrated the present insecurity of cyberspace.[170] However, the attacks did not speak for itself due to a lack of materiality.[171]Although it produced some physical and noticeable effects, the total consequences were only visible to those with access and technical expertise. Further, the attribution problem of being unable to trace the perpetrator makes the interstate-war-narrative contestable.[172] In the absence of a deed that speaks for itself, the identity of the doer is inherently unstable: it is the terrorist act that gives a terrorist its identity and cyber-attacks need to be seen as war before the antagonist becomes a warring party.[173] The attacks were reliant upon official representations that signified it as 1) being an act and 2) constituting a threat.[174] This also has effects upon its representation, making the threat more reliant upon conventions and parasitic upon stable discursive contexts.[175] Historical analogies can serve as proxies for the lack of foundational events in discourses of cyberwar.[176] Thereby, official narratives connected the event to militarized discourses of war and terrorism.[177] The Estonian minister of foreign affairs stated that the 'cyber terrorists' attacks

[161] Ibid, 82.
[162] As described in the previous chapter, the Estonian identity strongly draws on the spatial Russian 'Other'.
[163] Savchecnko. 'E-Estonia Reprogrammed: Nation Branding and Children Coding', 215
[164] Hansen & Nissenbaum, 'Digital disaster'.
[165]Hansen & Nissenbaum, 'Digital Disaster', 1170; Mark Trevelyan (2008) 'Security experts split on 'cyberterrorism' threat'. *Reuters.* April 16.
[166] The Daily Mail. (2007) Attack of the Cyber Terrorists. *The Daily Mail.* May 28.
[167] Barnard-Wills & Ashenden, 'Securing Virtual Space', 119.
[168] Emerson, 'Limits to a Cyber Threat', 10.
[169] For example: if a laptop works, the mechanism producing this system is often invisible to the user. If it crashes, people become aware of its physical components and vulnerability. Stevens, *Cyber security and the politics of time*, 117-118.
[170] Ibid, 119.
[171] With materiality, detectable and visible consequences are meant. The attacks in itself do not speak for itself: if one person was unable to reach banking services, it does not inherently mean the country is under attack/ at war. There is a need for someone to collect information (someone with access and technical expertise) and represent them as being cyber-attacks. Emerson, 'Limits to a Cyber Threat', 6.
[172] David J. Betz & Tim Stevens (2011). *Cyberspace and the state: Toward a strategy for cyberpower*. London: The International Institute for Strategic Studies, 32.
[173] Emerson, 'Limits to a Cyber Threat', 6.
[174] Ibid, 5.
[175] Ibid, 13.
[176] Stevens, *Cyber security and the politics of time*, 144.
[177] Adrian Blomfield (2007) 'Estonia Calls For a NATO Strategy on 'Cyber-Terrorists' After Coming Under Attack' *The Daily Telegraph*, May 18.

[…] originated from specific computers and persons in Russian Government agencies'.[178] This terrorist-narrative was repeated by the chairman of Estonia's cyber-defense coordination committee,[179] and the Estonian defense minister called it 'a national security situation'.[180] In this way, the 'real' could be re-injected, annexing more stable material elements onto the cyber-threat.[181]

Estonian securitizing actors connected the threat to different referent objects including the state, political sovereignty and cultural or national identity. Governmental IT consultant Linnar Viik argued 'This is not some virtual world. This is part of our independence. And these attacks were an attempt to take one country back to the cave, back to the Stone Age'.[182] The attacks were connected to the survival of the Estonian 'Self'-identity as 'E-Estonia', with digital modernity serving as a factor for differentiating between Western Estonia and its Soviet past.[183] It thereby simultaneously invoked spatial and temporal identities: the attacks sought to disrupt progress and take the country back to its Soviet time. The threat was also linked to individual security by arguing that it disrupted the everyday practices of citizens.[184]

To conclude, the cyber-threat only came into being through being represented as such by Estonian officials. If the threat is to be viewed as a war or state-to-state attack, and connected to sovereignty, it is important to have a culpable 'Other' (state). To domestic audiences, the politically powerful but ultimately not easily detectable cyber-threat was easily blended and integrated into discourses of national security with the Russian Other.[185] To international audiences, i.e. NATO allies, this connection did not resonate. Without a defined spatial Other, the militarized cyberwar discourse was unstable and contested. [186]

Scaling Threat: the level of urgency

The level of urgency implied in the securitizing narrative can be placed on a scale.[187] It is reliant upon how 'radical' the differences between a Self and Other are shaped, and in this way creates the boundaries for acceptable action. For the cyber-threat, the level of urgency is mainly drawn in terms of temporal boundaries, often referring to future disaster. Ultimately, the attacks in itself became a 'sign', a connection between the discursive context of cyberwar and present day reality.

The severity of the attacks was constructed with the following argument: 1) cyberspace is inherently insecure and thereby referent objects are vulnerable. 2) the events proved that the threat was realistic, and the internet a battlefield in the present 3) the attacks were a warning for future impeding danger. It constructed cyberwar as a policy objective, and the attacks as a 'wake-up call'.[188] Estonian President Ilves stated that 'Estonia was attacked with a weapon and in a manner whose full significance is just beginning to dawn on the whole world in the 21st century'.[189] Defense minister Aavikso stated: 'what took place was according to our interpretation cyberwarfare and cyber terrorism. In essence, cyber-attacks against Estonia demonstrated that the Internet already is a perfect battlefield of the 21st century'.[190]

---

[178] Paet, 'Declaration of the Minister of Foreign Affairs of the Republic of Estonia'.

[179] Blomfield, 'Estonia Calls For a NATO Strategy on 'Cyber-Terrorists'.

[180] Hansen & Nissenbaum, 'Digital disaster', 1168-1169.

[181] Emerson, 'Limits to a Cyber Threat', 10.

[182] Hansen & Nissenbaum, 'Digital disaster', 1169.

[183] Idem.

[184] Idem.

[185] Savchecnko. 'E-Estonia Reprogrammed: Nation Branding and Children Coding' , 215

[186] Hansen & Nissenbaum, 'Digital disaster', 1169.

[187] Wilhelmsen, 'How does war become a legitimate undertaking?', 7.

[188] Kaiser, 'The Birth of Cyber War', 13.

[189] Thomas H. Ilves (2007) *President of the Republic on Victory Day,* 23 June 2007, in Rapla. President of the Republic of Estonia, Speeches, 23 June.

[190] Jaak Aaviksoo (2007). *Cyber defense: The unnoticed third world war.* Estonian Ministry of Defense Website commentary on cyber defense.

Urgency and severity were implied through iterating a discourse of war and terrorism. With a lack of foundational events, those catastrophic precedents can serve as signs through which a connection to weapons and nuclear war are made. In describing cyber-attacks, references were made to weapons, specifically nuclear ones.[191] A speaker of the Estonian parliament argued: 'When I look at a nuclear explosion and the explosion that happened in our country in May, I see the same thing'.[192] In this formulation, the Estonian attacks became a historical anchor itself, a foundational event grounding the construction of cyber security and –warfare.[193] By linking hacking to terrorism, cross-fertilization of discourses took place in constructing ethical boundaries. This link constructed hacking as dangerous and without legitimate political purpose.[194]

Representations of the threat also focused on boundaries between perpetrators and referent objects. Russia as the enemy-Other was described as sufficiently strong to take the threat as seriously and urgent, but not as too strong because this could result in defeatism.[195] The referent object, Estonia, was represented as victorious and Tech-savvy. In doing so, the Estonian Self was (re)defined: it was spatially opposed to the Russian Other including the Russian ethnic minority. Further, it stabilized its reputation as cyber-experts on the international level and thereby claimed authority.[196]

A way out: boundaries for acceptable action

The representation of the cyber-threat and the urgency implied in this construction places a responsibility on the referent object and securitizing actor to react. The narrative emphasized that these attacks were possible and probable in the future, meaning Estonians had to remain vigilant and develop their capacities in cyber defense.[197] If the event was a war and a permanent new threat, there is also a call for military response.

Following the two competing narratives, Russia as a concrete threat versus the anonymous, inherently insecure nature of cyberspace created, different measures become logical and legitimate. First, a discourse focusing on (cyber) war with an antagonistic state creates the attacks as existential and thereby most radical. In constructing it as a problem of national security, military solutions (retaliation/ militarization) become logical. Secondly, if the attacks made visible the inherent vulnerability and threat of cyberspace, in which perpetrator and method are unknowable, long term anticipatory solutions are logical. An example of this is building resilience (under whole society and therefore also individual responsibility) and preparedness, but also solutions are found in international cooperation.

The call to action was mainly directed at international allies: to gain support from the EU and NATO.[198] The Estonian prime minister argued: 'we expect from the European Union a straightforward reaction to the well-coordinated attacks of Russia'. [199] NATO did not invoke Article 5 due to institutional constraints: at the time, there were no formal norms or protocols for situations of cyberwar and security. As Aviksoo complained: 'at present, NATO does not define cyber-attacks as a clear military action'.[200]

Discussion

Similar to the conclusions made by Hansen and Nissenbaum, this chapter finds that the efficacy of building the cyber-threat was limited. Although the cyber-threat image was taken seriously, the 'cyber-

[191] Stevens, *Cyber security and the politics of time*, 145-146.
[192] Myriam Dunn Cavelty (2013) 'From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. International Studies Review 15, 117.
[193] Stevens, *Cyber security and the politics of time*, 145-146.
[194] Hansen & Nissenbaum, 'Digital Disaster', 1171.
[195] Alenius & Warren, 'An Exceptional war that ended in Victory for Estonia or an Ordinary e-Disturbance?', 82.
[196] Kaiser, 'The birth of cyberwar', 15.
[197] Alenius & Warren, 'An Exceptional war that ended in Victory for Estonia or an Ordinary e-Disturbance?', 84.
[198] North Atlantic Treaty Organization. (1989). *The North Atlantic Treaty Organization : facts and figures. Brussels :NATO Information Service*, Article 5.
[199] Andrus Ansip (2007) *Prime Minister Andrus Ansip's speech in Riigikogu, 2. May*. Published at the government website: https://www.valitsus.ee/en/news/prime-minister-andrus-ansips-speech-riigikogu
[200] Ian Traynor. (2007) 'Russia Accused of Unleashing Cyberwar to Disable Estonia'. *The Guardian*, May 17.

attacks-as-war' discourse was more contested. The material event and its physical consequences were not considered severe enough to be an existential threat, an act of violence or warfare in itself. The initial cyberwar narrative was unstable and thereby not fully accepted. Fist, this was due to the fact that the cyber-threat only came into being through representation: there was no easily visible material effect or historical precedent for the event to speak for itself.[201] Second, the attribution problem makes representations of the attack contestable.[202] If Estonia had succeeded in presenting Russia as the perpetrator, the attacks could be connected to the broader context of the riots and to political motivations. This would make the cyberwar discourse more stable, and legitimize invoking NATO's Article 5 for collective defense.

The performative enactment of cyber-attacks as a realistic and imminent threat, and cyberspace as inherently vulnerable, was less contested.[203] This hyper securitization, a future oriented argument, heavily relied upon references to established conventions or -security threats. This narrative constructed a need for cyber security and societal resilience to counter a cyberspace that is inherently filled with threatening actors and threats to both the state and individual.[204] In this narrative, the attacks were considered a 'sign' or a wake-up call for the inevitability of future and present doom that a real cyberwar would be. The competing narratives thereby constructed boundaries for what was considered a sensible response to the threat: either by anticipating (waking up) and preparing the country to it, or by more direct military action. The securitizing narrative created responsibilities for the West, the Estonian state and for the individual. The next chapter sets out how this discourse materialized into securitizing practices, and how these in turn transmitted, (re)produced and influenced the threat identity in the securitizing argument.

[201] Emerson, 'Limits to a Cyber Threat', 6.
[202] Ibid, 14-15.
[203] Hansen & Nissenbaum, 'Digital Disaster', 1171.
[204] Barnard-Wills & Ashenden, 'Securing Virtual Space'.

Chapter 6: The Militarization of Cyber Security

'The Cyber Unit's mission is to protect Estonia's high-tech way of life, including protection of information infrastructure and supporting broader objectives of national defence'.[205]

As the previous chapter showed, the attacks were represented as a cyberwar. Yet, this narrative was initially not fully accepted. This chapter will argue that the militarization of the cyber-threat did emerge, but only gradually through securitizing practices that materialized cyberwar. The attacks, and its discursive representation, moreover became a sign in the cyber security imaginary. It became a material referent and foundational event ready to be iterated in new securitizing moves. This chapter will thereby analyze the securitizing practices that emerged in Estonia. These practices (re)produce the cyber-threat, and specifically the militarized cyberwar-discourse. Through this iteration and institutionalization, the discourse of cyberwar stabilized. Therefore it is not only the case that a securitizing narrative legitimizes the 'emergency measure', but that the 'emergency measures' are a constituent part of the threat narrative itself.[206] Put differently, instead of only being a reflection of the securitizing argument, securitizing practices enact it: they can retroactively produce meaning to the identity of the cyber-threat.[207]

This chapter focuses on the sub-question of how the securitizing narrative has materialized in policies, institutions and actions. It will look at how the securitizing narrative legitimizes existing security practices, and how these are changed to include tackling the cyber-threat as an objective. Securitizing practices, following the theoretical framework, are here understood as either associated with security practice (military) or new, as in never applied to this issue before. The practices studied are grouped into three categories: 1) policies, strategies and laws, 2) institutions and organizations, and 3) practices as patterned actions. The focus will be placed on how these securitizing practices confirm (or contradict) the identity constructions made in the securitizing narrative. First, it will discuss how Estonia created- and was able to disseminate cyber norms in the form of strategies, policies and laws. It will argue that the securitizing move granted the country a form of authority and a reputation of expertise that enabled them to speak. Secondly, it will look at how spatial boundaries between the West and East as well as ethnic Estonians and ethnic Russians were enacted in the formalization of international cooperation and the institutionalization of civic participation. These military organizations specifically perform the war discourse. Finally, it will look at how temporal construction of an inevitable future cyber-doom becomes performed through practices of anticipation. This includes building a resilient society as well as literally performing the future in exercises and simulations. This chapter will thereby show that the securitizing narrative legitimized security practices, which in turn (re)produced and strengthened the securitizing discourse. It will show how cyber security became an issue of the state and military.

Boundaries for acceptable action: legitimization of security practices

As discussed in the previous chapter, the different securitizing narratives create boundaries for acceptable, sensible and legitimate action. A militarized discourse of cyberwar allows for military responses. A securitized discourse of the cyber-threat, in which boundaries are less radical due to the lack of a material Other, would logically lead to less radical measures. The weakness of the cyberwar discourse was not only reflected in discussions, but also in the type of response seen as legitimate. The call for the invocation of Article 5 was not accepted, it was seen as too radical and not as legitimate. To Hansen & Nissenbaum this indicated that the securitization was only partially successful.[208] However, from the framework of performative securitization, the focus is placed on what a securitizing move has added and how this changes the conditions of possibility. In the case of the cyber-attacks, the

[205] Website 'Estonian Defence League Cyber Unit', retrieved at 03-08-2020 from: https://www.kaitseliit.ee/et/kuberkaitse-uksus
[206] Emerson, 'Limits to a Cyber-Threat'.
[207] Ibid, 13.
[208] Hansen & Nissenbaum, 'Digital Disaster', 1170.

securitizing narrative constructed cyberspace as a threat, be it not necessarily an existential one. As a new security threat, it created a need for state-involvement in cyber security. To ethnic-Estonian audiences, where the cyberwar discourse was less contested, it even legitimized militarized responses as will be shown in this chapter.

Creating ethical boundaries: norm-setting and policymaking

The failed attempt of Estonian securitizing actors to mobilize NATO allies in collective defense was partially due to a lack of (formal) norms, protocols and policies in response to cyberwar. Estonia was represented as being one of the only countries to have experienced (and to have been victorious in) cyberwar. This granted them authority to speak security, to promote norms and to influence international legislation.[209]

Estonia's goals for promoting cybersecurity norms include supporting a liberal and open cyberspace and to create laws and policies on how to establish responsibility in the case of state-to-state attacks.[210] The Estonian government promoted these cyber norms domestically, being the first to produce a national cybersecurity strategy in 2008.[211] This strategy focused on building capabilities and resilience, but also on creating international legal norms, cooperation and raise international awareness. Estonian securitizing actors and strategies later influenced NATO and EU policies and strategies.[212] The focus in NATO-cyber security- documents shifted from being preoccupied with protecting their own critical infrastructure or communication systems, to assisting Allies with protection'.[213] Formal legal norms were enacted through the Tallinn Manual, a document informing international laws for cyberwarfare and -security. Although this document is non-binding, it is one of the most cited papers in international courts.[214] In domestic legal provisions, the discourse of cyberwar became part of the Penal Code through amendments. Formerly, the code only mentioned cybercrime, whereas it now differentiated acts of cyber-terrorism or attacks to the critical infrastructures of a country, attacks with a political aim.[215] Estonian legal structures have further influenced and shaped international cyber law.[216] The norms established ethical boundaries between practices of the good (cyber security) and the bad (hacking). Its focus on open and free internet reflected western liberalist values as well as its international orientation. Cyber security sounds a-political but is normative, it is a *technified* discourse.[217] In practice, cyber security for one is insecurity for the Other: building cyber capabilities might create a threat abroad.[218] When the securitizing argument was launched, Estonia was empowered to act and legitimately undertake policies. Cyber security norms were enacted in laws and strategies in Estonia itself, documents that became material grounds that strengthened the securitizing narrative and the cyber-norms. Thereby Estonia was able to internationally disseminate its legal framework for dealing with cyberwar. The norms, strategies and policies further materialized and became enacted within institutions that simultaneously stabilized the spatial identities.

---

[209] Crandall & Allan, 'Small States and Big Ideas', 352.
[210] Ibid, 352-353.
[211] Ibid, 353.
[212] Kaiser, 'The birth of cyberwar', 16.
[213] Idem.
[214] Michael N. Schmitt (2013) *Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence*, 16.
[215] Herzog , 'Ten Years after the Estonian Cyber-attacks', 71.
[216] Ibid, 72.
[217] Hansen & Nissenbaum, 'Digital Disaster', 1167-1168.
[218] Myriam Dunn Cavelty (2014), 'Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities', Science and Engineering Ethics 20, no. 3: 701–15; Stevens, *Cyber Security and the Politics of time*, 9.

Reproducing spatial boundaries: institutionalization

The spatial boundaries between the West, Estonia and Estonianness versus Russia and Russianness materialized through the formation of alliances, institutions and organizations of cyber security. As its national strategy proposed, Estonia called for international cooperation in cyber security and envisioned a central role for itself in it. The strategy posed that: 'Owing to Estonia's unique experience in dealing with cyber-attacks in the spring of 2007 and subsequent policy initiatives, the international community expects a major contribution from us (…) more extensive participation in international organizations is vital to ensuring recognition of the problems of cyber security'.[219]

In this way, Estonia reproduced its own Self-identity as a Western and modern country with cyber-expertise and discursively constructed a Western cyber security alliance. Before- and at the time of the attacks, Estonia's international cooperation in cyber security was informal and limited. Although article 5 was not invoked, NATO, the EU and the US send cyber security teams to help respond to the attacks.[220] Estonian securitizing actors demanded that NATO clarified its position on cyberwar and how it would assist member states in cyber defense.[221]

In 2008, the NATO CCDCOE in Tallinn opened: a military organization focusing on cyber security research, consultancy and training. This center formalized international military cooperation and the exchange of expertise on cyber security. Its establishment was already planned prior to 2007, but was met with resistance. The center lacked funding and investments that it needed from the Estonian state, because cyberwar was not perceived as a serious threat at the time.[222] The securitizing discourse of cyberwar around the attacks consolidated, legitimized and accelerated the establishment of the center. The Center makes Tallinn a central hub for the community of Western cybersecurity practitioners, as well as confirms Estonia's claims to expertise and cyber-defensive capabilities.[223] This allowed Estonian experts to take on leadership roles in international institutions, such as NATO's Cyber Defense Management Authority (CDMA).[224]

The cyber security strategy did not only call its international allies to responsibility, but also mobilized individual responsibility of Estonian citizens. This is enacted and institutionalized within the Cyber Unit of the Estonian Civil Defense League. This Cyber Unit, established directly after the attacks, exists out of volunteers that are trained to fend of future attacks.[225] This league mobilizes private sector ICT specialists, and young people interested in cyber security. As featured in the quote at the start of this chapter, the unit's self-pronounced aim is to protect the Estonian way of life and contribute to national defense.[226] The organization enacts the narrative of whole of society defense: because the cyber threat does not only affect the state, but also the way of life or everyday practices of Estonian citizens they share responsibility to counter it. There has therefore been an institutionalization of the spatialized identity of the cyber-threat, i.e. military organizations have been established or adapted to prepare for cyber-tacks. This war discourse confirms boundaries between the West and the Other, the illegitimate and malicious hacker/ Russian antagonist. These organizations also enact the temporal identity of the cyber-threat: they recruit, prepare and train for future doom scenario's.

[219] Kaiser, 'The birth of cyber war', 15.
[220] Hansen & Nissenbaum, 'Digital disaster', 1170.
[221] Kaiser, 'The birth of cyber war', 15.
[222] Idem.
[223] Ibid, 16.
[224] Stephen Herzog, 'Ten Years after the Estonian Cyberattacks', 73.
[225] Ibid, 70.
[226] Website 'Estonian Defence League Cyber Unit', retrieved at 03-08-2020 from: https://www.kaitseliit.ee/et/kuberkaitse-uksus

Temporal boundaries: practices of anticipation

Temporal boundaries are reproduced through practices of anticipation. Anderson (2010) defines anticipation as a 'performative process of rendering the future actionable' in the present.[227] In preparing for future cyberwar, a central debate focused on deterrence versus resilience.[228] The first, which is prominently featured in policy statements and military doctrine, is difficult in the case of cyberwar. Deterrence, as well as prevention, are reliant upon knowable antagonists and objective measurability of the threat.[229] As discussed in the previous chapter, a cyber-threat is unknowable and uncertain. The cyber-threat is constructed as being a constant and inherent risk. This leads cybersecurity practitioners to focus on a different anticipatory strategy, a strategy of imagining and enacting a variety possible doom scenario's and then plan for those.[230] In preparing for uncertain futures, creating resilience through anticipatory action is the most used strategy.

Anticipatory practices bring the future into the present as something that can be experienced and allow people to imagine and rehearse these probable futures.[231] An example of such practices are simulations and military exercises. Existing military exercises were either extended to include cyber security elements or cyberwar was simulated in the form of separate exercises. These exercises either focus on future doom, possible doom scenarios without precedent, or they reproduce past events, such as the Estonian attacks.[232] Cyberwar-exercises are precautionary as they enact an imaginary of how bad cyberwar can and will be.[233] The Estonian attacks are reiterated within the cyber security imaginary that is performed in these exercises. [234] It reproduces boundaries between allies and enemy Others, as in most exercises, Russia and China take the role of the aggressor.[235] Thereby, the cyberwar- narrative is reproduced and performed in the imaginaries of generations of NATO soldiers. Finally, exercises also reproduce present vulnerabilities. Those participating in these exercises actively search for weak spots and thereby create them: an insecure spot in digital infrastructure only discursively exists if it is identified.[236]With the growing emphasis on raising awareness, these cyber exercises and simulations are often communicated to the public. In this way exercises materialize the virtual by demonstrating the possible effects of cyber-attacks.[237]

As a further anticipatory strategy, states might build resilience by populating cyber security futures, using tactics of recruitment and education.[238] It is a way of populating the future in a literal way with cyber security personnel and of delegating responsibility for security to citizens.[239] In Estonia, the government had already invested heavily in training its youth, and citizens in ICT related skills through the Tiger Leap Foundation.[240] This state-funded institute provides cross-sectoral training and workshops and aims to raise awareness.[241] The newly formed institutions discussed at the start of this chapter are important in educating, training and research on future cyber-attacks. The CCDCOE operates as a training and research organization, focused on elite actors. It produces its own research, operates as a hub for exchanging expert knowledge and acts as consultant to governments of member countries.[242]The

[227] Ben Anderson (2010). 'Security and the future: anticipating the event of terror'. *Geoforum*, 41(2), 229.
[228] Kaiser, 'The Birth of Cyber War', 17.
[229] idem.
[230] Ibid, 16.
[231] Stevens, *Cyber security and the politics of time*, 176.
[232] Ibid, 153.
[233] Kaiser, 'The Birth of Cyber War', 18.
[234] idem.
[235] Idem.
[236] Stevens, *Cyber security and the politics of time*, 151.
[237] Ibid, 153.
[238] Ibid, 166.
[239] Ibid, 176.
[240] Herzog, 'Ten Years after the Estonian Cyberattacks', 72.
[241] Idem.
[242] Kaiser, 'The Birth of cyberwar', 16.

Cyber Unit mobilizes and recruits civil society and trains individuals for future cyber-attacks to the country.[243]

Discussion

The cyber-threat is not only constituted through discursive practices, but is also performatively enacted through policies, institutions and physical actions.[244] These responses to the threat, in the form of institutions and policies, become material basis for the threat that the cyber-attack in itself lacked.[245] The securitizing practices, or extraordinary measures that emerged in Estonia after 2007 (re)produced the ethical, spatial and temporal elements of the cyber-threat-identity. Instead of being a separate sequence of a discursive event, or securitizing move, to a securitized response, these processes are entwined and together produce the cyber threat and security sector.[246] The materiality of the response is retrospectively re-injected in the virtual threat, becoming the material basis for a discourse of cyberwar and thereby overcoming the limits discussed in the previous chapter.[247] The practices of norm-setting, cooperation or institutionalization and anticipation enact the securitizing narrative of the cyber-threat and cyberwar. The securitizing narrative was made visible through these practices, institutions and policies, reinforcing over time the idea of the cyber-threat as realistic and imminent.[248] These securitizing practices iterate the cyberwar narrative and thereby make the securitizing move effective and stabilize the discourse.

[243] Website 'Estonian Defence League Cyber Unit', retrieved at 03-08-2020 from: https://www.kaitseliit.ee/et/kuberkaitse-uksus
[244] Emerson, 'Limits to a cyber-threat', 14.
[245] Idem.
[246] Ibid, 13.
[247] Ibid, 14.
[248] Wilhelmsen, *Russia's securitization of Chechnya*, 164.

Conclusion

Has there been a case of the securitization of cyberspace, or did conflicts become cyberized? This thesis positions itself within ongoing debates surrounding the politics of cyber security, the theory of securitization and finally in the debate surrounding the case of Estonia. Although in academic circles and in the international press there is a consensus that the attacks could not be branded as a war,[249] there was something going on in the country. There is a visible militarization of cyberspace, and cyber security is seen as integral to conceptions of national security.[250] If cyber war was not real, why did citizens and institutions in Estonia behave like it was?

The concept of cyberwar is in this thesis understood as a discursively constructed entity in which the security or –defense of cyberspace becomes an issue of the state and military. The construction of the 'cyber-threat' has often been studied using the framework of securitization theory. Yet, in its original CoS version, this framework is not able to capture the dynamic nature of meaning construction. Using a post-structuralist discourse analysis, the original theory is amended and used to answer the following research question: *How has a securitizing discourse on cyber threats legitimized the militarization of cyberspace in Estonia after the country experienced cyber-attacks in 2007?*

This question has been broken up into its constituent parts, in two processes implied in the question: discourses that legitimate military practices, but also a process of militarization in itself. Legitimation is studied by analyzing representations of the threat to a referent object, the degree of urgency and existentialism implied in this construction and finally by looking at the call to action: how should the threat be countered? The study of militarization implies looking at material securitizing practices that confirm and (re)produce the discourse of a cyber-threat. Although the parts are separated for analytical purposes, they are in reality intertwined and co-constitutive.[251]

In Estonia, two competing threat narratives emerged. The first connected the cyber threat to the broader security context in Estonia: the riots and the Russian enemy-Other. This made the attacks an act of war, and thereby constructed a discourse of cyberwar. Yet, the spatial boundary constitutive of this war-discourse was unstable and contested. Simultaneously, a discourse developed that emphasized the inherent insecure nature of cyberspace, using the cyber-attacks as a sign and warning of potential danger coming from faceless, malicious hackers. This narrative, however, constructed it as just that: a threat and security issue but nothing like a war. The way in which the cyber-threat was represented shaped the responses that logically followed. At this point in the story, conclusions drawn are not radically different from those of Hansen & Nissenbaum: the cyberwar discourse was not fully accepted, and therefore the most radical, extraordinary measures refuted.[252] Yet, the story does not end here.

This thesis understands the attacks as a catalyzing event, an event that became a sign or code that could be cited in future debates and securitizing moves. It provided these discussions with a more or less concrete, material referent and fueled the imaginations of what kind of threat cyber-space could be in the future. It further led to the acceptance of cyber as a threat that could be political, and therefore of interest of the state. In turn, the state began to develop practices of cyber security – be it in the shape of military/ defense or not. These visible manifestations of the cyber-threat in turn inject the cyber-threat imaginary with material grounds that help stabilize the discourse of cyberwar.[253]

Each time the cyber-threat narrative, constructed in securitizing moves following the 2007 cyber-attacks, is reiterated the conditions of possibility for new securitizing moves. Performative securitization is thereby a gradual iterable process of meaning construction. It is able to account for how

[249] Hansen & Nissenbaum, 'Digital Disaster', Valeriano & Maness, Thomas Rid, 'Cyber War Will not Take Place'; Gartzke, E. (2013). 'The myth of cyberwar. Bringing war in cyberspace back down to earth'. *International Security,* 38, 41–73

[250] Veebel & Ploom, 'Estonian perceptions of security: not only about Russia and the refugees', 55.

[251] Wilhelmsen, *Russia's securitization of Chechnya, 37-38.*

[252] Hansen & NIssenbaum, 'Digital Disaster', 1170-1171.

[253] Emerson, 'Limits to a Cyber-Threat', 15.

even securitizing moves that seem to fail add something to the discourse. In a framework of performative securitization, studying an event or speech act in itself does not make sense. It is through repetition that securitizing discourses are constituted. Finally, the iterative process of security also had effects on conceptualizations of what is considered to be national security in the country, now also including cyber security. The contradiction between securitization of cyberspace and cyberization of conflict, that constitutes the title of this thesis, therefore is a false one. Instead of either, the discourses of cyber security and military discourses of war are blended and are co-constitutive of the discourse of cyberwar and the militarization of cyber security. Far from being unreal, cyberwar is a discursively constructed imaginary and experienced as such in Estonia.

Finally, it is important to reflect upon the limitations of the research project as well as to identify gaps that could inform future research. As this thesis looks at the case from a holistic perspective: it looks at securitization over an extended time period and focuses on many different discursive acts. It thereby does not claim or aim to have covered all elements, speech acts or practices that have taken place during this time period. The sources used are mainly secondary literature and some English language primary texts. Because the case has been thoroughly covered and documented, this was possible in the first place. Yet, the study of practices as well as linguistic texts would always be better with more material. In this research, limits were posed due to a language barrier, the impossibility of fieldwork and in this way interviewing Estonians and observing practices, and due to the scope and time limit of this research project. The study would be enriched through anthropological methods or content analysis.

The fact that this thesis chose to take a holistic view, always opens up the road for future research. Scholars could for example focus at one of the different constituent parts of the framework and its (power) dynamics. This could include looking at it from a different scale: how do different securitizing actors compete to claim authority, how are different professionals assembled within for example the cyber unit to tackle the threat or what voices have been silenced such as perhaps those of ethnic Russians in the country.[254] It could also be interesting to look at how the cyber-threat and cyberwar are imagined and experienced by Estonian citizens in their everyday life, for which an anthropological approach would be more suitable.

.

[254] Sara Bertrand (2018). Can the subaltern securitize? Postcolonial perspectives on securitization theory and its critics. *European journal of international security*, *3*(3), 281-299. Lene Hansen, L. (2000). The Little Mermaid's silent security dilemma and the absence of gender in the Copenhagen School. *Millennium*, *29*(2), 285-306.

References

Adler, E., & Pouliot, V. (Eds.). (2011). *International practices* (Vol. 119). Cambridge University Press.

Alenius, K., & Warren, M. (2012). An Exceptional war That Ended in Victory for Estonia or an Ordinary e-Disturbance? Estonian Narratives of the Cyber-Attacks in 2007. *The Institute Ecole Supérieure en Informatique Electronique et Automatique, Laval, France 5-6 July 2012 Edited by*, 18.

Anderson, B. (2010). 'Security and the future: anticipating the event of terror'. *Geoforum*, 41(2), 227-235.

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

Austin, JL (1962) *How to Do Things with Words.* Oxford: Clarendon Press.

Balzacq, T. (2005). 'The three faces of securitization: Political agency, audience and context', *European journal of international relations*, *11*(2), 171-201.

Balzacq, T. (Ed.). (2010). *Understanding securitisation theory: How security problems emerge and dissolve*. Routledge.

Balzacq, T., S. Léonard & J. Ruzicka (2016). 'Securitization' revisited: theory and cases'. *International relations*, *30*(4), 494-531.

Barnard-Wills, D. & D. Ashenden (2012) 'Securing Virtual Space: Cyber War, Cyber Terror, and Risk'. *Space and Culture*, 15(2) 110-123.

Bertrand, S. (2018). Can the subaltern securitize? Postcolonial perspectives on securitization theory and its critics. *European journal of international security*, *3*(3), 281-299.

Betz, D., & Stevens, T. (2011). *Cyberspace and the state: Toward a strategy for cyberpower*. London: The International Institute for Strategic Studies.

Bigo, D. (2002). 'Security and immigration: Toward a critique of the governmentality of unease'. *Alternatives: Global, Local, Political*, 27, 63–92.

Bonacker, T. (2018) 'The militarization of security: a systems theory perspective'. *Critical Military Studies.*

Bourbeau, P. (2014). 'Moving forward together: Logics of the securitization process'. *Millennium*, *43*(1), 187-206.

Bourbeau, P. (2017). Migration, exceptionalist security discourses, and practices. In *Handbook on Migration and Security*. Edward Elgar Publishing.

Bueger, C. (2016). Security as practice. *Routledge Handbook of Security Studies, 2nd edn, Abingdon: Routledge*, 126-135.

Bueger, C., & F, Gadinger (2018). *International practice theory*. Basingstoke: Palgrave Macmillan.

Buzan, B., O. Wæver & J. De Wilde (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers.

Cavelty, M. D. (2007). *Cyber-security and threat politics: US efforts to secure the information age*. Routledge.

Cavelty, M. D. (2008). 'Cyber-terror—looming threat or phantom menace? The framing of the US cyber-threat debate'. *Journal of Information Technology & Politics*, *4*(1), 19-36.

Cavelty, M. D., & Holloway, L. (2018). 'Cyber threats in Popular Visual Culture'. *The Polish Journal of the Arts and Culture. New Series*, *2018*(7 (1/2018)), 7-28.

Cavelty, M.D. & Wenger, A. (2020) 'Cyber security meets security politics: Complex technology, fragmented politics, and networked science'. *Contemporary Security Policy* 41.1: 5-32.

Cavelty M.D (2020) 'Cybersecurity between hypersecuritization and technological routine'. E. Tikk & M. Kerttunen (ed.) *Routledge handbook of international cybersecurity*, Routledge, 11-21.

Clarke, R.A. & R.K. Knake, (2010) *Cyber War: The Next Threat to National Security and What To Do About It*. New York, NY: Ecco.

Crandall, M. & Allan, C. (2015) 'Small States and Big Ideas: Estonia's Battle for Cybersecurity Norms', *Contemporary Security Policy*, 36:2, 346-368.

Collier, J. (2018). 'Cyber security assemblages: A framework for understanding the dynamic and contested nature of security provision'. *Politics and Governance*, 6,13–21.

Côté, A. (2016). Agents without agency: Assessing the role of the audience in securitization theory. *Security Dialogue*, *47*(6), 541-558.

Deibert, R. (2017). 'Cyber security'. In M. D. Cavelty and T. Balzacq (Eds.), Routledge handbook of security studies (2nd ed., pp. 172–182). New York, NY: Routledge.

Demmers, J. (2017) *Theories of Violent Conflict: an Introduction*, 2nd ed. Routledge: London & New York.

Emerson, R. G. (2016) 'Limits to a cyber-threat', *Contemporary Politics. Vol. 22, no: 2,* 178-196.

Emerson, R. G. (2017). 'Towards a process-orientated account of the securitisation trinity: the speech act, the securitiser and the audience'. *Journal of International Relations and Development*, 1-17.

Fairclough, N. (2001). Critical discourse analysis as a method in social scientific research. *Methods of critical discourse analysis*, *5*(11), 121-138.

Färber, K. (2018) 'The Absence of Methodology in Securitization Theory'. In *E-International Relations,* 1-19

Flyktman, J., A. Huhtinen & L. Koreman (2020) 'Information Operations (Chapter 13)'. *Routledge Handbook of International Cybersecurity.*

Gartzke, E. (2013). 'The myth of cyberwar. Bringing war in cyberspace back down to earth'. *International Security*, 38, 41–73

Gomez, M. A. N. (2016). 'Arming Cyberspace: The Militarization of a Virtual Domain'. *Global Security and Intelligence Studies*, *1*(2), 5.

Hansen, L. (2000). The Little Mermaid's silent security dilemma and the absence of gender in the Copenhagen School. *Millennium*, *29*(2), 285-306.

Hansen, L. (2006) *Security As Practice : Discourse Analysis and the Bosnian War*, Taylor & Francis Group.

Hansen, L. & H. Nissenbaum (2009). 'Digital disaster, cyber security, and the Copenhagen School'. *International studies quarterly*, *53*(4), 1155-1175.

Herzog, S. (2017) 'Ten Years after the Estonian Cyberattacks: Defense and Adaptation in the Age of Digital Insecurity.' *Georgetown Journal of International Affairs*, vol. 18, no. 3: 67-78.

Huysmans, J. (2006). *The politics of insecurity. Fear, migration and asylum in the EU*. London: Routledge.

Huysmans, J. (2014). *Security unbound: Enacting democratic limits*. Routledge.

Jabri, V. (1996). *Discourses on violence: Conflict analysis reconsidered*. Manchester University Press.

Jackson, P. T. (2006). *Civilizing the enemy: German reconstruction and the invention of the West*. University of Michigan Press.

Jørgensen, M. W., & Phillips, L. J. (2002). *Discourse analysis as theory and method*. Sage.

Kaiser, R. (2015), 'The Birth of Cyberwar', *Political Geography*, Vol. 46 No. C, pp. 11-20.

Kattel, R. & I. Mergel (2019) 'Estonia's Digital Transformation: Mission Mystique and the Hiding Hand' in Mallory E. Compton & Paul 't Hart (ed.) *Great Policy Successes.* Oxford University Press, Oxford.

Kello, K. (2017) 'Identity and Othering in Past and Present: Representations of the Soviet Era in Estonian Post-Soviet Textbooks', *Journal of Social and Political Psychology* Vol. 4 (2), 665-693.

Kello, L. (2013). 'The meaning of the cyber revolution: Perils to theory and statecraft'. *International Security*, 38, 7–40.

Klüfers, P. (2014). 'Security repertoires: Towards a sociopragmatist framing of securitization processes'. *Critical Studies on Security*, *2*(3), 278-292.

Kremer, J. F., & Müller, B. (Eds.). (2013). *Cyberspace and international relations: Theory, prospects and challenges*. Springer Science & Business Media.

Kuus, M. (2002). 'European integration in identity narratives in Estonia: A quest for security'. *Journal of peace research*, *39*(1), 91-108.

Kuus, M. (2004). '"Those Goody-Goody Estonians": Toward Rethinking Security in the European Union Candidate States'. *Environment and Planning D: Society and Space*, 22(2), 191–207.

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

Léonard, S. (2010). 'EU border security and migration into the European Union: FRONTEX and securitisation through practices', *European Security*, 19:2, 231-254.

Léonard, S. & C. Kaunert, (2011). 'Reconceptualizing the audience in securitization theory', in Thierry Balzacq (ed.), *Securitization Theory: How Security Problems Emerge and Dissolve* (London: Routledge, 2011), pp. 57–76.

Léonard, S., & Kaunert, C. (2019). 'A new securitization framework' (Chapter 1) in *Refugees, security and the European Union*. Routledge. 14-40

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

McDonald, M. (2008) Securitization and the Construction of Security. *European journal of international relations*, *14*(4), 563-578.

McInnes, C., & S. Rushton (2013). HIV/AIDS and securitization theory. *European Journal of International Relations*, *19*(1), 115-138.

Muiznieks, N., J. Rozenvalds & I. Birka (2013) 'Ethnicity and social cohesion is post-Soviet Baltic States'. *Patterns of Prejudice*. Vol. 47 (3), 288-308.

Munk, T. H. (2015). *Cyber-security in the European Region: Anticipatory governance and practices*. The University of Manchester (United Kingdom).

Peoples, C. & N. Vaughan-Williams (2014). *Critical security studies: An introduction*. Routledge.

Philipsen, L. (2018). 'Performative securitization: from conditions of success to conditions of possibility'. *Journal of International Relations and Development*, 1-25.

Pretorius, J. (2008). 'The security imaginary: Explaining military isomorphism'. *Security Dialogue*, *39*(1), 99-120.

Ragin, C. C., & Amoroso, L. M. (2019). *Constructing social research: The unity and diversity of method*. Pine Forge Press (3rd ed.).

Raun, T. (1994). 'Post-Soviet Estonia, 1991-1993'. *Journal of Baltic Studies*, *25*(1).

Rid, T. (2013) *Cyberwar Will Not Take Place*. London: Hurst.

Salminen, M., & M. Kerttunen (2020). 'The becoming of cyber-military capabilities'. In *Routledge Handbook of International Cybersecurity* (pp. 94-107). Routledge.

Savchecnko, D. (2019) 'E-Estonia Reprogrammed: Nation Branding and Children Coding (Chapter 8.) in M. Biagioli & V.A.Lépinay (ed.) *From Russia with Coe: Programming Migrations in Post-Soviet Times.* Duke University Press. 213-228.

Sbisà, M. (2002). 'Speech acts in context'. *Language & Communication*, *22*(4), 421-436.

Schmidt, B., & I. Schröder, (2001). *Anthropology of violence and conflict*. Psychology Press.

Schmitt, M. N. (2013) *Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence*.

Shires, J. (2020). ‘Cyber-noir: Cybersecurity and popular culture’. *Contemporary Security Policy*, *41*(1), 82-107.

Singer, P. W., and A. Friedman (2013) *Cyberwar and Cybersecurity: What Everyone Needs to Know.* Oxford: Oxford University Press.

Stengel, F. A. (2019). ‘Securitization as Discursive (Re) Articulation: Explaining the Relative Effectiveness of Threat Construction’. *New Political Science*, *41*(2), 294-312.

Stevens, T. (2016). *Cyber security and the politics of time*. Cambridge University Press.

Stritzel, H. (2007). ‘Towards a theory of securitization: Copenhagen and beyond’. *European journal of international relations*, *13*(3), 357-383

Stritzel, H. (2014). *Security in translation: Securitization theory and the localization of threat*. Palgrave Macmillan, London.

Taampuu, P., K. Seppel & K. Simm, (2019) ‘Appropriation of the Nordic brand in the Estonian political discourse 1997-2017: consistencies and contestations’ (Chapter 15). *The Nordic Wave in Place Branding.* Edward Elgar Publishing, 191-206.

Taylor, C. (2004). *Modern social imaginaries*. Duke University Press.

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

Vigneau, E. (2019). Securitization theory and the relationship between discourse and context: A study of securitized migration in the Canadian press, 1998-2015. *Revue europeenne des migrations internationales*, *35*(1), 191-214.

Vuori, J. (2017) ’Chapter 6: Constructivism and Securitization Studies’ in Dunn Cavelty and Balzacq (ed.) *Routledge Handbook of Security Studies*. 2nd ed. Routledge, NY, 64-65.

Wæver, O. (1993). *Securitization and desecuritization* (p. 48). Copenhagen: Centre for Peace and Conflict Research.

Wæver, O. (2003) *Securitisation: Taking stock of a research programme in Security Studies.* Unpublished manuscript.

Walker, R. B. (1990). Security, sovereignty, and the challenge of world politics. *Alternatives*, *15*(1), 3-27.

Wilner, A. (2019). ‘US cyber deterrence: Practice guiding theory’. *Journal of Strategic Studies.*

Wilhelmsen, J. (2016) ‘How does war become a legitimate undertaking? Re-engaging the post-structuralist foundation of securitization theory’. *Cooperation and Conflict*, 1-18.

Wilhelmsen, J. (2016). *Russia's securitization of Chechnya: how war became acceptable*. Taylor & Francis.

News articles and speeches

Aaviksoo, J. (2007). *Cyber defense: The unnoticed third world war.* Estonian Ministry of Defense Website commentary on cyber defense http://www.mod.gov.ee/en/1468.

Ansip, A. (2007) *Prime Minister Andrus Ansip's speech in Riigikogu, 2. May*. Published at the government website: https://www.valitsus.ee/en/news/prime-minister-andrus-ansips-speech-riigikogu

BBC (2007) Estonia hit by 'Moscow cyber war'. BBC, May 17.

Blomfield, A. (2007) Estonia Calls For a NATO Strategy on 'Cyber-Terrorists' After Coming Under Attack. *The Daily Telegraph*, May 18.

Davis, J. (2007) 'Hackers Take Down the Most Wired Country in Europe'. WIRED aug. 21.

Ilves, T. (2007). President Ilves: Our own careless satisfaction and slack thinking that everything is okay are among Estonia's greatest enemies. Press Reports, 1 June. Office of the President, Public Relations Department, Tallinn, Estonia.

Meyer, D. (2010). ITU head: cyberwar could be 'worse than tsunami'. ZDNet, 3 September http://www.zdnet.com/itu-head-cyberwar-could-be-worse-thantsunami-3040089995/..

Mite, V. (2007). 'Estonian attacks seen as 'cyberwar''. *RFE/RL*, 30 May.

Landler, M. & J. Markoff (2007) 'In Estonia, what may be the first war in cyberspace'. *The New York Times,* 28 May.

Lesk, M. (2007). The new front line: Estonia under cyberassault. IEEE Security & Privacy, 5(4 (July/Aug)), 76e79

Paet, U. (2007) Declaration of the Minister of Foreign Affairs of the Republic of Estonia, 1 May 2007. Published on the Website: https://www.valitsus.ee/en/news/declaration-minister-foreign-affairs-republic-estonia\

The Daily Mail. (2007) 'Attack of the Cyber Terrorists'. *The Daily Mail.* May 28.

Traynor, I. (2007) 'Russia Accused of Unleashing Cyberwar to Disable Estonia'. *The Guardian*, May 17.