Securitization And Desecuritization In Estonia's Cyber Politics

by

Michael Phillip Roush

A thesis submitted in partial fulfillment of the requirements for the
degree of Master of Social Science in
Peace, Mediation, and Conflict Research

PEACE034 Master's Thesis
Supervisor: Dr. Frank Möller

School of Social Sciences
Master's Degree Program in Peace, Mediation and Conflict Research
MICHAEL ROUSH: “Securitization and Desecuritization in Estonia’s Cyber Politics”
Master’s Thesis, 85 pages
Major: Peace and Conflict Research
May 2015

Abstract

In response to the 2007 cyber attacks on Estonia’s critical cyber infrastructure there have been a wealth of documents produced by Estonian government ministries and the NATO Cooperative Cyber Defence Center of Excellence that address the topic of cyber security. This thesis examines the concept of desecuritization within the Copenhagen School’s Securitization Theory and the Estonian discourse on cyber conflict following the 2007 attacks. The overall aim of this thesis is to investigate some of the major public policy documents that were published by the Estonian government ministries and the NATO CCDCOE that address the issue of cyber conflict in order to assess the movement of the discourse generated by the public policy documents towards securitization or desecuritization. Through the methodological approach of discourse analysis, the documents evidenced a general trend towards securitizing movement throughout the examined period of 2008 to 2014. However, based on the theoretical conceptualization of desecuritization and its application to portions of the documents’ discourse, the potentiality of desecuritizing movement within Estonian cyber politics was evidenced. As a derivative of the findings in this thesis, a shift in the paradigm for the study of cyber conflict is proposed for future research. In particular, the employment of the desecuritization concept as a tool in which to analyze political discourse is emphasized as an initial step for researchers to alternatively study threat perception and security as it relates to cyber conflict. In addition to this, it is also proposed that the theorization of cyber peace building, as an associated concept to cyber desecuritization, be further analyzed in future research studies.

Acknowledgments

First and foremost, my thesis supervisor Frank Möller deserves the biggest thanks I can possibly give. He has been instrumental in guiding me throughout the thesis writing process. It has become apparent during this past year that beyond just forcing myself to actually sit down and write, half of the battle of thesis writing is having a supportive and engaged supervisor. So, thank you to Frank for always having an open door for me to come and receive feedback on my work as it progressed. Thank you to my parents, Cinny & Pippo. No matter what new academic endeavor I've decided to undertake, you two have always been extremely supportive of my decision. I certainly would not have been able to come to Finland and do this Masters Program without your support.

Abbreviations

ARPANET – Advanced Research Projects Agency Network

CCDCOE – Cooperative Cyber Defence Center of Excellence

CERT-EE - Computer Emergency Response Team for Estonia

CIP – Critical Infrastructure Protection

CISO – Senior Information Security Official

DoS – Denial of Service

DDoS – Distributed Denial of Service

DNS – Domain Name System

DNSSEC – Doman Name Security

EIF – Estonian Internet Foundation

EISA – Estonian Information Systems Authority

IETF – Internet Engineering Task Force

ICMP – Internet Control Message Protocol

IP – Internet Protocol

IPsec – Internet Protocol Security

IRC – Internet Relay Chatrooms

ISP – Internet Service Provider

IT – Information Technology

LOIC – Low Orbit Ion Cannon

MoD – Ministry of Defence

NATO – North Atlantic Treaty Organization

NCS – National Cyber Security

SME – Small & Medium Enterprises

TCP – Transmission Control Protocol

VPN – Virtual Private Network

Table of Contents

1. Introduction 1

2. Theory 4
   2.1 Securitization Theory 4
   2.2 Desecuritization 9
   2.3 Aspects of Cyber Securitization 14
   2.4 Security Constellations & Macrosecuritization 18

3. Methodology 24
   3.1 Discourse Analysis 24
   3.2 Research Objective 27
   3.3 Selection of the Case 28
   3.4 Data Selection (Inclusion / Exclusion) 30
   3.5 Limitations and Considerations 32

4. Cyber Context 35
   4.1 Cyber Infrastructure 35
   4.2 Modes of Cyber Attack 38

5. Estonian Case Study 43
   5.1 The Case: Estonia, 2007 43
   5.2 Primary Data 49
   5.2.1 NATO CCDCOE 50
   5.2.2 Estonian Ministerial Public Documents 62

6. Conclusion 78

7. References 82

1.0 Introduction

The month-long cyber attack against Estonia's critical cyber infrastructure during the spring of 2007 was a pivotal instance in which the destructive capacity of cyber operations against a state was evidenced for the international community. In a form of political protest, the attackers targeted the major websites of the Estonian government, some of the most widely distributed news agencies in Estonia, the biggest Estonian Internet service providers, and the major online banking services within Estonia. These attacks were carried out as a result of the movement of a memorial for fallen Soviet soldiers from the city center to a cemetery in the outskirts of the Estonian capital of Tallinn, which had the effect of angering a contingency of the Russian minority within the country as well as some Russians outside of Estonia. The ensuing cyber protest of this removal of the memorial came about in the form of various methods of cyber attack. For the sake of brevity, these attacks can be summated as modes of service denial for the Estonian networked infrastructure.

In effect, the cyber attacks rendered major elements of the Estonian populace's Internet connectivity unusable while also limiting the ability of the government and media to communicate with the Estonian people via the cyber medium. The scale of these attacks, in which the political, economic, military, and societal sectors were affected, prompted a movement to assess the way in which the Estonian government viewed its cyber security strategy, especially in terms of deterring future asymmetrical cyber attacks similar to what was experienced in 2007.

The movement to reassess the Estonian cyber security strategy began the following year in 2008 with the initial release of the Estonian Ministry of Defense's "Cyber Security Strategy" document. Following the publication of this cyber security strategy document, and the concomitant creation of NATO's Cooperative Cyber Defense Center of Excellence in Tallinn, both the NATO CCDCOE and the Estonian ministerial organs continued to publish documents aimed at addressing cyber security and putting forth policy recommendations with the intention of strengthening cyber conflict deterrence. In addition to policy recommendation documents, the Estonian Information Systems Authority published annual reports on the status of cyber security and peace in

order to track the efficacy of the implementation of the new security and policy directives.

The terminological usage of 'security' has varied interpretations within the field of international relations. One perspective that emerged in the early 1990s is the Copenhagen School's Securitization Theory. Whether viewed as a traditional theoretical perspective, or as a methodological framework, Securitization Theory's principle purpose remains that it aims to serve as a tool for the analysis of politics on various levels and sectors, particularly the transition of an issue (cyber attacks for instance) to an extreme level of politics through the conveyance of existential threat to a referent object. This movement of an issue to a status out of the realm of the political for the purpose of operating outside of legislative capacity represents a securitization. Conversely, the movement of an issue back to the spectrum of the politicized is the process of desecuritization. By using this understanding of security, the researcher can thus study the political maneuvering of a state in regards to a certain issue.

Thus, by speaking in terms of security the Estonian state effectively frames the issue of cyber conflict in a securitized manner. However, the Estonian policy recommendations in their publications on the issue of cyber conflict have been largely aimed at alleviating threat through both non-legislative means, and through politicized policy initiatives that do not generally reflect a movement towards the Estonian state taking exceptional measures to eliminate existential threat to the state. This realization presents a situation wherein the discourse of these public policy documents can be investigated from a perspective of analyzing the prospects of a desecuritizing movement on the political spectrum in Estonia rather than looking to assess a movement towards the securitized status of the issue of cyber threat. With that being said, the proposed research question (and subquestion) for this thesis is as follows:

What are the main elements of the discourse emanating from Estonian public policy documents on cyber security? And is this discourse indicative of desecuritizing moves in the publications following the 2007 attacks?

With regards to the above research question guiding the research objective, the

overall thesis is designed to first cover the aforementioned Copenhagen School Securitization Theory as it serves as the theoretical basis of the research. In particular, the theoretical chapter will cover the desecuritization concept in much deeper detail than what is offered in this introduction section in order to better elucidate its conceptualization before moving forward in the analysis. A point of emphasis as to why desecuritization was chosen as a focus rather than desecuritization lies in the Copenhagen School's authors' explanation of desecuritization as being the ultimate concluding goal of securitization itself. This sentiment is explored further in the theoretical chapter. Subsequently, the methodology chapter will cover the overall design and implementation of the research. As this research study is based on the analysis of discourse, the understanding and application of discourse analysis is further elaborated on. In addition to this, the methodology chapter will cover the topics of the case study design of analyzing the policy documents, and the research objective going forward from what has been established with the presentation of the research question. Chapter 4 breaks down the technical side of the thesis in that it covers the inherent meaning of the term 'critical cyber infrastructure' and includes a survey of the various known modes of cyber attack including the ones used in the Estonian case. Chapter 5 is a move into the heart of the discussion and analysis of the Estonian policy documents where the culmination of the theoretical and methodological frameworks allow for the assessment of discourse trends referent to securitization and desecuritization movements in Estonian policy. Finally, Chapter 6 serves as a reflective discussion of the findings in Chapter 5 as well as serving as a platform from which recommendations for future research initiatives will be offered in light of the research that was done herein.

2.0 Theory Chapter

The theoretical basis of this study is predominantly grounded in the Copenhagen School's Securitization Theory. The foundation of which is primarily attributed to Barry Buzan, Ole Waever, and Jaap de Wilde through their various works that culminated into their book, *Security: A New Framework for Analysis*, as well as numerous publications since the book's release in 1998, that have addressed criticisms of the theory and also added to the continued development of the theory. In addition to these primary authors of the Copenhagen School, I will also draw upon Lene Hansen's work on both the concept of desecuritization and the application of Securitization Theory to the field of study pertaining to cyber security. The following chapter will cover the fundamental aspects of the Copenhagen School's theory, as well as cover associated concepts of the theory for the purpose of providing a theoretical basis from which to base the later analytical sections of this study. Ultimately, the theoretical framework of this study will be applied towards the subject of cyber securitization, and subsequently used to examine the prospects of processes of cyber desecuritization within the public discourse created by the chosen primary documents.

2.1 Securitization Theory

As it is defined in their book, Buzan et al. explain, "'security' is the move that takes politics beyond the established rules of the game and frames the issue either as a special kind of politics or as above politics. Securitization can thus be seen as a more extreme kind of politics or as above politics."[1] Accordingly, the securitization of a selected issue is a process in which the issue transcends normal political means to resolve the threat that the issue presents. The term 'threat' is paramount within Securitization Theory as the threat to the existentialism of a referent object is the specified reasoning behind the move to securitize an issue in order to make it exceptional. Buzan et al. refer to the act of raising an issue above normal politics in order to seek a remedy to the existential threat posed to a referent object as a "securitizing move."[2] In the act of

[1] Buzan et al. *Security: A New Framework for Analysis:* 1998. p. 23
[2] Ibid. p. 25

initiating a securitizing move, the securitizing actor seeks to frame the issue in a way that the exceptionalized status of the issue allows for the actor to addresses the threat in a manner that is normally carried out when addressed in the political realm within the confines of a legislated framework.

Securitizing moves are incumbent on actors in an elite status to initiate. Securitizing elites require an elevated level of authority over the audience in which they seek to convey the necessity for the securitized status of a referent object. According to Waever, "by definition something is a security issue when the elites declare it to be so."[3] From this assumption, it can be said that the power possessed by the securitizing elites must be derived from an advanced level of epistemological, moral, and judicial authority that is held over the audience. Additionally, the persuasionary method of convincing the audience of the necessity for securitization indicates that securitization, in the most basic sense, operates as a speech act. Buzan et al. refer to the interconnected relationship between speech act and securitization in explaining that through the act of speaking security, the securitization of the referent object subsequently begins to take place. However, deference must be given to the audience's willingness to accept the securitization, as securitization is not wholly defined by the speech act itself.[4]

Within a study based within the theoretical framework of the Copenhagen School's Securitization Theory, there is a necessity to provide a brief introduction to the concept of sectors, and the practice of sectoral analysis. The use of Securitization Theory as an analytical tool to examine the processes of securitizing speech acts moving specified threats to an elevated status requires a delineation of which political sector the securitization occurs in. Buzan et al.'s *Security* text offers 'Military, Environmental, Economic, Societal, and Political' as the different sectors in which securitization occurs. The Copenhagen School's understanding of sectors and the referent objects within them has slowly expanded over time, from simply viewing the state as the referent object within the five previously stated sectors, towards the realization that numerous other referent objects are affected by securitization other than just the state.[5]

---

[3] Waever, Ole. Securitization and Desecuritization, in Lipschultz, *On Security*, 1995. p. 54
[4] Buzan, Barry. "Rethinking Security After The Cold War." *Cooperation and Conflict* 32 (1997). p. 15
[5] Buzan et al. *Security:* 1998. p. 8 refers to Ole Waever's text, *Identity, Migration, and the new Security Order in Europe* (1993: 24-27) as the starting point from which the Copenhagen School altered its

Securitization Theory's sectoral aspect goes hand in hand with the levels of analysis that are expressed in the *Security: Framework* text. If Securitization Theory is to be understood as an analytical tool for the purpose of assessing the process of securitization, then it is important to examine what constitutes the specific levels of analysis of the theory. The purpose in doing this is to identify the different actors that can potentially be considered as referent objects of securitization, and thus underscore how the levels of analysis can be used as a way to compare the different sectors.[6]

The Copenhagen School views the levels of analysis[7] in their theory to include: 1. *International systems*, which is the largest possible level, due to it essentially being a blanket term for the trans-global systemic relationship. 2. *International subsystems*, or "groups of units within the international system by the particular nature or intensity of their interactions with or interdependence of each other", and can be regionally, economically or ideologically based in terms of the reasoning for their establishment. 3. *Units*, "meaning actors composed of various subgroups organizations, communities, and many individuals and sufficiently cohesive and independent to be differentiated from others and to have standing at the higher levels." Buzan et al. exemplify the term 'units' as, "states, nations, [and] transnational firms." 4. Subunits, which refers to "organized groups of individuals within units that are able to affect the behavior of the unit. 4. *Individuals*, which is the smallest level of analysis in the theory.[8] Later, in the exercise of applying Securitization Theory to the specific focus of this study, cyber securitization and desecuritization, it will be exceedingly important to draw a connection between the different levels of analysis and the extent to which cyber securitization permeates these objects.

"Classical Security Complex Theory" is closely linked with the sectoral analysis aspect of the Copenhagen School's theory. This theory was first presented by Buzan in his book, *People, States, and Fear* (1983) and further developed in other Copenhagen School publications including the *Security: Framework* text. The definitive explanation

---

original conception of sectors to become a multisectoral approach that includes multifarious referent objects.

[6] Buzan et al. *Security:* 1998. p. 164

[7] Buzan et al. *Security:* 1998. p. 5 clarify the term "levels of analysis" to mean "objects of analysis that are defined by a range of spatial scales, from small to large."

[8] Ibid. p. 5-6.

of this theory is explained by Buzan et al. as "a set of units whose major processes of securitization and desecuritization, or both are so interlinked that their security problems cannot reasonably be analyzed or resolved apart from one another."[9] The benefit of the security complex concept, as Buzan et al. explain, is that it "posits the existence of regional subsystems as the objects of security analysis and offers and analytical framework for dealing with those systems" as well as serving as a reasoning to underscore the importance of the regional level in the context of global security analysis.[10] Additionally, it is important to further emphasize the author's definition of security complexes noting that rather than viewing the state's securitizing actions within the security complex as directly affecting the dynamics of the security complex, it is, in actuality the units within the state that shape the complex through their securitizing actions.[11] Though Security Complex Theory ultimately plays a relatively small part within the necessary overall framework for this particular research study, it is relevant in the sense that it serves as a foundation from which other more relevant concepts of Securitization Theory will be applied to cyber securitization. In particular, this theory will be beneficial in introducing the related Securitization Theory concepts of 'Macrosecuritization' and 'Security Constellations', as well as their connection to cyber security.

The Copenhagen School's description of securitizing a particular threat / issue as a speech act is further expounded upon, as well as critiqued for the purpose of reconceptualization, by Thierry Balzacq in his article *The Three Faces of Securitization: Political Agency, Audience, and Context*. Balzacq holds a contention with the basic normative assumptions of Buzan, Waever, and de Wilde that the securitizing speech act operates as a static "code of practice"[12] in which the securitizing actor and the audience of the speech act are bound to a mutually reciprocal understanding of the necessity to securitize an issue. Balzacq describes the Copenhagen School's assumption as a conventional procedure wherein the conditions for success, or "felicity circumstances" as

[9] Ibid. p. 201
[10] Ibid. p. 11
[11] Ibid. p. 200
[12] Balzacq, Thierry. "The Three Faces Of Securitization: Political Agency, Audience And Context." *European Journal of International Relations* 11 (2005). p. 172

they are described in the text, "must fully prevail for the act to go through."[13] Rather than understanding the speech act in this manner, Balzacq offers a new conceptualization in which the speech act is viewed as a "strategic (pragmatic)" practice that is ensconced within a dynamic relationship of persuasion between the securitizing actor and the audience. More specifically, Balzacq maintains that the "audience, political agency, and context" are three incredibly important factors that weigh in on the success of a securitizing speech act that have been generally overlooked by the members of the Copenhagen School.

In terms of the specific nature of the speech act referred to in Securitization Theory, Balzacq points to John Austin's Speech Act Theory as the foundation from which Buzan, Waever, and de Wilde base their understanding of the speech act as it is presented in their theory. From Austin's theory, Balzacq offers three types of performative speech acts, " (i) locutionary – the utterance of an expression that contains a given sense and reference; (ii) illocutionary – the act performed in articulating a locution … and (iii) perlocutionary, which is 'consequential effects' or 'sequels' that are aimed at evoking the feelings, beliefs, thoughts or actions of the target audience."[14] Consequently, Balzacq draws a parallel between Austin's theory and the Habermas' *Theory of Communication Action* (1985) in which "to say something, to act in saying something, to bring about something through acting in saying something" are referred to as summated expressions of the aforementioned speech acts. Thus, the amalgamation of these acts into a singular concept constitutes the pragmatic action that Balzacq refers to as being differentiated from the speech act that's was presented by Buzan et al. in *Security: Framework.*

In effect, securitizing speech acts are massively influenced by multiple factors surrounding the instances of persuasion between the securitizing actor and the audience. The perlocutionary act is dependent on the linguistic capacity of the actor to elucidate the necessitation to securitize a threat for the audience. Therefore, as explained by Balzacq, the success of a securitizing move by a particular actor is reliant on three basic assumptions: 1. The move is "context-dependent"; 2. There must be a high degree of

[13] Ibid. p. 172
[14] Ibid. p. 175

specificity towards the target audience of the securitization; 3. "Securitization dynamics are power-laden" between the securitizing elite and the audience they are trying to convince of the imminent threat.[15]

2.2 Desecuritization

Ole Waever's *Securitization and Desecuritization* article, similarly to *Security: A New Framework for Analysis*, is a text that is essential to the foundational understanding of Securitization Theory. Waever's text answers the question of what the threshold for determining whether an issue has been securitized is. Waever explains that securitization is essentially a "speech act", and as such, the mere utterance of "security", and its inherent implication for the necessity to remedy a threatening security issue, constitutes the threshold whereby it gains a securitized extra-political status.[16] Though the securitization act can be carried out on as small of a scale as amongst individuals, for instance, Waever commonly refers to "elites" as the actors that are responsible for initiating the securitization of a particular issue. Waever explains that the extra-political status always accompanies the securitization of an issue / security problem due to the state and the main power holders within the state's natural inclination to use all means within the possessed power to eliminate existential threats to the state before any other less threatening issue can be addressed.

Additionally, Waever makes a point in his text to dispel the notion that security and insecurity have a binary relationship where there can only be one or the other. Insecurity, according to Waever, is still a situation where existential threat has been established, but no response has been initiated to counteract the threat.[17] Desecuritization is the aspect of the theory that represents the binary alternative to securitization. As the alternative to securitization, desecuritization is the process that removes an issue from the position of being transcendent of the sphere of political discourse to alleviate the threat posed to the referent object.

---

[15] Ibid. p. 179
[16] Waever, Ole. *Securitization and Desecuritization*, in Lipschultz, *On Security*: 1995. p. 55
[17] Ibid. p. 56

The term "desecuritization" is rarely used in Weaver's article as he opts to use "détente" as an exemplary term to describe desecuritization. Waever accomplishes this by examining the dynamics within the East-West dialogue during the later stages of the Cold War, particularly the efforts made by "détente-orientated" Western actors towards guiding the Eastern actors in the avoidance of securitizing issues that they felt to be threatening.[18] The Western actors' push for the Eastern elites to shift "threats into challenges and security into politics" evidences the way in which détente-orientated dialogue represents the process of desecuritizing issues so as to remove them from the speech-act-induced transcendent position above political discourse.[19] Waever's text is far more instrumental in terms of explicitly determining the foundational theoretical understanding of the desecuritization concept than Buzan et al.'s *Framework* text. However, Waever's *Securitization and Desecuritization* falls short in offering a detailed explanation of the application of desecuritization with respect to the multifarious issues that have or could become securitized by actors whom have a stake in the existentialism of a particular referent object. The task of applying Waever's conceptual framework for desecuritization towards the broadened field of potential referent objects within security studies falls upon other academics, both within and outside of the Copenhagen School, to articulate the nature and dimensions of desecuritization.

Lene Hansen's *Reconstructing desecuritization: the normative-political in the Copenhagen School and directions for how to apply it* is perhaps the best and most up to date consolidation and analysis of the essential works that have been done on the topic of securitization and desecuritization. Hansen draws from the conceptualization of desecuritization as it is originally presented by Waever, as well as from the subsequent critiques emanating from academics outside of the Copenhagen School in order to assess the current standing of both the shortcomings and applicability of this theoretical concept. One of Hansen's initial tasks in her analysis is to reference the critical evaluation that the Copenhagen School lacks any "normative connotations due to its repudiation of the concept of emancipation."[20] Hansen cites Rita Taurek's critique of *Securitization and*

[18] Ibid. p. 60
[19] Ibid. p. 60
[20] Hansen, Lene. "Reconstructing Desecuritisation: The Normative-political in the Copenhagen School and Directions for How to Apply It." *Review of International Studies* 38, no. 3 (2012). p. 527

Desecuritization in which she criticizes the lack of initial theorization leaving "the door wide open for interpretation", as well as Taurek's claim that desecuritization can be seen as an "emancipatory ideal" because of its nature as being a process in which an issue is freed from its securitized status as an existential threat as the two largest gaps in the theorization of desecuritization.[21]

Hansen's second point of emphasis is to highlight the diverse pool of influences on both the primary Copenhagen theorists and the critical theorists outside of the school in their interpretation of the theory. Hansen notes that Buzan et al. have not been particularly explicit in their definitive position on the understanding of politics, but cites their brief admission of being "a middle ground" of numerous theorists that include, "Arendt and David Easton, Schmitt and Habermas, and Max Weber and Ernesto Laclau."[22] Despite listing these influences, the lack of an explicit discussion of the epistemological basis for the political as it is understood in the theory, is a serious indictment of the original theorists.

Hansen also spends a significant amount of time in her article articulating the foundational understanding of the desecuritization concept as presented by Waever and other academics in their application of the concept to other fields of study (gender, identity, & migration) in order to further develop the concept beyond the superficial presentation originally offered by Waever. Hansen explains that desecuritization is reliant on the fluctuation of identities, specifically a change in the "friend-enemy" dynamic wherein there is an existence of oppositional identification.[23] In this explanation, Hansen references the east vs. west Cold War dynamic used by Waever in Securitization and Desecuritization in order to express the necessitation of process of transforming or destroying the attribution of a threatening enemy towards the "Other" to facilitate a cessation of security inducing speech acts.[24]

Finally, Hansen completes her analysis by listing four political forms of desecuritization in what can be seen as an attempt to expand the ability of the researcher to more accurately discern between the varied ways in which desecurtization takes place.

---

[21] Taureck, Rita. "Securitization Theory And Securitization Studies." *Journal of International Relations and Development* 9 (2006). p. 57
[22] Hansen. "Reconstructing Desecuritisation": 2012. p. 527
[23] Ibid. p. 533
[24] Ibid. p. 533

Hansen's legitimization for doing this is that there are no particular instances in which the process of desecuritization aligns with all four of the categories, and thus can be used as analytical tool to presuppose a theoretical articulation of the trajectory of a selected conflict. The first of these four political forms is "Change through stabilization." This form of desecuritization is most closely associated with the détente concept as originally explained by Waever in his *Securitization and Desecuritization* article. The major critique of this manifestation of desecuritization that is offered by Hansen is the "conservative, system building character" it exhibits.[25] In addition to this, change through stabilization generally operates on the macro scale and fails to address the security issues on the micro scale, as exemplified by the case of attempted stabilization in Iraq and Afghanistan with the intervening actors leaving local actors to take up the responsibility to maintain small-scale security.[26]

The second political form of desecuritization, "Replacement" is simply defined as, "the combination of one issue moving out of security while another is simultaneously securitized."[27] As explained by Hansen, replacement desecuritization occurs as a result of the persistently changing state identities as well as power dynamics both locally and abroad. Through the process of change and replacement, potentially securitized threats are replaced by threats relevant to the new dynamic. As a result of this progressive change, a securitized threat will fall out of security discourse and effectively become desecuritized in place of a new threat that concomitantly becomes securitized in its place. Replacement desecuritization, however, carries about an implication in which there are threats within the same categorization (e.g. different 'enemy' states) periodically replacing one another's statuses of securitized and desecuritized. This points to the necessity for a close evaluation of whether political dynamics related to 'replacement desecuritization' are based in a normative inclination of the state to require an "other"[28] for the maintenance of a figurative vacuum of desecuritization / securitization.

Hansen's third form of desecuritization is "Rearticulation." Hansen explains that rearticulated desecuritizations are defined as a direct action in which "an issue from the

[25] Ibid. p. 540
[26] Ibid. p. 540
[27] Ibid. p. 541
[28] Ibid. p. 541

securitised by actively offering a political solution to the threats, dangers, and grievances in question."[29] Rearticulation of an issue for the purpose of bringing it back into the realm of political discourse has a much greater positive connotation than the prior two forms of desecuritization because it is not naturally followed by an eminent securitization of a new threat as a result of the initial desecuritization. In spite of this generally positive connotation for this manifestation of desecuritization, it is important to note that it has the appearance of offering finality to the conflict and securitization surrounding an issue, but in reality Rearticulation does not inherently prevent a threat from reappearing and subsequently becoming re-securitized.[30]

The fourth and final type of desecuritzation introduced in the Hansen article is "Silencing." Hansen defines Silencing as "when an issue disappears or fails to register in security discourse."[31] Viewing Silencing as an actual form of desecuritization is extremely problematic when keeping in mind that the Copenhagen School views desecuritization as the desirable result within the overall theory, as well as being a move from the special status of the securitized issue down into a state within the realm of political discourse. The reason why this type of desecuritization is so problematic is because Silencing actually removes the issue completely out of the proverbial securitization spectrum.[32] In this regard, it is clear that understanding Silencing as a certain form of desecuritization is quite difficult. Though the issue, once silenced, has technically become desecuritized in the sense that it is no longer in a securitized status, it is still problematic when juxtaposed with the way in which the Copenhagen School views the nature of desecuritization. As such, this form of desecuritization must be approached cautiously when used by a researcher as a tool for the analysis of the desecuritization of a particular threat.

---

[29] Ibid. p. 542
[30] Ibid. p. 544
[31] Ibid. P. 542
[32] An important point of reference for the discussion of the political spectrum that securitization operates on is Jef Huysmans' article, The Question of the Limit: Desecuritization and the Aesthetics of Horror in Political Realism, *Journal of international Studies* (1998). Huysmans rejects the notion of securitization being "the extreme form of politicization on the continuum of non-politicised, politicised, securitized" (p. 580). Huysmans believes that the act of securitization cannot be located within the continuum at all as Buzan et al understand it due to Huysmans' view of securitization being a practice aimed at destroying the conventional political process rather than being a process of transcending the point of politicization. For the purposes of this study, however, securitization will be understood in the Copenhagen sense of the term as operating on the spectrum of politicization.

One of the particularly difficult gaps in the current theorization regarding the concept of desecuritization is the possibility for the target audience to not accept a move out of the securitized and back to the political realm. There are many instances of literature covering the topic of the possibility of a securitizing move failing because the audience chooses not to accept the elite's attempted conveyance of the necessity to protect a referent object from existential threat.[33] The converse instance of audience non-reciprocity of desecuritization, however, has yet to have any traction within the field of security discourse. The way in which authors like Waever and Hansen present the concept of desecuritization inherently implies that unlike securitizing moves, desecuritizing moves are normative in their nature for the audience to reciprocate the feelings expressed by the desecuritizing actor. This contention with the theory will be explored further in the analytical section of this study as the strengths and weaknesses of the previously mentioned modes of desecuritization are assessed in comparison to their potential application cyber security discourse.

2.3 Aspects of Cyber Securitization

Another point of emphasis in regards to who may securitize a specific issue out of the political realm, is the distinction that Securitization Theory does not only refer to macro-scale, state-centric moves to securitize through threat establishment. The speech act wherein a referent object becomes securitized can similarly be committed on a smaller individual scale, though this assertion is weakly expounded upon. The authors explain that the "size and significance" issue of securitization can be illustrated in an instance where the Pentagon designates "hackers as a catastrophic threat and a serious threat to national security, which could possibly lead to actions within the computer field but with no cascading effects on other security issues."[34] In exemplifying this notion, Buzan et al. reveal a shortcoming in their ability to assess the effects that nefarious cyber activity can have on multifarious security issues. The extent at which the "cascading" effect towards other security issues was severely underestimated in light of how the securitization discourse around cyber conflict has moved into sectors beyond just the

[33] See Hansen: 2012, Balzacq: 2005, Huysmans: 1998.
[34] Buzan et al. *Security:* 1998. p. 25

computer field (military & societal sectors must be taken into consideration when discussing cyber securitization).

The constitutional makeup of cyber security has been previously theorized by Ronald Deibert as consisting of four separate discourses (National Security, State Security, Private Security, and Network Security).[35] Deibert's first security discourse, National Security, refers to the state's perceived threat to national collective identities emanating from the undermining effect created from the inter cultural exchange facilitated by internet access.[36] A state's predilection for assessing internet access as a threat to national cultural identity is largely incumbent on a regime's socio-political and socio-economic stances. Deibert cites authoritarian and conservative regimes as having more inclination towards censorship of outside influence in order to preserve the integrity of their constituent's collective identity, whereas liberal democratic regimes opt for either a "cultural alliance" approach for the sake of trade promotion, or through an approach in which collective identity degradation is circumnavigated by the state insistence on the creation of a larger domestic presence in digital media and communications in lieu of outright censoring the outside influence.[37]

The term, State Security, is a relatively complex umbrella heading that refers to the external and internal threats to a state's functional integrity. In the context of this study, the internet is inherently seen as a new avenue by which the government envisions itself as being able to conduct military activities. In actively acknowledging that the internet represents a mode of military attack, the state intrinsically acknowledges the possibility that another state or non-state actor would conduct its own military-related operations against them via the internet. This acknowledgement of external threat creates a self-reinforcing securitization process as the movement towards the exploitation of global network instability is further pursued. Consequently, the movement towards alleviating network vulnerability through methods such as encryption further confuscates the origin of exploitative actions, thus undermining the ability of the state to effectively govern both internally and externally.[38] State fears over controlling the flow of

[35] Deibert, *Circuits of Power*: In *Information Technologies and Global Politics,* Rosenau. 2002.
[36] Ibid. p. 120
[37] Ibid. p. 121
[38] Ibid. p. 123

information closely links state security discourse with national security discourse, however the key difference being the emphasis on cultural dynamic control in the national security context, and governance dynamic control in the state security context.

Private security discourse is representative of the micro end of the cyber security scale of analysis. The level of integration of an individual's personal data continues to expand as commercial and governmental services expand and require such information. As such, every individual is continuously developing their personal data profile with every digital interaction they commit. The development of this profile is also done both on a voluntary basis of interaction as well as through a non-voluntary interaction in the form of surveillance. As a result of the continuous proliferation of personal data from online interaction, privacy has the potential to fall into the realm of securitizing discourse rather than a political discourse depending on the extent of the threat towards individual-related referent objects that is conveyed by the securitizing actor. An example of contemporary securitization of this sector can be seen in the claims that governmental surveillance and proliferation of personal data is representative of an existential threat to the right to privacy by the constituency.

The term 'networked' is a vital descriptive in cyber security discourse that is referent to the structural relationships that permeate all sectors of analysis. Networked infrastructure, for instance, is integral within global financial institutions, military organs, and critical civic works. Thus, the network itself represents the fourth referent object within cyber security discourse as the operational integrity of the network structure within the various sectors is necessitated for the facilitation of the information flow between users and providers. Deibert explains that the securitization of network integrity can be seen in the incorporation of "firewalls, virus protection software, logging and real-time alarm systems, and various forms of encryption" as a reactionary move that has resulted from increasing network attacks and breaches.[39]

Similarly to the work done by Deibert, Lene Hansen's article *Digital Disaster, Cyber Security, and the Copenhagen School*, co-written with Helen Nissenbaum, serves as reference point for the application of Securitization Theory to the case of cyber conflict, as well as specifically referencing the desecuritization aspect of the theory in

[39] Ibid. p. 129

relation to cyber conflict. One of the first important points made by Hansen and Nissenbaum is delineating what is meant by the term "cyber security." As mentioned before, the allusion made by Buzan et al. to responsive actions being made within the computer field as a result of "hackers" and threats to national security may have been short sighted, but it also begs the question of 'what is computer security?' and how does this concept differ from the term cyber security. Hansen and Nissenbaum approach this problematic by elucidating the fact that the use of the term security in relation to computer security is not theoretically compatible with the Copenhagen School.[40] This is because computer security discourse is technical in nature and more focused on altering technical systemic flaws that lead to unintended uses of various computer based technologies. In this sense, computer security fails to register on the politicized spectrum, as would be the case for a Copenhagen School understanding of the term. Consequently, Hansen and Nissenbaum postulate that there is a connection between computer security and cyber security in that the "technical discourse is linked to the securitizing discourse" and ultimately the term " 'Cyber Security' can, in short, be seen as 'computer security' plus 'securitization,' " in the Copenhagen School's sense of the term 'securitization.'[41]

Hansen and Nissenbaum next explain how the securitizing speech act can be carried out in relation to cyber securitization. The authors point to the role of "technification" in legitimizing securitizing actions as a proactive process that capitalizes on the technical ignorance of the general public whom subsequently accept the necessity to securitize the issue conveyed by the securitizing elites. The authors refer to this privilege held by the securitizing elites as an "epistemic authority" held over the public.[42] The epistemic authority held by the securitizing elites asserts that the audience of the securitizing speech act is far more likely to accept the securitization of cyber threat because the audience's lack of held knowledge relating to the cyber field prevents them from objecting to the securitizing act.

Audience acceptance of cyber securitization is not, however, always derived from an imposed epistemic authority of securitizing elites. The lexicon associated specifically

---

[40] Hansen, Lene & Nissenbaum, Helen. "Digital Disaster, Cyber Security, and the Copenhagen School" *International Studies Quarterly*, 53: (2009). p. 1160
[41] Ibid. p. 1160
[42] Ibid. p. 1167

with cyber securitization is an important factor in initiating the process of accepted securitization, as its terminology (technical and metaphorical) directly influences whether or not the issue of cyber conflict is perceived as an existential threat to the various referent objects it affects. Cyber security discourse is riddled with grammatical ploys to convey the necessity to give emergency status to securitizing elites to circumvent cyber-based threats. The number of cases in which major instances of cyber conflict have occurred is both small and entirely up for debate, and because of this, cyber security discussants have largely relied upon the use of historical analogies to exemplify the possible outcomes emanating from cyber threat. Two often cited examples of historical analogies used in cyber security discourse are the terms, "electronic Pearl Harbor"[43] and labeling a cyber attack as "the Hiroshima of cyber-war."[44]

Though the nebulousness of cyber security discourse cannot be alleviated without concrete exemplifications of the extent of damage done by previous cyber attacks, there is still much work that can be done towards better identifying the referent objects of cyber securitization. As mentioned when discussing the Buzan et al. *Security: Framework* text, the Copenhagen theorists failed to estimate the breadth of the cascading effects that cyber securitization potentially has in other sectors covered by the securitization umbrella, including military, economic, political, and societal. This gap in foresight by the Copenhagen School's theorization is a great starting point to introduce the debate over what constitutes the referent object of cyber securitization, as without such a discussion, it is impossible to establish what object(s) potentially face existential threat, and thus warrant securitization.

2.4 Security Constellations & Macrosecuritization

A major point of discussion that is essential within the developing field of cyber securitization research is the necessity for developing an understanding of 'cyber's' place within securitization. Specifically, this is in terms of distinguishing whether the research is being done with the belief that cyber security is a distinct sector on its own, similar to

[43]Bendrath, Ralf "The American Cyber-Angst and the Real World – Any Link?". In Robert Latham (Ed.): Bombs and Bandwidth: The Emerging Relationship between IT and Security, New York: The New Press: 2003. p. 50

[44] Rid, Thomas. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35, no. 1 (2012). p. 6

the established sectors presented by the Copenhagen School. Or if 'cyber' is not a sector in its own right and, rather, the cascading effects of cyber security simultaneously permeate the various sectors that are currently analyzed in the field of Security Studies. This problematic sets the stage for the introduction of Buzan and Waever's added facets of Securitization Theory, Security Constellations and Macrosecuritization. Through the application of these two elements of Securitization Theory, the theoretical structure of cyber security stands to gain a significantly higher degree of coherence.

The term 'Macrosecuritization' was born out of the criticism of the Copenhagen School for failing to conceptualize security on a more expanded scale, which stems from securitization having the primary focus of the state as the referent object of securitization. This, as Buzan refers to it, is "middle-scale" focused securitization.[45] At polar ends of the referent object spectrum exist microsecuritization and macrosecuritization. Microsecuritization, being the end of the scale that represents individuals or small groups as the referent objects, is generally understood to be unsuccessful in securitizations because its size drastically limits the level of legitimacy that it can forge for a securitization to take place.[46] On the other end of the spectrum, macrosecuritization represents the 'international systems' dimension of Securitization Theory's levels of analysis. This means that macrosecuritization has had the connotation that its referent object is humanity as a whole, with contemporary attempts to frame environmental security as a humanity-wide threat as an example of macrosecuritization by Buzan and Waever.[47] Despite the difference in scale, micro and macrosecuritizations are similar in that macrosecuritization also generally fails to gain enough legitimization to have a consistent level of audience acceptance. The reasoning behind this is because middle level securitizations possess a "we" dynamic as a result of "self-reinforcing rivalries with other limited collectives" and thus "create a consistently more durable scenario for securitization."[48]

The caveat to the previous assessment of referent object scale and success is that when keeping the levels of analysis in mind, there are additional levels of referent objects

[45] Buzan, Barry, and Ole Waever. "Macrosecuritization and Security Constellations: Reconsidering Scale in Securitization Theory." *Review of International Studies* 35, no. 2 (2009). p. 255
[46] Buzan & Waever. "Macrosecuritization and Security Constellations": 2009. p. 255
[47] Ibid. p. 255
[48] Ibid. p. 255

in existence than what is simply covered by the macro – middle – micro scale continuum. In particular, the 'international subsystem' level of analysis is a space of operation in which securitization can take place between middle-scale and macro-scale. In essence, the securitizations created on the part of entities within the international subsystem level of analysis can theoretically develop into the competitive securitizations and subsequent 'we' dynamic that Buzan and Waever feel is necessary for sustainable legitimacy to be achieved. Under this line of reasoning macrosecuritization becomes more viable and significantly more likely to be seen as legitimate once enacted on the international subsystem level.

Discussing the nature and efficacy of the macrosecuritization concept inherently provokes a subsequent discussion of the concept, 'security constellations.' The term security constellations originally appears in Buzan et al.'s *Security: Framework* text[49] wherein the authors attempt to explain a concept in which multiple securitizations are interconnected amongst various levels of analysis. Similar to the classical 'security complexes' concept that was explained in the section of this chapter covering sectoral analysis, the security constellations concept is an analytical tool with the purpose of highlighting the relationships of securitizations within different sectors and levels of scale with a specific emphasis on the international subsystem as a level of analysis with a direct effect on the international scale. The difference between security complexes and security constellations is the overall extent and scale at which the two can be used to analyze large scale interconnected securitizations. While the theory of security complexes runs under the understanding that there are four different tiers of interaction within the security complex,[50] the framework for security constellations transcends the regional focus to expand the lens for the analysis of an amalgamated dynamic relationship between all security-related levels of analysis as well as the intermingling of securitizations in the military, environmental, economic, societal, and political sectors in relation to a particular issue.

---

[49] Buzan et al. *Security:* 1998. p. 168-170, 201-202

[50] Buzan et al. Explain in *Security: A New Framework For Analysis* that the tiers of interaction within the security complex are either "within states (focusing especialy within weak states), between states (linking them into regional complexes), between complexes (a minor or residual category concept in places where the boundaries between complexes were unstable), and between great powers (defining the system level or, in neorealist terms, the polarity of the system." p. 201

The connection between macrosecuritizations and security constellations is evident in the assertion that the macrosecuritizations, themselves, are responsible for the creation of a security constellation.[51] In the case of securitizations occurring on the international subsystem level of analysis, concomitantly competing securitizations construct one integrated constellation. The catalysts for competing securitizations on the macro scale and the consequential formulation of constellations are attributed to the permeation of ideological universalisms amongst the securitizing actors. Buzan and Waever refer to the existence of universalisms in instances of macrosecuritization as a signifier of the creation of security constellations. Universalisms manifest themselves in four different forms: Inclusive Universalisms, Exclusive Universalisms, Existing Order Universalisms, and Physical Threat Universalisms.[52] The following text is a description of the four different manifestations of universalisms originally taken from Buzan and Waever's *Macrosecuritization and Security Constellations* article.

1. Inclusive Universalisms: ideological beliefs, whether secular or religious, about the best way to optimize the human condition. These are universalist in the sense that they claim to be directly and immediately available to all of humankind (for example, Liberalism, Marxism, Christianity, Islam).
2. Exclusive Universalisms: ideological beliefs that claim superior rights and status for one group over the rest of humankind (for example, Marxism, white supremacy, European imperial doctrines; Japanese imperial doctrines). These are universalist in the sense that they claim the right of one group to rule over, or even replace, all of humankind.
3. Existing Order Universalisms: political claims about threats to one or more of the institutions of international society, which are universalist in the sense that they take the global level international social structure as their referent object. Such claims could overlap with (1) if one universalist ideology had provided the framework for international society, as for example liberalism has done for the current global economy. But existing order universalisms could be independent, where for example in a pluralist international society claims were made that sovereignty was being threatened by transnational actors.

[51] Buzan & Waever. "Macrosecuritization and Security Constellations": 2009. p. 259
[52] Ibid. p. 260-261

4. Physical Threat Universalisms: claims about dangers that threaten humankind on a planetary scale (for example, nuclear weapons, global warming, new diseases). These are universalist because they take the physical fate of humankind as their referent object.[53]

For the purpose of this study, a vital connection that needs to be made is the link between macrosecuritization, security constellations, universalisms and the specific nature of cyber securitization. Keeping Deibert's understanding of cyber securitization in mind, the separate discourses of cyber securitization that operate at varied levels of scale are closely representative of a framework for macrosecuritization, especially in the case of national, state, and network security being the referent objects of cyber threat. Consequently, the designation of cyber securitization as a partial representation[54] of a macrosecuritization begs the question of whether the various referent objects across different levels of scale indicate the existence of a security constellation, or whether the field of cyber security discourse operates under the understanding that the referent objects of cyber securitization are separate as Deibert presents them. In the case of this study, an allegiance will be held with Hansen and Nissenbaum's claim that cyber securitization's various referent objects are in fact a part of a complex security constellation that was born out of competing articulations at different levels of analysis in the field.[55] Thus, cyber security will be understood as its own separate sector with permeations of referent objects traditionally associated with the initial sectors of analysis espoused by the Copenhagen School.

When it comes to making a connection between the universalisms concept raised by Buzan, and Waever and the dynamics of the cyber framework, there are two of the four manifestations of universalism that resonate within this framework. Existing Order universalisms are representative of the current dynamic standing of cyber security in that the general political perception of cyber threat against existing social institutions and state sovereignty are threatened by global nature of cyber attack eminence. Cyber security also exemplifies Buzan and Waever's Physical Threat Universalism. Though this

[53] Buzan & Waever. "Macrosecuritization and Security Constellations": 2009. p. 260-261
[54] The inclusion of "private security" within the framework of cyber securitiztion as it was presented by Deibert's text, removes the discourse from a wholly macro focus, and leaves the scale of securitization to be reliant on the articulation of the threat by the securitizing actor.
[55] Hansen & Nissenbaum. "Digital Disaster": 2009. p. 1163

assumption is still partially theoretical, the case of the 2007 cyber attacks on Estonia gives it significantly more credence due to the potentiality for cyber attacks to specifically target critical state and emergency infrastructure, which has a subsequent direct effect on the human security of a targeted state. This threat becomes universal with the continued global reliance by state citizenry on these vulnerable networks.

To summate the overall assessment of the Copenhagen School's Securitization Theory expressed in this chapter, the main points of emphasis will be highlighted again in preparation for their application within the analytical portion of this thesis in chapter 5. The act of securitization has been defined as a deliberate expression of existential threat towards a referent object by a securitizing elite for the purpose of moving an issue out of the political spectrum, and in doing so, the securitizing actor(s) seek to address the issue through exceptional measures beyond what is expressed in non securitized politics. As such, the concept of desecuritization works conversely to securitization as the ultimate end-goal of the securitization process and moves an issue from its exceptional status back to the political realm.

3.0 Introduction to Methodology

As the theoretical framework that this research study is based in has been thoroughly established in the previous chapter, it is logical to move to a discussion of the methodological framework that will be employed. As a first point of emphasis, it must be established that this research study is done through a solely qualitative methodological approach. This is not to say that there is no place for the use of statistical analysis as a basis for studies focused on cyber conflict, but as the intention of this research study is to delve into emerging theoretical conceptualizations relating to the discourse on cyber desecuritization, it makes the most sense to base the study in a qualitative approach as a means to achieve the desired end. It this case, 'desired end' is referent to the research outcome, which along with the chosen research question, will be further elaborated on later in this chapter. In addition to this, the other important elements in the methodological framework of this study such as the chosen form of analysis, the data that will be analyzed, and the case study will all be introduced throughout the remainder of this chapter.

3.1 Discourse Analysis

The primary type of analysis that has been chosen for this research study is discourse analysis. Obviously, in stating that this type of methodological analysis will be used, there becomes a requirement to not only briefly examine the essence of the discourse analysis in general, but also to refer to the research objectives in order to justify the selection of the discourse approach. As a first step in determining what analytical approach would be taken, it was extremely helpful to assess which approaches are associated with studies based in the securitization theoretical framework. In fact, there is an inherent association between 'discourse' and 'security'. Buzan et al. express this sentiment in the *Security: A New Framework* text by stating, "The way to study securitization is to study discourse and political constellations"[56] and thus securitization is reliant on the discursive construction surrounding whatever particular issue is in

[56] Buzan et al. *Security:* 1998. p. 25

question. Consequently, the meaning of the term discourse, as well as the functionality of discourse analysis as a whole must be examined more closely.

Much of the theoretical underpinnings of the methodological framework in this research study will be derived from the work done by Copenhagen School researchers, Ole Waever and Lene Hansen's work on discourse analysis put forth in their text, *European Integration and National Identity: The challenge of the Nordic States*. Waever and Hansen first note that their understanding of discourse is a derivative of perspectives from Foucault, Laclau, and Mouffe[57] in what they describe as an "early postructuralis[t]" perspective.[58] Within the text, it is also explained that Waever and Hansen's provided understandings of discourse was developed with deference to Jacques Derrida's work on the discussion of the inherent meaning of language.[59] How these previous works were adopted into Waever and Hansen's understanding of discourse will be expounded upon later, as it is beneficial to first begin with an excerpt from the text in which the two authors offer their definitive view of the essence of discourse.

> "Discourse analysis works on public texts. It does not try to get to the thoughts or motives of the actors, their hidden intentions or secret plans. Especially for the study of foreign policy where much *is* hidden, it becomes a huge methodological advantage – and one inherent in the approach – that one stays at the level of discourse. If one sticks rigorously to the level of discourse, the logic of the argument remains much more clear – one works on public, open sources and uses them for what they are, not as indicators of something else. What interests us is neither what individual decision makers really believe, nor what are shared beliefs among a population (although the latter comes closer), but what codes are used when actors *relate* to each other."[60]

Briefly, as a point of criticism on the above quote from Hansen and Weaver, the use of "advantage" as a descriptive of this type of methodological framework should be addressed in order to give a frame of reference for the position of myself as an author on this perception. It is rather difficult to view the discursive methodological framework as an advantageous approach due to its insistence on not focusing on the rhetorical

[57] See Foucault: 1972, Laclau & Mouffe: 1985
[58] Hansen, Lene, and Ole Waever. *European Integration and National Identity the Challenge of the Nordic States*: 2003. p. 23
[59] Ibid. p. 23
[60] Ibid. p. 26-27

connotations within the text. The distinctions of the methodologies are merely just two separate approaches and thus will not be viewed within some sort of a hierarchical framework wherein some methodological approaches provide researchers with a more enriched analytical perspective.

As a researcher it is vital to draw a line that separates the concept of discourse from that of rhetoric. In placing one's self in a position wherein discourse is chosen as the method for analysis in a study, the researcher must understand that the point is not to explore the intended meaning of what is being analyzed. Rather, the conscious approach of "sticking to discourse as discourse", or specifically looking at the framework that has shaped how things are discussed, is the focus of discourse analysis, and what separates it from the act of assessing rhetoric and the underlying attribution of meaning.[61] When considering the different types of speech acts that were discussed in the theory chapter, the differentiation made in discourse analysis is made between assessing the locutionary act rather than the perlocutionary act.

Perhaps another way in highlighting the discourse approach of this thesis would be to borrow from Foucault's explanation of discourse from *The Archaeology of Knowledge*. As previously mentioned, Waever and Hansen base much of their viewpoints on this particular work. They assert that rather than discourse acting as a form of interpretation after the fact, it acts "as a system for the formulation of statements"[62] and that the rules that govern within the system must be analyzed in connection with statements that are being made in the public discourse, and additionally discourse is essentially the formulation of linked objects within structured relationship.[63] Foucault approaches a summation of these ideas by offering a definition of discourse in saying, "We shall call discourse a group of statements in so far as they belong to the same discursive formation; it does not form a rhetorical or formal unity … it is made up of a limited number of statements for which a group of conditions of existence can be defined."[64]

---

[61] Ibid. p. 27
[62] Ibid. p. 29-30.
[63] Foucault, Michel. *The Archaeology of Knowledge*: 1972. p. 46-49
[64] Ibid. p. 117

In the case of language, and its association with discourse analysis, the aforementioned work by Derrida, Laclau, and Mouffe will be referenced again. The biggest point of emphasis to be made is the distinction of language's place within the act of analysis. One has, for instance, the option to view language from the referential point of view wherein the objects in one's environment are signified through language in order to be identified. As a means of discourse analysis, Waever and Hansen reject the use of a referential view of language due to the psychological connotations it has by association with terms like "'perceptions' or 'belief systems' or 'images' in Foreign Policy Analysis"[65] and ultimately commits the researcher to an analytic level of accessing implied meaning and the thought processes made by the author. The alternative to this line of thinking lies in the differential understanding of language in which meaning becomes a derivative from the differentiation between concepts.[66] Herein lies the connection between the previous delineation of discourse and the differential understanding of language. The production of statements forms a system of discourse, and from the system of discourse, the researcher must approach the act of analysis from a frame of reference that allows the researcher to "explain meaning and intelligibility as a function of the text, rather than conversely."[67]

3.2 Research Objective

In his article, *Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War*, Adam Liff offers an excellent quote that partially aids in legitimizing the thematic selection of cyber conflict for this research study:

> "Despite its increasing salience to policymakers and defense planners, the issue of cyberwarfare has not caught the attention of most students of international relations. Much of the limited existing literature has emerged from US war colleges, policy-oriented research institutions, and think tanks and is often under-theorized."[68]

---

[65] Hansen & Waever. *European Integration*: 2003. p. 28-29
[66] Ibid. p. 28-29
[67] Bartelson, Jens. *A Genealogy of Sovereignty*: 1995. p. 70
[68] Liff, Adam P. "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War." *Journal of Strategic Studies* 35, no. 3 (2012). p. 403

Though the use of the term, 'cyberwarfare' is a small controversy in itself, and my personal stance on this issue as a researcher going forward will be explored later in this chapter, Liff raises an important issue by pointing out the glaring gap in the theorization relating to the topic of cyber conflict. Not only is it a beneficial contribution for the world of academia to continuously work towards getting in front of this topic and trying to fill the massive research gaps, but as a researcher in the field of Peace Research it is even more beneficial to look towards making contributions to this field of study from a perspective that is converse to the ones held by researchers from American war colleges, research institutions, and think tanks that Liff mentions. Peace researchers have so far under researched the cyber realm as a legitimate or important theater of conflict from which to envision a movement towards the construction of peace.[69]

The identification of gaps in theory and contemporary research is at the heart of the development process of a research objective. In regards to this topic, George and Bennett explain that the research objective "should be embedded in a well informed assessment that identifies gaps in the current state of knowledge, acknowledges contradictory theories, and notes inadequacies in the evidence for existing theories. In brief, the investigator needs to make the case that the proposed research will make a significant contribution to the field."[70] With that being said, this research study aims at addressing the massively under theorized concept of desecuritization as it relates to the topic of cyber conflict, particularly with the focus of the political discourse within Estonian policy documents.

3.3 Selection of the Case

In terms of the selection of a case and its importance to a research study, or more specifically, its benefit to a research study is well summated by Michael Shapiro in his book *Methods and Nations* in the quote: "Conceptualizations (as opposed to

[69] There are, however, two great pieces of literature aimed at the promotion of the theorization of cyber peace from Scott Schakelford, *Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace*: 2014; and Hamadoun I. Touré, *The Quest For Cyber Peace*: 2011.
[70] George, Alexander, and Andrew Bennett. *Case Studies and Theory Development in the Social Sciences*: 2005. p. 74

generalizations) are best developed in the context of specific historical episodes."[71] Determining the case study that will be used in a research study is an important step in the overall design process. In general, the chosen case is an integral tool to aid in the facilitation of testing a hypothesis and maintaining the path originally laid out in the research objectives of the study. George and Bennett stress the importance of rather than selecting a case for the research plan based off of factors such as the author's level of interest or the availability of source material, the author must accept that, "the primary criterion for the case selection should be relevance to the research objective of the study, whether it includes theory development, theory testing, or heuristic purposes."[72] Thus, it is exceedingly vital for the case selection for this particular research study exhibits a high degree of relevance in relation to the topic of cyber conflict, as well as being an applicable case for the study of desecuritization. Accordingly, the remainder of this subsection will focus on the having a discussion on the process case selection for this research study as well as defending the relevance of the case in relation to the pre-established research objective.

George and Bennett define a research case study as, "a well-defined aspect of a historical episode that the investigator selects for analysis, rather than a historical event itself."[73] In addition to this, the chosen historical event for the case study is considered to be "classes of events" that take place as part of the overall dynamic interaction over the course of time that the case study occurs.[74] In this respect, choosing a case study for this research study requires a specific historical instance of dynamic interaction that remains pertinent to the topic of cyber conflict, while still serving as an event that can be used in the pursuit of applying and observing the concept of desecuritization.

In a preliminary assessment of potential case studies on cyber conflict and security, researchers who study the topic of cyber conflict and cyber securitization will find copious mentions of the cyber attacks that occurred during April and May 2007 that targeted government, media, banking, and internet service provider websites in Estonia. As will be shown in more detail within Chapter 4 of this research study, officials both

[71] Shapiro, Michael J. *Methods and Nations: Cultural Governance and the Indigenous Subject*: 2004. p. 35
[72] George & Bennett. *Case Studies and Theory Development in the Social Sciences*: 2005. p. 83
[73] Ibid. p. 18
[74] Ibid. p. 18

within and outside of Estonia, as well as members of the media and academics have been quick to dub the barrage of cyber attacks on Estonia during the nearly month long period as the first instance of cyber warfare against a sovereign state. Though there have been more recent examples of cyber attacks causing significant damage to a state such as the Stuxnet attack on an Iranian nuclear facility, the Estonian case remains, at the time of writing, the most relevant case study for the examination of an instance in which nearly all security-related sectors came under direct attack from foreign entities for a prolonged period of time. The infancy of the cyber realm being considered as a potential vector for the advancement of military, economic, and political objectives considerably limits the pool of historical instances which can be drawn from as research case studies. As a result of this, researchers in this field are inherently handcuffed to this case study as a means to test different hypothesis related to cyber conflict.

In the pursuit of maintaining consistency with the necessary elements for a case study listed above, it is important to note that the Estonian case exemplifies the classes of events that were previously mentioned as factors that must be included and addressed in the case study selection process. The dynamism of the interaction of different actors related to the Estonian attacks, especially the involvement of the Estonian governmental ministries combined with NATO involvement in the wake of the attacks will stand to be examined as a contextual exemplification of cyber conflict. Additionally, this case will also serve as a justifiable basis for the theoretical application and examination of the desecuritization concept. Finally, the elements that encompass the conceptualization of cyber peace building will be used in reference to the actions taken by both the Estonian ministries of government and the organ of NATO that was established as a response to the attacks that were committed against Estonia, now known as the Cyber Defense Center of Excellence (NATO CCDCOE). The following subsection will go into detail as far as elaborating on the formulation and collection of the data that will be used in conjunction with the case study.

3.4 Data Selection (Inclusion / Exclusion)

Within any field of study, the process of formulating the data that will be used can

potentially be an arduous and heavily selective task. Careful work must be done to make sure that from the vast expanses of sources one can draw from, they are not only relevant to the chosen case, but also useful within the overall context of the research plan. These considerations were extremely important in the instance of choosing the data that would be included, as the discourse on cyber conflict extends globally and permeates disciplines other than just ones based in security studies or peace research. However, the case study that was selected for this research study significantly narrows the field of potential data that can be analyzed. As such, the following subsection will briefly reflect on the selection of the data, particularly covering the reasoning for the inclusion or exclusion of existing potential material.

There has been a wealth of information produced that addresses the aftermath of the Estonian cyber attacks in 2007. These data sources are in the form of news media coverage, policy documents produced by Estonian government ministries, manuals and reports produced by NATO's CCDCOE, academic discourse, and discourse from the community of cyber security professionals. Though one choice could be to do an analysis of this data in order to gain a snapshot of the general response during a specific period of time following the attacks, this is potentially far too great of a task for the scope of a master's thesis. Accordingly, the analysis chapter of this research study will solely address the documents produced by the Estonian government ministries and the NATO CCDCOE from the seven-year period between 2007-2014. In some instances like the Estonia Information Systems Authority (EISA), the production of concise annual reports on cyber security strategy only came about in 2012. Prior to this, EISA produced digital yearbooks covering a myriad of topics beyond just cyber security strategy. Because of this, these sources were intentionally excluded from the analysis.

With this being stated, the primary data that has been selected for this research study includes:

- Cyber Security Strategy (2008 – 2013) [Estonian Ministry of Defense]
- Cyber Security Strategy (2014 – 2017) [Estonian Ministry of Economic Affairs and Communication]
- Tallinn Manual on the International Law Applicable to Cyberwarfare [NATO Cooperative Cyber Defense Center of Excellence]

- National Cyber Security Framework [NATO Cooperative Cyber Defense Center of Excellence]
- 2012, 2013, 2014 Annual Report [Estonian Information Systems Authority]

The information within these documents serves as the basis from which the theoretical framework discussed in the previous chapter will be used as a tool for the goal of assessing the existence or inexistence of desecuritization processes occurring in the wake of the cyber attacks. In this regard, the data analysis is meant to create a space for providing theoretical contributions regardless of whether the Estonian responses to the attacks exemplify processes of securitization or desecuritization.

3.5 Limitations & Considerations

The inclusion and exclusion of each of the above-mentioned sources was consciously made as a result of the necessary tie-in with the framework of Securitization Theory's levels of analysis. As was stated in the previous chapter on theory, Buzan noted that the primary processes of securitization and desecuritization successfully occur on the 'units' and 'international subsystem' levels of analysis. In this regard, the chosen sample data fits well with both the theoretical and methodological framework of this study in the ultimate pursuit of answering the research question. In spite of this general perception of cohesion within the research study, there are admittedly some instances in which there are limitations in the overall research design that must be taken into consideration prior to moving on to the chapters that cover the analysis and discussions of the primary data materials.

Those with a background in the field of Peace Research may question the exclusion of peace-related theoretical underpinnings for this research study as it, in addition to a security-studies perspective, includes similar perspectives to that of Galtungian peace research. In response to this potential inquiry, the issue of scope and ambition for a master's thesis should be quickly addressed. Merging two theoretical and epistemological foundations for a research study, as well as working towards a new theoretical contribution is far too ambitious for the small scope of this type of study. As such, these elements have been consciously omitted from both the theoretical basis of the

study as well as the research strategy. Such academic contributions will be later addressed in the concluding remarks as potential recommendations for future researchers working with this specific thematic research.

One final point of consideration within this methods section is addressing the placement of this research study within the debate over the use of terminology concerning cyber conflict. In particular, this is in reference to the use of terminology that implicates various types of cyber actions as instances of cyber war. Though it will be stated early on that the intention is to place myself as a researcher within a perspective on this debate for the sake of coherent terminology usage throughout the remainder of the text. As such, it must me noted that rather than having the intention of focusing on further developing the terminological coherence within this field of study, the aim of presenting this debate is to curb possible misconceptions regarding the meaning that can later be derived from the analysis of 'cyber conflict' as opposed to 'cyber warfare.'

On one side of this argument you have a loosely related cohort of academics, military leaders, and governmental personnel who fall somewhere within a spectrum that extends from casual to incendiary usage of the term 'cyber war'.[75] The other side of the terminological debate is primarily composed of academics working to base actions in the cyber context within pre-existing understandings of terms like 'attacks', 'conflict', and 'war' especially. The most notable of these academics whom shun the usage of the war simile is Thomas Rid, whose journal article, *Cyber War Will Note Take Place* stands as a compelling argumentative piece aimed at cautioning against the prevalence of attributing nefarious cyber actions as examples of warfare. Based in a perspective of war from the Clausewitizian definition of war, Rid breaks war down into three different necessary elements and attempts to make a connection to the known and theorized capacities of cyber attacks. The three elements listed in the text include: the inherent existence of violence in war, the instrumentality of war wherein force is the means by which the submittal of the defensive entity to the offensive entity is the end, and finally war, at its core, is transcendent of the perpetration of force as it serves as an extension of politics.[76]

---

[75] See: Clarke & Knake. *Cyber War*: 2012; Liff. *Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War*: 2012; Stone, *Cyber War Will Take Place*: 2013.
[76] Rid. *Cyberwar Will Not Take Place*: 2012. p. 8

With these three necessary elements established, Rid follows with the succinct expression that "there is no cyber offense that meets all three criteria."[77]

The biggest question left to answer then is, 'why does the current conceptualization of cyber attack not meet the criteria to constitute actual instance of warfare?'. When it comes to the element of violence, the biggest detriment to the cyberwar argument is the lack of physical damage resulting from the attack, especially damage manifest as a body count as a result of the attack. Perhaps the most glaring factor in relation to the cyber war debate is that a cyber attack has yet to cause a human casualty. Though physical damage to a power plant was caused in the Iranian Stuxnet attacks (covered in chapter 4), this represents only one instance within a countless list of cyber attacks that have been committed.[78] Additionally, on the topics of the instrumentality and political extension of warfare, the common theme of nebulous emanation of attack creates a problematic for the attribution of war terminology.

The three biggest examples of cyber attack: Estonia (2007), Georgia (2008), and Iran (2010) are examples of attacks with relative ease of attribution to the attacking entity, but without any major entity actually taking credit for the attacks. The case for these attacks as extensions of political will is strong, but the instrumentality of these attacks is still quite weak. These major cyber attacks have remained just singular instances of aggression. There was no submittal by the defensive entity to the attacker, and the aggression ended as quickly as it began. So, to summate having assessed the parameters of war, and assessed their applicability to known cases that can be potentially seen as examples of cyber war, the use of this terminology within this research study will not be used on two accounts. First, being that neither of the arguments for and against the use of 'cyber war' are solidly grounded, there appears to be more work needed for a deeper conceptualization of the term before it can be used definitely in cyber discourse (an endeavor that will not be taken up within this study). Second, there is little benefit to the legitimacy of this study to refer to the case study of the Estonian attacks as war against the Estonian state when this claim is illegitimate in itself.

---

[77] Ibid. p. 10

[78] Rid cites no damage ever being done to a building as a contributor to his argument that cyber attacks are not violent, but his text was written prior to the widespread distribution of information on the extent of damage caused in Iranian attacks.

4.1 Cyber Infrastructure

Prior to discussing the topics of cyber infrastructure, cyber conflict, and cyber security, it is hepful to establish some fundamental understandings about the basic structure of the internet, what is meant by the term 'cyber infrastructure', and how cyber attacks are actually carried out. The first topic, cyber infrastructure, requires a brief synopsis of the initial formulation of the Internet and the development of its operational framework. From the establishment of the basic timeline of cyber infrastructural development, the key phraseology relating to cyber conflict as well as the technical pathology by which cyber attacks are perpetrated can be further elaborated on in order to provide a higher degree of coherence in the presentation of the case study on the cyber attacks against Estonia in 2007.

Understanding the structural framework of the Internet begins with the United States' Department of Defense's Advanced Research Projects' Network (ARPANET) that was developed in 1959 as a communication network between four computers at University of California Los Angeles, Stanford University, University of California Santa Barbara, and University of Utah.[79] ARPANET was based on the process of packet switching between computers in different locations in order to form a network for communication. Packet switching, in the most basic terms, is a process in which information is broken down into 'packets' that can be delivered across a network more quickly and easily than if the information is delivered in its whole form, and then the packets of information are subsequently reassembled into their original form upon arrival at the desired destination.[80]

The network model originally created by ARPANET continued to grow in size over time from a closed singular network to the model similar to the Internet as it is known today in which there are numerous interconnected networks, and later adopted a set of standardizing design protocols known as "Transmission Control Protocol and Internet Protocol (TCP / IP)" in order to develop a more functional form of

[79] Shackelford, Scott. *Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace*: 2014. p. 21
[80] Murray, Andrew. *Information Technology Law: The Law and Society*: 2010. p. 17

communication within the networks.[81] TCP/IP essentially functions as common language of the Internet that allows for computers within a network to communicate with one another regardless of differentiating operating systems, hardware, and software.[82] The TCP/IP system is important not only due to the fact that it allowed for significantly increased levels of efficiency in information sharing within a network, but it also has greater implications in terms of the eventual commission of cyber attacks. Scott Shackelford asserts that because the TCP/IP system reconstructs packet sizes uniformly in order to allow any network to easily distribute them, this process consequently "[sets] the stage for cyber attackers masking attribution" as attacking users can easily employ different methods with the purpose of changing their apparent IP address to avoid attribution for the attack.[83] Additionally, as will be discussed in more detail in the section outlining modes of cyber attack, certain cyber attacks like Denial of Service attacks, for example, target the IP address of a chosen website in order to cause it to be unable to be accessible to other users.

In the early days of the Internet's development, IP addresses were the primary way in which an Internet destination was designated. IP addresses are commonly written out in a dotted decimal notation.[84] For instance, the IP addresses associated with the University of Tampere at the time of writing are on a range of: 153.1.0.0 – 153.1.255.255. However, for the vast majority of contemporary Internet users, the use of an IP address as a means of accessing an online destination has become irrelevant as a result of the development of the Domain Name System (DNS). Rather than a user looking to access the University of Tampere's website via the specific IP address, the DNS allows for a simpler pathway for user access; in this case www.uta.fi is the specified domain name of the university's website.

Internet infrastructure is entrenched within a system of code, and the way in which code is written facilitates how interactions occur online. Since the early 1990s the Internet Engineering Task Force (IETF) has largely overseen the maintenance of the Internet's structure and functionality. The IETF simply defines their mission by saying,

---

[81] Shackelford. *Managing Cyber Attacks in International Law, Business, and Relations*: 2012. p. 21
[82] Blank, Andrew. *TCP/IP Foundations*. Sybex: 2004. p. 2
[83] Shackelford. *Managing Cyber Attacks in International Law, Business, and Relations*: 2012. p. 24
[84] Ibid. p. 26

"The goal of the IETF is to make the Internet work better. The mission of the IETF is to produce high quality, relevant technical and engineering documents that influence the way people design, use, and manage the Internet in such a way as to make the Internet work better. These documents include protocol standards, best current practices, and informational documents of various kinds."[85] One example of the major contributions to the operational framework of the Internet made by the IETF is seen in their involvement with the development of the 'text/html' media format that a significant amount of the Internet is based in.[86] On the subject of their involvement in the development of this pillar of web infrastructure, the IETF write, "HTML has been in use in the World Wide Web information infrastructure since 1990, and specified in various informal documents. The text/html media type was first officially defined by the IETF HTML working group in 1995 in [HTML20]."[87] The IETF is a representative example of how the Internet's operational framework is in a perpetual state of flux and expansion. In the most basic summation, the core infrastructural backbone of the Internet is based in code that aims to facilitate communication within and amongst networks.

Finally, the connection between the topic of cyber infrastructure and that of the critical infrastructure of the state is an important one to be made. In the pursuit of defining what is meant by the term 'critical infrastructure' of the state, I refer to the 1997 "Marsh Report" drafted by the Committee on Critical Infrastructure Protection for former United States President Bill Clinton regarding the necessity for the protection of critical infrastructure with respect to the United States continued electronic integration of state infrastructure. In this report, committee chairman Robert Marsh both defines critical infrastructure of the state, and then refers to its interconnection of cyber infrastructure by writing:

> "national defense, economic prosperity, and quality of life have long depended on the essential services that underpin our society. These critical infrastructures—energy, banking and finance, transportation, vital human services, and telecommunications—must be viewed in a new context in the Information Age. The rapid proliferation and integration of telecommunications and computer systems have connected infrastructures to one another in a complex network of interdependence.

[85] Alvestrand, Harald. "A Mission Statement for the IETF." October 1, 2004.
[86] Connolly, Dan. "The 'text/html' Media Type." June 1, 2000.
[87] Ibid.

This interlinkage has created a new dimension of vulnerability, which, when combined with an emerging constellation of threats, poses unprecedented national risk."[88]

Though the listed facets of critical infrastructure have always existed before the onset of the so-called "Information Age", the networked cyber integration of these infrastructural sectors has opened up the possibility for nefarious action against a state, specifically with the possibility for existential threat to the state and its citizenry depending on the scale of the infrastructural breakdown, but now with the reality that such actions can be performed independently of location. The networked nature of these infrastructural sectors is essential to the potentiality for threat against human life as large-scale breakdowns in one sector, like a power grid failure from a cyber attack, can lead to a "domino effect" in which multiple critical components of the state systematically break down and severely exacerbate the harmful effects of the cyber attack.[89]

4.2 Modes of Cyber Attack

In order to fully understand the idea of cyber conflict, it is essential to receive a well-developed presentation of the various modes of attack that can be committed between cyber actors. One can simply refer to the existence of cyber attacks, but understanding how the different sectors of critical state infrastructure can be attacked and subsequently disabled requires some exemplification of attack methodology. In addition to the presentation of these attacking methodologies, it will be within this section that the terminological use of 'war' and 'weaponry' in relation to the cyber domain will be addressed. Terms like cyber war and cyber weapons are used significantly often in the discourse pertaining to the field, and thus require a brief mention for the purpose of distinguishing between what constitutes war, versus what constitutes and attack, as well as the general viability of using the term 'cyber war' at all in this study demands addressing. Also, the viability of labeling various modes of attack as examples of cyber weaponry that can be used against a state must be discussed prior to moving into an analysis of the Estonian case study. Accordingly, the following sub-section will be

[88] Marsh, Robert. "Critical Foundations Protecting America's Infrastructures." The Report of the President's Commission on Critical Infrastructure Protection. October 13, 1997. p. ix
[89] Estonian Ministry of Defense. "Cyber Security Strategy." Cyber Security Strategy Committee. 2008.

organized so as to first list and define the attack methodologies, and subsequently survey the delineations between the different attack typologies.

Distributed Denial of Service (DDoS) attacks are easily the most important method of cyber attacks for this study to examine, as it was through the employment of DDoS attacks that the large majority of damage was done in the case study cyber attacks against Estonia in 2007. DDoS attacks manifest in various forms, as will be discussed further in the following introductions to flood attacks, and are the contemporaneously preferred method for cyber attacks. Shackelford points out that DDoS attacks are the most logical choice of cyber attacks due to the extreme ease of perpetration and cost efficiency when compared to more advanced types of attacks; DDoS attacks namely being particularly inexpensive with a high potential to inflict costly damage to a victim.[90] The way in which DDoS attacks work is that they overload targets with millions of connection requests (similar to a user refreshing a website thousands of times in a minute) in order to use up the servers allotted amount of bandwidth that would be able to handle the requests. The result of the sudden influx of connection requests is that service for all normal users is denied due to the inability of the server to cope with additional requests.

The element of DDoS that designates it as 'distributed' is the incorporation of botnets to amplify the scale and damaging capacity of the attack. Botnets are simply a network of computers that can be taken control of to serve the purpose of a single attacker. The size of a botnet can vary greatly in size, and most importantly the users of the computers being used in the botnet are unaware of the existing software on their computer that allows for it to be controlled by another user. Botnets can be taken control of by various means. Computer security company Symantec has stated that criminally renting a botnet can cost "as little as $100-$200 per day."[91] In addition to the use of botnets, individuals can assist others in a DDoS attack on a voluntary basis through the use of an open source program like Low Orbit Ion Cannon (LOIC) wherein the user can select a targeted IP, and the program facilitates an influx of a large amount of "connect

[90] Shackelford. *Managing Cyber Attacks in International Law, Business, and Relations*: 2012. p. 140
[91] G., Tim. "Renting a Zombie Farm: Botnets and the Hacker Economy." Renting a Zombie Farm: Botnets and the Hacker Economy. August 8, 2014. [Author's full last name was withheld on Symantec's website.]

requests" as a contribution to the other botnets concomitantly enlisted to attack the target.[92]

Another oft-employed method for cyber attackers is referred to as 'flood attacks.' Flood attacks are technically within a subcategory that also falls under the umbrella heading of Denial of Service (DoS) attacks, as they primarily operate as a means to overwhelm a target in order to render it unable to be accessed or used as it normally would. What differentiates these from that of DDoS attacks is that they are performed by single entities, and thus do not possess a distributed nature. Flood attacks can be broken down into two different methodologies: Internet Control Message Protocol (ICMP) and TCP SYN floods.[93] ICMP floods (also referred to a 'smurfing') are a method for attack in which a targeted IP address is sent to an IP broadcast server, and from there numerous other IP addresses receive information packets from the targeted IP. The result of this broadcast is that the IPs receiving the information packets will reciprocate the attempted communication to the original source, but due to the large amount of foreign IPs participating in this reciprocation of packet distribution, the originally targeted IP becomes overwhelmed with a sudden influx of information. Due to the sudden influx of information the target will become bogged down in its operational capacity until the flood has subsided.

TCP SYN floods differ greatly from ICMP floods in that rather than flooding an individual target directly, SYN floods work to overwhelm a server so that others can no longer access the server. The key to understanding how this type of attack works is to first understand the 'Three-Way TCP Handshake' (stylized as SYN > SYN-ACK > ACK).[94] In attempting to make a TCP connection, a segment of information must first be sent to a server. This represents the SYN part of the handshake and is point at which this type of connection can be exploited in order to disable use of a server. The IETF clarifies how a flood of SYN requests can be exploited in explaining, "The goal is to send a quick barrage of SYN segments from IP addresses … that will not generate replies to the SYN-

[92] Moses, Asher. "The Aussie Who Blitzed Visa, MasterCard and PayPal with the Low Orbit Ion Cannon." The Age. December 9, 2010.
[93] Richards, Jason. "Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security." International Affairs Review.
[94] Microsoft Support. "Explanation of the Three-Way Handshake via TCP/IP." Explanation of the Three-Way Handshake via TCP/IP. February 12, 2010.

ACKs that are produced. By keeping the backlog full of bogus half-opened connections, legitimate requests will be rejected."[95]

Though the aforementioned modes of attack have the potentiality for causing damaging effects on networked targets both in the public and private sector, a more recent and more destructive method of cyber attack has manifest itself as the so-called 'Zero-Day Exploits.' According to Shackelford, zero-day attacks occur as a result of the discovery of a massive error in software yet to be known to the users or developers, which is then exploited in order to satisfy the goals of the attacker.[96] One particular zero-day attack that has garnered a significant amount of international attention is the Stuxnet infection. The Stuxnet infection was originally discovered in 2010 by Belarusian anti-virus company Virusblokada as a piece of malware with an unknown purpose or destination. Throughout the summer of 2010 numerous other anti-virus and computer forensics teams around the world went to work in order to discover what the purpose of the infection was.

One of the central figures in the investigation of Stuxnet is Ralph Langer, who explained in a TED talk regarding the Stuxnet infection that his computer forensics team soon revealed that the infection was designed specifically to target the Natanz Fuel Enrichment Plant in Iran.[97] From this revelation it was also revealed that Stuxnet specifically targeted the uranium enrichment centrifuges at the plant, causing them to operate at unsafe levels, while simultaneously working to intercept the data readouts at the enrichment plant and provide inaccurate data that indicated normal operation of the centrifuges.[98] The Stuxnet infection proved to be a successful venture for the developers of its code as it infiltrated devices in the Natanz plant by taking advantage of four different zero-day exploits.[99] For the Natanz plant, the Stuxnet infection resulted in having "wiped out roughly a fifth of Iran's nuclear centrifuges and helped delay, though not destroy, Tehran's ability to make its first nuclear arms" according to an article

---

[95] Eddy, W. "RFC 4987 - TCP SYN Flooding Attacks and Common Mitigations." RFC 4987 - TCP SYN Flooding Attacks and Common Mitigations. August 1, 2007.
[96] Shackelford. *Managing Cyber Attacks in International Law, Business, and Relations*: 2012. p. 141
[97] Langer, Ralph. "Cracking Stuxnet, a 21st-century Cyber Weapon." TED. March, 2011.
[98] Ibid.
[99] Collins, Sean, and Stephen Mccombie. "Stuxnet: The Emergence of a New Cyber Weapon and Its Implications." *Journal of Policing, Intelligence and Counter Terrorism* 7, no. 1 (2012). p. 86

chronicling the attacks in the New York Times.[100] In this regard, Stuxnet was a turning point in the speculation surrounding the destructive capacity for cyber attacks as it resulted in physical damage to state infrastructure.

[100] Broad, William, John Markoff, and David Sanger. "Israeli Test on Worm Called Crucial in Iran Nuclear Delay." The New York Times. January 15, 2011.

5.1 The Case: Estonia, 2007

In Tallinn, the capital city of Estonia, there stands a Soviet-era World War II memorial in the form of a bronze Red Army soldier. The bronze solider memorial serves as a commemoration of the fallen Soviet soldiers that died fighting the Nazis in the Estonian region. Following the Estonian attainment of independence, the monument was the source of a significant amount of ire and provocation for Estonians, as it was perceived to be representative of Soviet occupation and oppression that followed the end of the Second World War. As a result of the controversy that the bronze soldier drew, the Estonian government decided to move the memorial away from its original location, at Tõnismägi Park in the city center of Tallinn, to a new location within the Defense Forces' Cemetery of Tallinn, which is located further away from the city center. The movement of the bronze solider is representative of the breaking point amongst those divided by ethnically Russian and Estonian perspectives on the meaning attributed to the soldier memorial. The actions taken by the Estonian government in April 2007 to remove the bronze soldier memorial had two subsequent results: tangible and non-tangible protest. In terms of tangible protest, the ethnically Russian Estonians held demonstrations in Tallinn to voice their displeasure with the decision to remove the memorial in which numerous protestors clashed with the Estonian authorities. The demonstrations occurred over April 26th and 27th and with the protests taking on a violent turn, subsequently resulted in the arrests of 1,300 people, and another 100 injuries with one resulting in a fatality.[101]

More importantly though, the protest against the Estonian government concomitantly manifest itself in the intangible sense through the employment of cyber attacks against various facets of critical Estonian cyber infrastructure. The cyber attacks were initiated immediately following the suppression of the street demonstrations on April 27th. The attacks initially began with relatively simplistic methods of ping flooding and DDoS attacks against various Estonian websites. Instructions on how to go about using these methods of attack were distributed on Russian-language online forums and Internet Relay Chatrooms (IRC) in order to allow less technologically advanced activists

[101] Rid. "Cyber War Will Not Take Place": 2012. p. 11

to assist in the large-scale DDoS attacks against Estonian government websites.[102] For some users, participation in the attacks was as simple as launching an executable .bat file that was distributed through the aforementioned communication channels.[103] In one description of the extent of attacks on the government websites, Peter Finn of the Washington Post writes, "The Web sites of the Estonian president, the prime minister, Parliament and government ministries were quickly swamped with traffic, shutting them down. Hackers defaced other sites, putting, for instance, a Hitler mustache on the picture of Prime Minister Andrus Ansip on his political party's Web site."[104] Despite these initial successes on the part of the attackers, the CCDCOE described the first days of the attack as "simple, ineptly coordinated, and easily mitigated."[105]

The cyber attacks continued to grow in scale and intensity over the following days as the attackers employed more advanced methods. April 30th marked the turning point in the cyber attacks wherein botnets were introduced as a mode of attack in order to sustain the large-scale DDoS attacks that had occurred over the previous two days. The Estonian minister of defense, Jaak Aaviksoo estimated the number of drone computers that encompassed the botnet used on April 30th was at least one million. The computers used in the botnet were located in states spanning the globe, including "The United States, China, Vietnam, Egypt, and Peru."[106] In the days following the end of the attacks, it was estimated by Arbor Networks that the total number of locations that housed computers used in the botnet attacks on Estonia to be about 178 different countries.[107] The e-mail servers used by public officials were also targeted during the first few days of the attacks. The mode of attack in this instance was a mass distribution of spam e-mails, and in the case of the parliamentary members' e-mail server, the inability to cope with the massive influx of usage caused there to be a twelve hour period in which the service was unavailable for members of parliament.[108]

---

[102] Finn, Peter. "Cyber Assaults on Estonia Typify a New Battle Tactic." Washington Post Foreign Service. May 19, 2007.
[103] Tikk, Eneken, Kadri Kaska, and Liis Vihul. "International Cyber Incidents: Legal Considerations." Cooperative Cyber Defence Centre of Excellence (CCD COE): 2010. p. 18
[104] Finn "Cyber Assaults on Estonia Typify a New Battle Tactic." 2007.
[105] Tikk, Kaska, Vihul. International Cyber Incidents: Legal Considerations.": 2010. p. 19
[106] Finn "Cyber Assaults on Estonia Typify a New Battle Tactic." 2007.
[107] Tikk, Kaska, Vihul. International Cyber Incidents: Legal Considerations.": 2010. p. 23
[108] Finn "Cyber Assaults on Estonia Typify a New Battle Tactic." 2007.

Soon after the commencing days of the attack, the private communications sector began to experience the brunt of the effects of the botnet usage similarly to what was being felt by government-related websites. At this point, the targeted websites no longer included only government related domains, and had expanded to target Elion, Elisa, and Starman routers and domains to cause widespread service disruptions and loss of connectivity within Estonia, at one point resulting in a brief period of simultaneously complete service denial for all Elion users.[109] The simultaneous targeting of the Estonian news media by the attackers further exacerbated the situation in Estonia. The CCDCOE claims that "three of Estonia's six largest news organizations and news portals (including Postimees.ee, Delfi, EPL Online, Baltic News Service)" were significantly affected in their ability to keep their websites online during the attacks.[110] With Estonia's largest news publications being attacked at once, both people trying to access the websites through Estonian IP addresses, and those accessing from foreign IP addresses were continuously denied access to Estonian media reports on the progression of the attacks throughout multiple days of the attacks.

The cyber attacks continued steadily from the night of April 27th to early hours of May 9th at which point the volume of incoming traffic ascended to its highest point of the multi-week barrage. The significance of the May 9th date is that it is the date in which Russia celebrates Victory Day in honor of the Soviet victory over Nazi Germany's forces in World War II, which is indicative of the poor timing chosen by the Estonian to remove the bronze soldier monument so closely to the holiday that also commemorates the Soviet soldiers involved in the fighting. Upon the arrival of 23:00 EET in Tallinn, or 00:00 MSK (Moscow time) on May 9th, the volume of incoming attacks on Estonian cyber infrastructure increased by 150% in comparison to previous days' numbers.[111] In addition to increased attacks on government websites, the arrival of the May 9th holiday also marked the incipience of attacks that specifically targeted the web-based economic infrastructure of Estonia. Two of the primary targets for the attackers were the largest banks in Estonia, Hansapank and SEB Eesti Ühispank, who own an estimated 75-80% of

[109] Tikk, Kaska, Vihul. International Cyber Incidents: Legal Considerations.": 2010. p. 19
[110] Ibid. p. 22
[111] Ibid. p. 20

the Estonian banking market share.[112] Throughout the remainder of the attacks (the last official wave of attacks is May 18th, 2007 with a few sporadic disruptions following) the Estonian online banking services experienced numerous periods of denial of service attacks that resulted in the inability of bank customers to access their online banking services.

In the wake of the Estonian cyber attacks, DDoS mitigation specialists and researchers, Arbor Networks ran an analysis of the DDoS attacks against Estonian websites from the April 27th onset until May 17th in order to quantitatively assess multiple aspects of the attacks. As far as the volume, type, and distribution of the attacks, Arbor Networks researcher Jose Nazario writes, "We've seen 128 unique DDoS attacks on Estonian websites in the past two weeks through ATLAS[113]. Of these, 115 were ICMP floods, 4 were TCP SYN floods, and 9 were generic traffic floods. Attacks were not distributed uniformly, with some sites seeing more attacks than others:[114]

Attacks	Destination	Address or owner
35	"195.80.105.107/32″	pol.ee
7	"195.80.106.72/32″	www.riigikogu.ee
36	"195.80.109.158/32″	www.riik.ee, www.peaminister.ee, www.valitsus.ee
2	"195.80.124.53/32″	m53.envir.ee
2	"213.184.49.171/32″	www.sm.ee
6	"213.184.49.194/32″	www.agri.ee
4	"213.184.50.6/32″	*(Dept of Data & Communications)*
35	"213.184.50.69/32″	www.fin.ee (Ministry of Finance)
1	"62.65.192.24/32″	*(Starman ISP)*

[Source: http://www.arbornetworks.com/asert/2007/05/estonian-ddos-attacks-a-summary-to-date/ (Accessed 11.3.15) Italicized text does not appear in the original publication.]

[112] Ibid. p. 22
[113] Arbor network's Active Threat Level Analysis System (ATLAS) is a free public portal made for the purpose of analyzing ongoing denial of service attacks and threat sources. (https://atlas.arbor.net/).
[114] Nazario, Jose. "Estonian DDoS Attacks – A Summary to Date." Arbor Networks DDoS & Security Reports: The Arbor Networks IT Security Blog. May 17, 2007.

The table presented by Arbor Networks clearly shows the distribution of attacks depending on what web locations were deemed by the attackers to be the primary targets. The targeted locations with at least thirty-five unique attacks represent the main governmental websites that include the website of the parliament and prime minister, as well as the websites for the Ministry of Finance and the Department of Data Communications, Estonian Informatics Center. In addition to the location data analysis done by Arbor networks, they also provide information regarding the length of time the unique attacks occurred for, as well as the size (measured in megabits per second and abbreviated as: 'Mbps') of the attacks.

Attacks	Length
17	<1 minute
78	1 min - 1 hour
16	1 hour - 5 hours
8	5 hours - 9 hours
7	10 or more hours

Attacks	Bandwidth Size
42	Less than 10 Mbps
52	10 Mbps - 30 Mbps
22	30 Mbps - 70 Mbps
12	70 Mbps - 95 Mbps

[Source: http://www.arbornetworks.com/asert/2007/05/estonian-ddos-attacks-a-summary-to-date/ (Accessed 11.3.15)]

Arbor Networks' numbers presented in the tables above are very revealing in terms of evidencing the technical capacity and goals of the attackers. Though the larger total numbers of attacks on the spectrum of short duration and low bandwidth size point to widespread involvement of less technically advanced attackers following the directives that were sent out over IRC and forum posts, it is the numbers on the larger end of the size and length spectrum of the attacks that are the most revealing. Arbor Networks mentions that an aggregate bandwidth of 100 Mbps for a cyber attack is the maximum size that is measured by ATLAS, and that ten of the attacks that fell into the '70 Mbps – 95 Mbps' range registered at a size of 90 Mbps and additionally lasted at or near ten hours in total length of time.[115] Thus, these attacks that are on the extreme end of the spectrum are emblematic of a contingent amongst the conglomerate of attackers that

[115] Nazario. "Estonian DDoS Attacks – A Summary to Date." May 17, 2007.

possessed both an elevated level of technological capability and direct intent to inflict a large amount of damage to the Estonian cyber infrastructure.

The final step in the contextualization of the Estonian cyber attacks is to briefly cover the discourse relating the attribution of the perpetrators of the attacks. Due to the consideration of the factors of: the attacks occurring immediately following the movement of the bronze solider monument, the instructions for carrying out the attacks posted in Russian on Russian websites, and the May 9th attacks commencing at midnight in the Moscow time zone, the easy generalization is to assume that the attacks were committed by an unknown entity within Russia. Though no Estonian officials actually go as far as to assign blame directly to Russian citizens or the Russian government, there was still a high level of insinuation by some Estonian officials. The Estonian Prime Minister at the time of the attacks was quoted as saying, "the continuing cyber-attacks from the servers of Russian state authorities … indicates that our sovereign state is under a heavy attack."[116] However, Merit Kopli, the editor of an Estonia newspaper targeted in the attacks was less diplomatic about assigning blame for the attacks by saying that there was "no question" that "the cyber attacks are from Russia."[117]

In the pursuit of identifying the origin of the attacks, IT professionals can sometimes rely on the IP addresses of the incoming attacks. In the Estonia attacks, many attacking IPs came from Russia, and as mentioned by the Estonian Prime Minister Ansip's speech, some attacking IPs actually belonged to Russian government state institutions.[118] However, it must be noted that using the incoming IPs is not always as reliable as it sounds because of the possibility for an attacker to mask their identity through a process known as 'IP spoofing' in which a user selects an alternative IP (ex. a known Russian governmental IP address) and conceals their identity during the attack while simultaneously leaving misleading digital footprints back to a user whom did not actually participate. In addition to this method, the employment of Virtual Private Networks (VPN) similarly allows a user to be able to reroute their original IP address over a network, which then changes the user's IP address to appear as though it is

[116] Anderson, Nate. "Massive DDoS Attacks Target Estonia; Russia Accused." Arstechnica. May 14, 2007.
[117] Traynor, Ian. "Russia Accused of Unleashing Cyberwar to Disable Estonia." *The Guardian*, May 17, 2007.
[118] Ibid.

actually from another country of origin. Hypothetically speaking, the IP addresses that appeared to have come from Russian sources may have actually been from another state, but the user was using a VPN to mask their origin. Thus, there is an extreme difficulty to immediately assign blame to a state or group within a state for a cyber attack until more work has been done in terms of forensics to make an attempt at unveiling the true origins of those committing cyber attacks.

Mikko Hyppönen, a Finnish IT expert from the Helsinki-based computer security company F-Secure commented on the attacks alleged perpetration by Russian authorities by saying, "In practice there is just one IP address that leads to a government computer. It is of course possible that an attack was launched from there, too, but the person behind it could be anyone, from the son of some ministerial janitor upwards"[119] and added that the Kremlin is more than technically capable to carry out more devastating attacks than what Estonia experienced during the month of attacks.[120] Soon after the attacks, a further connection between Russia and the attacks was made when a leader within the Russian youth nationalist group, 'Nashi' named Konstantin Goloshokov took credit for participating in the attacks, as well as a Tallinn-based student named Dmitri Galushkevich.[121] The latter of these two self-proclaimed attackers was later convicted in Estonia for taking part in the attacks. Though the general consensus in the years following the cyber attacks is that the perpetrators were primarily Russian-based politically motivated activists, there has been neither an official attribution of responsible persons, nor any large-scale prosecutions of persons involved in the cyber attacks. The lack of arrests for the attacks other than the singular case in Estonia is indicative of the overwhelming difficulty that exists for victimized governments have in attempting to locate the origins of attacks with certainty.

5.2 Primary Data

The remainder of this chapter will reintroduce the primary data first mentioned in the methodology chapter, and subsequently provide an analysis and discussion of these

[119] Anderson. "Massive DDoS Attacks Target Estonia; Russia Accused." Arstechnica. May 14, 2007.
[120] Traynor. "Russia Accused of Unleashing Cyberwar to Disable Estonia." *The Guardian*, May 17, 2007.
[121] Tikk, Kaska, Vihul. International Cyber Incidents: Legal Considerations.": 2010. p. 23

documents in relation to research objective. More concisely, the intention of this chapter is to serve as a place for the examination of the discourse emanating from post-cyber conflict Estonia, and a discussion regarding the existence or potential for desecuritization processes relating to cyber conflict. For the sake of organization, the documents will be introduced as two separate, but equally important categories. The first category will include the documents produced by the NATO CCDCOE, and the second will be cyber security-related documents that were published by the Estonian Ministry of Economic Affairs and Communication, Ministry of Defense, and the Information Systems Authority. Chronologically speaking, only the documents from the Information Systems Authority will be presented in the order they were published as these are annual reports, and are the only primary data that can be used to reference alterations in discourse over time.

5.2.1 NATO CCDCOE

The first document to be analyzed is the *National Cyber Security Framework Manual*, edited by Alexander Klimburg, and published by the NATO CCDCOE in 2012. Firstly, the text is positioned by the authors in a way in which it is not meant to serve as document that suggests policy decisions for the members of NATO. Instead, it is a theoretically based interpretation of cyber security. Within the introduction of the document, Klimburg explains, "the 'National Cyber Security Framework Manual' does not strive to provide a single universally applicable checklist of things to consider when drafting a national cyber security strategy. Rather, it provides detailed background information and theoretical frameworks to help the reader understand the different facets of national cyber security, according to different levels of public policy formulation."[122] In regards to the theoretical basis for the framework manual, the CCDCOE base themselves partly in a perspective derived from the Copenhagen School's Securitization Theory.[123] The large portion of Klimburg et al.'s theoretical viewpoint comes from their conceptual development of 'National Cyber Security.' As a result of the way in which

[122] Klimburg, Alexander. "National Cyber Security Framework Manual." NATO CCDCOE. 2012. p. XV
[123] Ibid. p. 49. See note 168.

this text positions itself as offering somewhat of an analytical perspective on the operational nature of cyber security, it serves as a great starting point for the data analysis of which can be referred to in the comparison to the state documents from the Estonian ministries.

Klimburg et al.'s National Cyber Security (NCS) framework is a multi-layered approach to security analysis in which their levels of analysis (labeled 'stake holders' in their text) include private units, state governments, and international subsystems, and their sectoral analysis is broken down into military, political, economic, and societal relationships with cyber interaction.[124] As such, the authors define NCS by stating the following:

> "'The focused application of specific governmental levers and information assurance principles to public, private and relevant international ICT systems, and their associated content, where these systems directly pertain to national security.'" [125]

In addition to this, the understandings of national security and cyber security are explored in the text in order to further assess the definitive understanding of NCS. From a survey of the strategy documents produced by France, Britain, Germany, Canada, and Australia in 2008 Klimburg et al. claim that the political discourse surrounding the topic significantly blurs the line that separates the security focus of the national level with that of the international level, leading the authors to see a trend towards states understanding general cyber security and national cyber security analogously.[126] The most important revelation to come from Klimburg analysis of NCS strategy was that the contemporary focus of the states that were surveyed in the year following the Estonian cyber attacks indicated that the primary goal has been to shore up domestic threat deterrence capabilities.[127] This internally facing focus for state cyber strategy also indicates that there is little initiative being taken to better a state's exploitative capacity in the

[124] Ibid. p. XVI. See Table 1.
[125] Ibid. p. XVI
[126] Ibid. p. 21-28.
[127] Ibid. p. 28-29.

international theater.[128] However, there are obvious cases in which this is not the case, particularly when it comes to the strategic foci of the major hegemonic powers.

Once the CCDCOE's understanding of the term NCS has been established in the first section of the framework manual, Klimburg et al. move to elucidate their 'Five Mandates of National Cyber Security.' Though they chose to use "mandates", this portion of their document is clearly reminiscent and influenced by the sectoral analysis that is presented in the Copenhagen School texts. The five mandates laid out by the CCDCOE include: 'Military Cyber', 'Counter Cyber Crime', 'Intelligence and Counter Intelligence', 'Critical Infrastructure Protection and national Crisis Management', and 'Cyber Diplomacy and Internet Governance'.[129] At this point, it is extremely beneficial to give a brief summation of these mandates in order to begin the process of establishing trends within the documents that have been chosen for analysis.

The Military Cyber mandate is referent to the development of state capacities within the cyber sector with the intention of developing offensive and defensive military actions. Though NATO admits that as many as 120 countries are looking into advancing their technical capabilities, should the perceived necessity for militaristic cyber actions arise, this is in regards to the incorporation of cyber actions into greater military action rather than solely waging war through cyber means.[130] Similarly, the Intelligence and Counter-Intelligence mandate has strong ties to the military sector. Another name that is commonly associated with this mandate is 'Cyber Espionage.' In the most basic sense, cyber espionage is a tactic of unlawfully taking intellectual property, particularly intellectual property of the government and military. Though not referenced in this summated explanation of the Intelligence and Counter-Intelligence mandate within the NATO text, this cyber tactic has garnered more attention following the theft of United States military aircraft design plans through cyber espionage. In this regard, Klimburg et al. write, "Cyber espionage, when directed toward states, also makes it necessary to develop specific foreign policy response mechanisms capable of dealing with the inherent ambiguity of actor-nature in cyberspace."[131]

---

[128] Ibid. p. 28-29
[129] Ibid. p. 32-24
[130] Ibid. p. 32
[131] Ibid. p. 33

The Counter Cyber Crime mandate has a strong connection to the aforementioned Intelligence mandate in that both are positioned around the theft of intellectual property.[132] However, this mandate has more to do with the economic and societal sectors of security analysis than with the military sector. Klimburg et al. admit that upon the preponderance of the discourse related to cyber criminal activity, the actions referenced in this mandate have yet to pose the same level of threat to conflict on a state versus state level, even shunning conventional association of terrorism with any past exemplifications of cyber criminal activity.[133]

As the meaning of critical cyber infrastructure has already been established, it is not necessary to preface Klimburg et al.'s mandate terminology in so far as discussing Critical Infrastructure Protection (CIP). However, National Crisis Management's cyber tie-in requires slightly more explanation. Klimburg et al. cover this by saying, "National Crisis Management must be extended by an additional cyber component. This includes institutional structures which enhance the cooperation between state and non-state actors both nationally and internationally, as well as a stable crisis communication network and an applicable legal framework to exchange relevant information."[134] The development of a legal framework regarding cyber interaction is then built upon by the 'Cyber Diplomacy' and Internet Governance mandate. However, this mandate is much larger in scope than the previously mentioned mandate as it promotes the involvement of international actors like the UN to become more active in the facilitation of developing a better legal framework as well as international cyber governance mechanisms for the purpose of addressing the threats posed by the issues within the aforementioned mandates.

Klimburg et al. provide the following table to provide an assessment of the level of national impact each of the different types of activity mentioned within the mandates have based on a scale of either "low" or "high" levels of impact:

[132] Ibid. p. 32
[133] Ibid. p. 32
[134] Ibid. p. 33

TYPE OF ACTIVITY	NATIONAL LEVEL IMPACT	
	Low	High
Information Theft	Counter Cyber Crime	Intelligence/CI
Information Disruption	Counter Cyber Crime and/or CIP – Nat'l Crisis Mgmt	CIP – Nat'l Crisis Mgmt and/or Military Cyber

(Source: Figure 3. Klimburg & Healey. "Strategic Goals and Stakeholders" in *Nation Cyber Security Framework Manual*. NATO CCDCOE: 2012, p. 78.)

The facilitation of addressing the issues posed within the mandates of the framework manual is further elaborated on as such conceptualization has had little traction amongst international policy makers. Authors Luiijf and Healey describe the approach to addressing the five mandates as supplemental "cross-mandates."[135] These three separate cross mandates include (1) Coordination, (2) Information Exchange and Data Protection, and (3) Research and Education.[136] The cross mandates proposed by Luiijf and Healey are indicative of a dual layer approach to addressing cyber security issues wherein the public and private sectors are needed to address their own separate but equally important steps towards threat reduction. This relationship is explained as one where the private sector is relied upon to make positive steps towards threat reduction (i.e. computer security firms), but in such cases where the private sector has failed to beneficial progress, the state becomes compelled to enact legislation and "regulatory frameworks" in order to alleviate the problem.[137] As an alternative to this scenario, however, the authors explain that the reliance on "stick-and-carrot approach[es]" by liberal democracies for the development of a cyber governance framework exists as the

[135] Luiijf, Eric & Healey, Jason. *Organizational Structures Considerations*. In Klimburg, Alexander. "National Cyber Security Framework Manual." NATO CCDCOE. 2012. p. 110
[136] Ibid. p. 110
[137] Klimburg, Alexander. "National Cyber Security Framework Manual." NATO CCDCOE. 2012. p. 61

primary option.[138] In this sense, the move towards securitization can be avoided through more emphasis being placed on the private sector working towards addressing the three cross mandates provided by Luiijf and Healey; as the incumbency for threat reduction lies in the successful development of deterrence and resiliency measures for computer security through the work of the private sector rather than the government.

Of particular note within the text regarding the work towards eliminating the threat of cyber conflict is the importance that must be placed on the promotion of education regarding the operational understandings of cyber interaction. This emphasis falls under the heading of the third cross mandate, 'Research and Education', and authors Luiijf and Healey explain the importance of education by writing, "Cyber security at the national level will fail when there is an inappropriate level of cyber security awareness and education. A nation requires its ministry of education and/or science to develop strategic/operational programmes for cyber security awareness and education."[139] In addition to this sentiment, the text also emphasizes the need for an education initiative to target the general public, cyber security professionals, and the personnel of state governments equally.

This would be a beneficial point to step back from presenting this first text in order to assess the mandates and cross mandates as they relate to the desecuritization concept, and its processual betiding that was discussed in chapter two of this research study. First, in regards to the cross mandate of Research and Education, this approach has a very strong impact on the successfulness or failure of a securitizing move. The initiative to further educate members of all facets of a society regarding the functionality of cyber interaction raises the awareness level of how to better ameliorate users' deficiencies that may eventually lead to exploitations for nefarious purposes (i.e. the commission of a cyber attack.)

Indeed, such an initiative is a positive step in considerably reducing the threat of cyber attacks and exploitation of lapses in user oversight in the future, but the initiative of this cross mandate also has the potentiality for drastically repositioning audiences in their reception to securitizing discourse. This relates to one of the questions brought up in the

[138] Ibid. p. 61
[139] Luiijf, Eric & Healey, Jason. *Organizational Structures Considerations*. In Klimburg, Alexander. "National Cyber Security Framework Manual." NATO CCDCOE. 2012. p. 133

Theoretical Chapter of this research study regarding potential instances in which an audience fails to reciprocate the feelings of necessity to securitize an issue presented by a securitizing elite. If one operates under the assumption that cyber conflict is an issue which has either been securitized as a whole, or is headed in a direction of becoming securitized by different securitizing entities internationally, then the way in which this cross mandate is framed in relation to securitization is altered. Rather, this becomes a question of whether this mandate has a connection to the desecuritization of the issue.

To answer this quandary, perhaps it is beneficial to refer to the four different political manifestations of desecuritization. As a first point of reference, two of the political manifestations of desecuritization, replacement and silencing desecuritization, fail to accurately define the processes described in the cross mandates of the CCDCOE's framework manual text. This is due to the fact that there is neither a new threat emanating as a derivative of the desecuritization of cyber threat to the state or international subsystem, nor has a threat source for cyber conflict been totally removed from the equation, as would be necessary for silencing. What is left is 'change through stabilization' and 'rearticulation'. In reviewing the mandates of the text, it is apparent that these two political forms of desecuritization are applicable for different aspects and approaches deemed necessary for the alleviation of cyber conflict.

The promotion of cyber governance principles, though not exactly what was envisioned by the Copenhagen School scholars when developing the conceptualization, is most closely associated with a change through stabilization approach to desecuritization. This assertion has the potentiality for developing into a larger discussion of the future of cyber governance building, and its relation to the connotation of state building that Hansen had raised as a problematic relating to change through stabilization. As for the proposed initiative for the promotion of research and education, this mandate is most closely related to the rearticulation process of desecuritization. This association is seen in the inherent implication that by shifting the way in which the incipience of cyber conflict is viewed, the threat eminence then becomes rearticulated. More specifically, by looking at cyber conflict as a result of lapses in deterrence and defense preparedness resulting from a lack of epistemic competence amongst all levels of a society, the view of outside threat to the state's critical infrastructural security from unmitigated offensive capacities

becomes rearticulated in order to facilitate political resolution of an issue rather than a securitizing approach.

The second of the two documents from the NATO CCDCOE that has been chosen for analysis in this research study is the *Tallinn Manual on the International Law Applicable to Cyber Warfare.* This document was published in 2013 as an amalgamation of the CCDCOE analysts' work on the reconceptualization of international law and governance as a facet of resolving cyber conflict, or as they call it, 'cyber warfare.'[140] This document will be analyzed in a similar manner to the previous NATO CCDCOE document wherein the major points of emphasis and clarifications of terminology / concepts will be covered, and the major additions to the overall discourse of cyber conflict resolution will be discussed and analyzed as far as their connection to the potential desecuritization of the issues that are addressed. The text itself defines the Tallinn Manual as "an expert-driven process designed to produce a non-binding document applying existing law to cyber warfare."[141]

For a contextualization of the sections of the text that work towards the reapplication of international law to cyber space, it makes sense to begin with a brief overview of the way in which the CCDCOE authors position themselves within the discourse of the subject in their introductory section. As a first point of emphasis in the Tallinn Manual, it is said that its overall aim is guided by the pursuit of addressing both *Jus ad bellum* and *Jus in bello* as they relate to cyber conflict; concepts of which the authors of the Tallinn Manual notably felt were applicable to cyber conflict analysis unanimously.[142] However the scope of the manual is not one that nefarious cyber actions like espionage / counter intelligence and cyber crime register in their understanding of war or conflict.[143] In addition to this distinction, the manual continues by strictly avoiding any analysis of assessing the topic of "individual criminal liability" as it relates to cyber conflict.[144] The final notable element of the Tallinn Manual's contextualization is the

[140] See Tallinn Manual p. 18, Note 18 for clarification of the use of this terminology.
[141] Schmitt, Michael N., ed. *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.*: 2013. p. 16
[142] Ibid. p. 19
[143] Ibid. p. 18
[144] Ibid. p. 18

rejection of the use of security terminology in their research. This was done because the overall aim of the manual was intended to be written as purely an examination of international law applicability, and delving into the topic of cyber security is inherently a move in a completely different heuristic direction than was intended.

Despite the conscious omission of a specifically security-related focus on the part of the manual's authors, the initial section for analysis in the manual covers various state actions in cyber space and a progressive development of 'International Cyber Security Law.' The following excerpt addresses this section of the text, its purposes, and the ultimate research outcome.

> 1. The term 'international cyber security law' is not a legal term of art. Rather, the object and purpose of its use here is to capture those aspects of general international law that relate to the hostile use of cyberspace, but are not formally an aspect of either the *jus ad bellum* or *jus in bello*. Hence, the term is only descriptive. It incorporates such legal concepts as sovereignty, jurisdiction, and State responsibility insofar as they relate to operation of the *jus ad bellum* and *jus in bello*.
>
> 2. In this regard, the International Group of Experts rejected any assertions that international law is silent on cyberspace in the sense that it is a new domain subject to international legal regulation only on the basis of new treaty law. On the contrary, the Experts unanimously concluded that general principles of international law applied to cyberspace.[145]

From the establishment of the parameters espoused in the antecedent excerpt, the text moves toward a survey of the issue of state sovereignty as it applies to operations in cyber space. The issue of the critical cyber infrastructure of the state is strongly integrated into the development of the CCDCOE's understanding of the constitution of state sovereignty.

For the remainder of the analysis on this portion of the Tallinn Manual I will discuss the numerous proposed rules associated with the development of International Security Law. However, not all proposed rules will be discussed in detail, particularly the rules relating the "Conduct Hostilities" (Encompassing Rules 20-69, although Rule 20 will be briefly discussed before moving on to non-NATO CCDCOE documents) as these issues have either been covered previously or are not pertinent to the thematic discussions

[145] Schmitt. Tallinn Manual: 2013. p. 24

of this research study. The discussion of the proposed rules from the Tallinn Manual will thus begin with the affiliated rules that were prefaced by the introduction of the facets of International Cyber Security Law.

The proposed rule on sovereignty from this section of the text is thus, "A State may exercise control over cyber infrastructure and activities within its sovereign territory."[146] Broken down, this rule proposal is reliant on multiple underlying facets. These underlying facets include an established understanding of sovereignty over the state's critical cyber infrastructure are based on where the cyber infrastructure is situated geographically. The terminological use of 'geographic location' is clarified in the text by saying that "the land territory, internal waters, territorial sea (including its bed and subsoil), archipelagic waters, or national airspace is subject to the sovereignty of the territorial State."[147] This also refers to cyber infrastructure possessed by private citizens or government entities, as it is all infrastructures that falls under the sovereign umbrella described in this rule of International Cyber Security Law.

The second rule proposed in conjunction with International Cyber Security Law is that of 'Jurisdiction.' This rule is one that strongly ties back in with the case of the Estonian cyber attacks. This is because the Estonian attacks serve as a phenomenal case study in which one can actually theorize what the extent of the Estonian government's jurisdiction was in terms of enforcing the its laws in response to the attacks that were committed against its cyber infrastructure. The Tallinn Manual addresses this quandary by offering the following analysis: "As to those acts which violated Estonian law, Estonia would, at a minimum, have been entitled to invoke jurisdiction over individuals, wherever located, who conducted the operations. In particular, its jurisdiction would have been justified because the operations had substantial effects on Estonian territory, such as interference with the banking system and governmental functions."[148]

Continuing with the topic of sovereignty and jurisdiction as it relates to cyber infrastructure, the third proposed rule from the Tallinn Manual addresses the problematic created by cyber infrastructure in non land-based locations. This, for instance, refers to cyber infrastructure based within international waters, international airspace, and outer

[146] Ibid. p. 25
[147] Ibid. p. 25
[148] Ibid. p. 28

space. In this respect, the authors of the Tallinn Manual alleviate the potential ambiguity of jurisdiction over instances in which infrastructure in these locations is attacked by offering the solution of: "Cyber infrastructure located on aircraft, ships, or other platforms in international airspace, on the high seas, or in outer space is subject to the jurisdiction of the flag State or State of registration."[149] While this clarification does not directly link to the Estonian case study, it is a distinction and provision that will be beneficial for future developing theorization on governance practices and norms as they relate to cyber governance and consequent conflict resolution.

With the above-mentioned distinctions in place, the Tallinn Manual thus moves to address the applicability of international law. The initial task in doing this is delving into state responsibility in instances in which a cyber attack on a state's critical cyber infrastructure occurred as a result of another state's sponsorship of this action. This topic is covered by proposed Rules 6, 7, and 8 of the Tallinn Manual. Respectively, these proposed rules are as follows:

> RULE 6 – *Legal Responsibility of States*
>
> A State bears international legal responsibility for a cyber operation attributable to it and which constitutes a breach of an international obligation.[150]
>
> RULE 7 – *Cyber Operations Launched from Governmental Cyber Infrastructure*
>
> The mere fact that a cyber operation has been launched or otherwise originates from governmental cyber infrastructure is not sufficient evidence for attributing the operation to that State but is an indication that the State in question is associated with the operation.[151]
>
> RULE 8 – *Cyber Operations Routed Through a State*
>
> The fact that a cyber operation has been routed via the cyber infrastructure located in a State is not sufficient evidence for attributing the operation to that State.[152]

In keeping with the theme of referring back to the Estonian case as an exemplification in which one can reflect on the rule proposals of the Tallinn Manual, the issue of assigning blame for a cyber attack to one country (in the Estonian case it was Russia) becomes extremely problematic when taking VPNs into account. As was explained chapter 5.1, IP addresses of the attacking entities have multiple ways in which their owners can obscure them. Rule 8 makes reference to this problem by saying that just because the attack

[149] Ibid. p. 29
[150] Ibid. p. 35
[151] Ibid. p. 39
[152] Ibid. p. 40

appears to have emanated from one state does not immediately point to that state's responsibility for the attack.

Consequently, the instances mentioned in Rules 6 and 7 are extremely difficult to enforce, especially when considering that in the Estonian example there were attackers involved that intentionally spoofed their IP in order to make it appear as though the attack was coming from the Russian government's cyber infrastructure, when this was not necessarily the case. From an analytical standpoint, this difficulty in the feasibility of the proposed rules begs the question of what can be done to overcome inabilities in attributing attack origin that undermine the ability of the international community to assign legal responsibility for attacks that may be committed against a state's cyber infrastructure. Legally speaking, this is a very difficult question to answer. However, the alleviation of the complication that stems from attack source ambiguity has potentiality in the aforementioned mandate for increased initiatives for research and education in the computer security sector. Advanced capabilities in computer forensics coupled with more defined codification of cyber conflict law would simultaneously erode the attribution problematic as more development is made in these areas.

The final proposed rule from the Tallinn Manual for analysis is RULE 20 – Applicability of the Law of Armed Conflict. This rule is framed within the manual by the following statement: "Cyber operations executed in the context of an armed conflict are subject to the law of armed conflict."[153] As was stated when this document was introduced in this chapter, Rule 20 is set within a portion of the text that deals the theorization of law on armed conflict and conduct in conflict situations as they relate to cyber conflict, and thus much of this section is consciously omitted from the discussion in the analysis sections. Despite this, this rule was chosen for inclusion due to its connection with the Estonian cyber attacks as a point of reference. As such, the sub-rules written in conjunction with Rule 20 explain, "in 2007 Estonia was the target of persistent cyber operations. However, the law of armed conflict did not apply to those cyber operations because the situation did not rise to the level of an armed conflict. By contrast, the law of armed conflict governed the cyber operations that occurred during the international armed conflict between Georgia and Russia in 2008 because they were

[153] Schmitt. Tallinn Manual: 2013. p. 75

undertaken in furtherance of that conflict."[154] This statement indicates that cyber conflict in and of itself does not constitute an instance of armed conflict, but with keeping in mind the terminological connections cyber conflict discourse has made to things like cyber weaponry and arms, this is a highly relevant argument against this standpoint. As it is framed here, cyber conflict only has the potentiality for a categorization as a tool within the framework of a greater armed conflict or a self contained instance of non-armed conflict.

Upon the assessment of this document, the findings as they relate to the existence of securitization or desecuritization movement lie primarily within the policy proposals for more developed international legislation on cyber conflict. Establishing a more robust framework for international law regarding cyber conflict opens up the space within the political realm for policy makers to address the issue of cyber conflict. As securitization moves the issue of cyber conflict into the exceptional status that is removed from the sort of legislative framework that aims at addressing such issues there is a potentiality for ameliorating perceived cyber threat through political means rather than securitizing means. However, this is not to say that what was included in the CCDCOE documents directly indicates a movement of desecuritization due to the fact that expanded political capacity to address cyber conflict does not necessarily result in a cessation of securitization by policy makers.

5.2.2 Estonian Ministerial Public Documents

At this point, the analysis will move from looking at major documents from the NATO CCDCOE and now focus on the discourse developed from the public documents that were published by various ministries within the Estonia government following the cyber attacks. Again, the selected documents are: the Estonian Ministry of Defense's Cyber Security Strategy for 2008, EISA's Summary on Ensuring Cyber Security in 2012, the subsequent 2013 and 2014 EISA Annual Reports on Cyber Security, and the Estonian Ministry of Economic Affairs and Communication's Cyber Security Strategy for 2014-2017. Accordingly, the documents will be introduced in their chronological order of

[154] Schmitt. Tallinn Manual: 2013. p. 68

publication so that not only can the general discourse created by these documents be established, but also any potential variations in the policy over the course of publication dates can be noted as well. Contextually speaking, these documents do far more to create a sense of the Estonian governmental discourse on cyber threat mitigation than the CCDCOE documents, and thus they provide a perspective from a lower level of analysis from the international subsystem level to the state level. It should also be noted that general trend in Estonia's cyber discourse is that of a securitizing movement, especially over the progression time between 2008 and 2014. This sentiment will be reflected on more thoroughly during the assessment of the final strategy document for 2014-2017. In spite of this trend, the overall goal is still to highlight trends in the discourse that hold the potentiality for desecuritization.

With documents and their order of analysis having been established, the first document that will be examined is the Estonian Ministry of Defense's (MoD) Cyber Security Strategy for 2008 (henceforth referred to as '2008 CSS'). As the oldest of the chosen documents in this analysis category, the 2008 CSS document allows for the discourse to be framed from a perspective in which the initial publication of strategy mandates following the 2007 cyber attacks serves as a reference point from which to ultimately observe any trends or changes in the other Estonian documents as time progresses. From the outset of the document, the Estonian MoD identifies the "asymmetrical threat posed by cyber attacks and the inherent vulnerabilities of cyberspace" as the primary issue in which they seek to remedy through the execution of their strategy plan.[155] In addition to this, the document also goes on to explain what the MoD envisions as potentially the best overall type of approach to alleviating cyber threat. As a first point of emphasis, the asymmetric cyber threat is viewed by the MoD as an issue that must be "addressed at the global level", but also that states like Estonia have a responsibility to identify potential vulnerabilities in their cyber infrastructure and draft policies to address these vulnerabilities accordingly, both domestically and through international cooperation.[156]

[155] Estonian Ministry of Defense. "Cyber Security Strategy." Cyber Security Strategy Committee. 2008. p. 3
[156] Ibid. p. 3

The 2008 CSS then goes on to discuss the domestic and international dimensions of threat deterrence, and specifically goes into what areas of focus these approaches should have. The Estonian MoD put forth four different "policy fronts" that they identify as areas in which the Estonian state would stand to make great strides in the future deterrence of cyber threat. The indentified policy fronts from the text are as follows:

- application of a graduated system of security measures in Estonia;
- development of Estonia's expertise in and high awareness of information security to the highest standard of excellence;
- development of an appropriate regulatory and legal framework to support the secure and seamless operability of information systems;
- promoting international co-operation aimed at strengthening global cyber security.

Accordingly, the identification of these policy fronts is subsequently succeeded by an extended list of policy recommendations that specifically target each of these policy fronts. These policy recommendations provide great insight into the initial direction the Estonian government envisioned for altering the vulnerabilities of their cyber infrastructure. The first of these policy recommendations is, in short, creating a push to enhance the technical robustness of Estonian computer security as it specifically relates to the resilience of the state's critical cyber infrastructure. The sub-recommendations within this general recommendation mentions the need for "enhancing" or "ensuring" cyber security through the concomitant bolstering of internet security.[157] What is necessary here is to delineate between understandings of security, especially if one views this policy recommendation as a move towards securitization in the Copenhagen sense of the word in order to facilitate the preparedness of infrastructure against cyber threat.

However, the intention is not to uncover the intended meaning of the document authors, but rather to acknowledge identifiers in the text as to the direction of the policies. In this case, the enhancement of infrastructural resilience is associated with an enhancement of technical capabilities to ensure security, rather than the enhancement of the state's ability to enact legislation to ensure infrastructural security. This assessment is derived from the technical nature of the sub-recommendations, specifically the inclusion

[157] Estonian Ministry of Defense. "Cyber Security Strategy." Cyber Security Strategy Committee. 2008. p. 3-4

of the following: "The security of the Internet is vital to ensuring cyber security, since most of cyberspace is Internet-based. The main priorities in this respect are: strengthening the infrastructure of the Internet, including domain name servers" ; "to improve on an incessant basis the capacity to meet the emergence of newer and technologically more advanced assault methods" ; "to enhance inter-agency co-operation and co-ordination in ensuring cyber security and to continue public and private sector co-operation in protecting the critical information infrastructure." These initiatives are completely rooted in the promotion of enhanced technical capacity for both the government and private sector, and in the case of the last point, an enhanced level of inter-agency communicative capacity.

The next policy recommendation is entitled, "Increasing competence in Cyber Security."[158] This is along the same lines as the mandate from the NATO CCDCOE document that alluded to the necessitation of heavily increasing education and research relating to cyber competency. Similarly to the CCDCOE document, the MoD 2008 CSS document heavily stresses the point that the research and education initiative in tended for both the public and private sectors in order for its optimal efficacy. The specific objectives in this document include research and development for an higher level of training for IT staff in both sectors, as well as technical research and development for further advancement in personnel capabilities in both managing and preventing any attacks against cyber infrastructure.

However, contrary to the CCDCOE document, the 2008 CSS separates the general public from the initiative for the promotion of cyber-related research and development. The inclusion of the general Estonian public in this equation is discussed as the potential policy for "Raising Awareness on Cyber Security."[159] This policy recommendation is explained as an initiative for the purpose of "Raising public awareness on the nature and urgency of the cyber threats."[160] As was stated in the previous sub-chapter (5.2.1) on the CCDCOE documents, the promotion of public knowledge on cyber interaction across various sectors, the connection state infrastructure has to cyber interaction, and the nature of both cyber threat and cyber deterrence all

[158] Ibid. p. 4
[159] Ibid. p. 5
[160] Ibid. p. 5

factor into the publics' ability to understand cyber security better, and thus have the potentiality to be less accepting a move towards cyber securitization. In the pursuit of providing a means by which this can be achieved, the 2008 CCS offers the following initiatives: "raising awareness of information security among all computer users with particular focus on individual users and [Small & Medium Enterprises] SMEs by informing the public about threats existing in the cyberspace and improving knowledge on the safe use of computers" and "co-ordinating the distribution of information on cyber threats and organising the awareness campaigns in co-operation with the private sector."[161]

In a more direct and further assessment of the two previous policy proposals, the connection to the concept of desecuritization – specifically the desecuritization of threat from cyber conflict – stems from potentiality for the existential threat of cyber infrastructure of the state to fail to register as an issue that gains acceptance from the various facets of society. The move towards desecuritization in this regard is multifold, as both the epistemological authority of the securitizing elites is severely diminished through the advancement of the knowledge base of the private and public entities. Additionally, the technical proficiently of IT professionals in the public and private sector ultimately leads to further ability to respond to or prevent attacks of an asymmetric nature on the scale of what was seen in Estonia. In short, these factors lead to a cascading effect where the pre-existing epistemological lapses and technical ineptitudes of state citizenry that lead to threat being levied against the state begins to be mitigated over time.

To conclude the analysis of the MoD's 2008 CSS document, the final two policy recommendations will be introduced. These two, in a similar fashion to the two aforementioned policies, are interconnected due to their scale of implementation; in this case they are on the international level of analysis. As they are listed in the document, the two policy recommendations are: "Improvement of the legal framework for supporting cyber security" and "Bolstering international co-operation."[162] The former of these two does, indeed, refer to the domestic level of legislation in addition to the international level of implementing law for the curbing of cyber actions detrimental to the operability of

[161] Ibid. p. 5
[162] Ibid. p. 4-5

cyber infrastructure. In particular, the document lists the overall lack of development of both terminological agreement within the context of international legislative bodies as a major problem in need of being addressed; "Several terms, such as *cyber war*, *cyber attack*, *cyber terrorism* or *critical information infrastructure*, have not been defined clearly. Everywhere they are used, but their precise and intended meaning will vary depending on the context."[163] Once again, this initiative is in agreeance with the CCDCOE's stance on terminological coherence in legislation. And in the context of desecuritization, the promotion of domestic and international legislative development as a whole, and in terms of cyber-related terminology brings the discourse away a drift towards securitization as a result of ambiguous pre-existing legislation, back to a realm in which the discourse on cyber conflict is grounded in a coherent and internationally agreed upon framework. In this case, still unresolved threat posed by threats in the cyber theater are able to be addressed without the issue being elevated to a specialized political status.

Finally, the policy of 'Bolstering International Co-operation' operates as both an extension and a continuing development of the previous policy regarding the development of international and domestic legislation on cyber conflict. This is seen as an extension of the previous policy due to the sub recommendation that states that one of the ultimate goals is "promoting countries' adopting of international conventions regulating cyber crime and cyber attacks, and making the content of such conventions known to the international public."[164] Again, this is a move towards the politicization of the issue of cyber conflict rather than a move towards securitization in that goals such as this promote not only further development of a legislative framework to deal with cyber attacks and conflict, but also promoting the mass distribution of this information to the public. In doing this, both Estonian and other states become more engaged in the active political process focusing on the resolution of an issue rather than allowing for the issue to be taken out of the political realm of discourse.

In summation of the previous analysis on the 2008 CSS document, the three major findings have been the importance placed on the themes of: knowledge advancement

[163] Ibid. p. 17
[164] Ibid. p. 5

amongst computer professionals and the general public, increased emphasis on creating a more comprehensive legislative framework in both the international and domestic settings, and the promotion of international cooperation in addressing the mitigation of cyber threat. These points of emphasis for the future mitigation of cyber threat stand as themes that will permeate the remaining annual reports as well, and ultimately serve as the benchmark for what can be seen as the potentiality for avenues in which desecuritization manifests in relation to cyber conflict.

The next document for analysis is EISA's 2012 Summary on Ensuring Cyber Security. Apart from covering the main task and responsibilities of EISA, the document covers two main points. The first is the promotion of initiatives similar to the 2008 MoD CSS document, and the second is a summation of the cyber conflict-related events of the 2012 calendar year. In this respect, the first topic covered within the documents is "Ensuring Security Through Enhanced Knowledge."[165] This points to a rising trend within the documents so far reviewed as far as their general consensus on the necessity for the advancement of knowledge trough education and training initiatives in Estonia. The document explains that over the course of 2012 this initiative was facilitated by the organization of "5 seminars, 1 conference, 1 information day, and 17 trainings," In addition to this, EISA held a symposium in Estonia aimed at training IT professionals in both public and private positions in how to best mitigate the potentiality for cyber attacks, as well as coping with cyber attacks directed at critical cyber infrastructure.[166] One particular added point of emphasis is that this initiative targets "resolving civil and military cyber crises."[167] The capability of responding and resolving crises that arise as a result of cyber attacks, in essence, diminishes the level of threat attribution that can be assigned to cyber conflict. Rhetorically speaking, the advancement in cyber crisis management amongst IT professionals limits the ability of potential securitizing actors to claim the existentialism of cyber infrastructure is at risk from cyber attacks.

EISA's 2012 Annual Summary covers the topic of cyber-related legislation similarly to the MoD 2008 CSS document, but in the case of EISA's document, there had

[165] Vaks, Toomas. "Summary of the Estonian Information System's Authority on Ensuring Cyber Security in 2012." 2012. p. 2
[166] Ibid. p. 2
[167] Ibid. p. 2

been enough time elapsed between the publications of the documents that the specific legislation in Estonia could be discussed in more detail. The document explains that during 2012, EISA made proposals to the Estonian government regarding making changes to the Public Information Act, the Emergency Act, the Electronic Communications Act, and the State Secrets and Classified Information of Foreign States Act regarding the intention of "amending and changing regulations governing cyber security and its supervision."[168] More specifically, EISA sought and received from the Estonian government more regulation targeting the information security standards within Estonia. The realization of this initiative materialized as the creation of senior information security official (CISO) as a position required of Estonian authorities to appoint for the purpose of "ensuring security requirements for electronic systems relevant for the functioning of vital services" in the public sector.[169] As a further aspiration of this plan, the goal of this document's publication was to have this role extended into the private sector for businesses as well. This, in effect, bolstered the deterrence and coping capabilities of all levels of cyber infrastructure in Estonia.

The last topic covered in this document is the promotion of cooperation both internally and internationally. As had been discussed before, the protection of cyber infrastructure does not fall into the hands of any one entity within a state. Rather, this obligation is distributed amongst different authorities depending their functional nature. When it comes to internal cooperation, EISA refers to the opening of communication amongst the different organs of government. On this topic, the document lists numerous agencies within the Estonian government that gather monthly under the facilitation of the Critical Information Infrastructure Protection Commission and the Computer Emergency Response Team for Estonia (CERT-EE) for the purpose of constant cross-agency information sharing.[170] This same initiative was taken on a broader scale with EISA strengthening their communication between research institutions in France, Germany and the United States, which resulted in further training and information sharing regarding cyber-related crises.[171]

---

[168] Ibid. p. 3
[169] Ibid. p. 2
[170] Ibid. p. 2
[171] Ibid. p. 2

The document closes by stating that 2012 was seen as a "peaceful year in Estonian cyberspace."[172] Additionally, it goes on to restate the importance put on continued development of cooperation and communication especially for the development of better research and training for the handling of cyber conflict, as well as stressing the look forward to future years for more legislative response to continuing the administrative support that things like the creation of the CISO position had in 2012.[173] In taking a step back from the document to again assess what was proposed with respect to the theoretical underpinnings of this research study, one issue that remains uncertain is the connection desecuritization, specifically the different delineations of desecuritization, have in this case. Particularly, a point should be made to assess the applicability of these delineations further than what has already been covered. As was stated in section 5.2.1, moves towards desecuritization such as 'change through stabilization' and 'replacement' have little to no applicability in what was discussed in this document. If the promotion of these initiatives is clearly not a continuation of securitization of an issue, what is left is desecuritization through 'rearticulation.' The trajectory of the cyber conflict issue is altered by actively offering both political and societal alternatives that seek to mitigate the threat posed by the issue. This change points to a move towards a desecuritization of the issue by altering how Estonia has decided to provide new alternatives and solutions to preventing future cyber crisis.

The next document is the subsequent EISA 2013 Annual Report. The 2013 Annual Report begins its analysis in the same manner in which the 2012 Annual Report finished in that it comments on the status of peace in Estonia relating to the committal of cyber attacks. The document describes 2013 as "a relatively peaceful year as far as serious incident are concerned", citing the fact that major cyber incidents had declined during the year when compared to the year prior.[174] Though this was not completely indicative of a year permeated by peace on the cyber-front as the document continues on its assessment of the year by saying that there was still an existence of isolated cyber attacks. The attacks registered by EISA in 2013 consisted of "13 cases of DDoS attacks"

[172] Ibid. p. 5
[173] Ibid. p. 5
[174] Vaks, Toomas. "2013 Annual Report Cyber Security Branch of the Estonian Information System Authority." January 1, 2013. p. 6

and website defacements had increased in comparison to previous years, of which EISA documented "240 cases."[175] The extent of the analysis of the status of Estonia's cyber incidents and attacks within the report is significantly more expansive than what was seen in the 2012 report as there are numerous more statistics to analyze as a result of the 2013 Estonian government requirement for state institutions to report all instances of cyber incidents to EISA.[176]

In a further analysis of the reported cyber incidents in 2013, the collected data on the incidents is broken down by the cause attributed to why the incident occurred. On this topic the document says, "As causes for the incidents, attacks and administrative errors were cited most often, followed by deficiencies in software and hardware."[177] This realization supports the notions made by NATO and EISA in their previous documents wherein they stress the urgency of importance being placed on the promotion of technical research and education in order to increase the level of capability amongst the user base. The connection that inadequate technical capability has to the continued perpetration of cyber attacks and incidents is a point that cannot be stressed enough. This is especially the case when looking at the promotion of education and user competence in cyber interaction as a contributing factor towards a desecuritization of cyber conflict.

Due to the shift in the way in which cyber attacks were undertaken over the time between 2008 and the publication of this 2013 document, EISA, within the section on future policy recommendations, address the rise of defacement as a chosen method for attack. Again, this problem is largely tied to the lapses in technical competence of users, particularly web administrators' lapses in taking advantage in developments in software that prevents the ability for users to with nefarious intentions to commit defacements. As a response to this, EISA cites the Estonian Internet Foundation's (EIF) development of domain name security (DNSSEC) as a means to promote increased DNS security for administrators and ultimately severely limit the possibility of future defacements and continue the trend of decline in cyber attacks.

The 2013 Annual Report thus concludes with the sentiments that the transition into the 2014 calendar year will require continued persistence in emphasizing to users in

[175] Ibid. p. 6
[176] Ibid. p. 7
[177] Ibid. p. 8

the public and private sector the importance of continued development system administrative competency and adoption of advancements in software and hardware. With that being said, we will now move to the final annual report, EISA's 2014 Annual Report. In a preliminary assessment of the documents contents, the 2014 calendar year proved to be a difficult year in the pursuit of deterring cyber conflict. In his introduction within the report, Toomas Vaks, the director of Cyber Security at EISA goes as far as to say that it "faced new challenges in 2014. The security situation deteriorated noticeably; [Estonia is] now operating in Europe, where a war is being fought."[178] This conflict, as Vaks asserts, had a connection to the deteriorating cyber security situation in Estonia during 2014 wherein there was a rise in the total number of DDoS attack and defacements against Estonian domains.[179]

Similarly to the 2007 attacks on Estonia the reported attacks in 2014 saw a trend in the employment of DDoS attacks to specifically target the primary government-related websites of Estonia. However, the document explains the recent development in the use of DDoS attacks is that they no longer have been used to solely focus on government or economic based domains; they have now been expanded in their employment into other sectors.[180] As such, a key focus of the policy recommendations of the 2014 annual report is on addressing the continued threat posed by unmitigated DDoS attacks against domains extended across all sectors of the Estonian state. In this case the proposed remedy is bolstering monitoring of web activity and traffic for indicators of possible DDoS inundation against critical domains in order to provide faster responses to such attacks.[181] In addition to the proposal to address the continued problems with DDoS attacks, EISA also takes up again the discussion of major lapses in the adoption of patched software, which results in subsequent security lapses in various public and private web domains. 2014 proved to be increasingly difficult in this regard due to the emergence of Heartbleed[182] and the discontinued support of Windows XP, leaving open and exposing numerous avenues for attack as a result of revealed vulnerabilities. These realizations

[178] Vaks, Toomas. "2014 Annual Report Cyber Security Branch Of the Estonian Information System Authority." January 1, 2014. p. 4
[179] Ibid. Inforgraphic, p. 3
[180] Ibid. p. 7-8
[181] Ibid. p. 8
[182] Heartbleed is an exploitative security bug that exposes online data that was originally encrypted.

support the previous annual reports insistence that a realistic threat is posed cyber infrastructure by easily preventable user errors.

Very little changes occurred between the latter discussion within the 2014 annual report on "Cyber Risk Prevention" compared to what was espoused in the previous two year's reports. The same themes occur again in the form of insistence on: Increased training and education, increasing public awareness of cyber threats, DNSSEC implementation, and the expansion of international cooperation.[183] Being that there is little change in these proposed initiatives, there is not a need to re-hash a parallel assessment of them with respect to the theoretical framework of this research study. What is more relevant for analysis is the discussion of legislative developments in regards to cyber security. The 2014 Annual Report serves as a preface to the Estonian Cyber Security Strategy for 2014-2017. A document which the 2014 Annual Report explains as an exemplification of a shift in thinking on cyber security strategy to expand its scope in an international direction rather than having an inward focus on strategically working on cyber threat deterrence.

With that being said, the Estonian Cyber Security Strategy for 2014-2017 that was published by the Estonian Ministry of Economic Affairs and Communication (henceforth referred to as 'CSS 14-17') is the final document that will be examined in this research study. The trend of the specific points of emphasis continues within this text, as the primarily challenges in which Estonia seeks to overcome during the period between 2014 and 2017 are listed as, "shaping the legal framework, promoting international cooperation and communication, raising awareness, and ensuring specialist education as well as the development of technical solutions"[184], all of which have been covered extensively in the previously examined documents.

The contents of the document that are of more pertinence to a pursuit of examining security-related discourse are found in the list of the "Principles of Ensuring Cyber Security." The principles are framed within the text as way of supporting the assertion that to ensure the aforementioned challenges are resolved, specifically through

[183] See EISA 2014 Annual Report p. 20-22
[184] "2014–2017 Cyber Security Strategy." Ministry of Economic Affairs and Communication. 2014. p. 6

policy recommendations that develop into a "modern legal framework" to mitigate the committal of cyber attacks. These principles are listed as follows:[185]

1. Cyber security is an integral part of national security, it supports the functioning of the state and society, the competitiveness of the economy and innovation.
2. Cyber security is guaranteed by respecting fundamental rights and freedoms as well as by protecting individual liberties, personal information, and identity.
3. Cyber security is ensured on the basis of the principle of proportionality while taking into account existing and potential risks and resources.
4. Cyber security is ensured in a coordinated manner through cooperation between the public-, private- and third sectors, taking into account the interconnectedness and interdependence of existing infrastructure and services in cyberspace.
5. Cyber security starts with individual responsibility for safe use of ICT tools.
6. A top priority in ensuring cyber security is anticipating as well as preventing potential threats and responding effectively to threats that materialize.
7. Cyber security is supported by intensive and internationally competitive research and development.
8. Cyber security is ensured via international cooperation with allies and partners. Through cooperation, Estonia promotes global cybersecurity and enhances its own competence.

Without treading too far into a trajectory of connoting the underlying meaning of the above-listed principles' rhetoric, there is an inherent link that the principles have to the status of state existentialism and cyber security. Particularly, there is an extension of this connection to existentialism across the different sectors of analysis within the Copenhagen School Theory. This extension is derived from the apparent link that cyber security has in protecting the economic system of the state, the freedoms of the societal sector, and the integrity of national sovereignty. In turn, the principles highlight the way in which the security of cyberspace and cyber operations directly affects the security of other sectors.

In terms of the integrity of the state and its connection to cyber security, a proposed sub goal within the CSS 14-17 addresses "Ensuring digital continuity of the state."[186] This is explained to be achieved through ensuring that "E-services, processes, and information systems (including digital registers of evidential value) that are essential for the digital continuity of the state … have mirror and backup alternatives. Virtual embassies will ensure the functioning of the state, regardless of Estonia's territorial integrity."[187] With these factors in mind, the process of securitization through the speech

[185] Ibid. p. 7
[186] Ibid. p. 9
[187] Ibid. p. 9

act of establishing threat to the existence or operability of the state is largely evident within Estonia's CSS 14-17. While there are elements of the document that align with what has already been discussed as paradigms indicative of desecuritizing patterns, the focus on the eminent threat to state security shows, at least for the contemporary strategy objectives, that the trend in the discourse is one marked by a continued securitization.

In terms of concluding remarks for this chapter, one caveat to the overall analysis on the discourse of the documents should be a discussion of the permeation of references to security terminology within all of the NATO and Estonian ministerial texts. Being that the act of speaking security is inherently a move towards a securitized status, there exists underlying difficulty with assessing the initiatives and recommendations within the documents as exemplifications of moves towards desecuritization. Rushing too quickly into pointing out that any possible moves towards desecuritization within the same text that discusses these initiatives as progress towards increasing the national security of Estonia is incredibly problematic. Obviously, it is not as black and white as making a sweeping statement as to whether the discourse tells us that there is clearly a securitization or desecuritization occurring. Securitization Theory is merely a tool for analysis – a methodology for research – in this case looking at public document discourse following the 2007 cyber attacks. There are much deeper dynamics that must be assessed than just looking at securitizing processes through a general survey of the discourse, as the necessity for audience reciprocity of an elite's conveyance of existential threat factors in as well. This factor has been taken into great account, as one can reference the discussion of this topic in the chapter 2, and the issue of audience non-reciprocity by way of rearticulation was noted as a signifier of desecuritization throughout chapter 5's analysis.

For the concluding remarks of this chapter, the primary question to answer is: What has this analysis uncovered? And specifically, answering what can be said about the signification or non-signification of any movement towards cyber desecuritization at this point is an essential addition to the concluding remarks as well. The analysis of the collective discourse generated from the chosen public policy documents lacks enough evidence to describe the overall directive of the discourse as moving the issue of cyber conflict in a desecuritizing direction. This is due to the permeation of discourse

continuously aimed at elucidating the existential threat facing referent objects within multiple sectors of analysis. This was especially evident in the analysis of the CSS 14-17 document in which the self vs. other dynamism was at its most invigorated status since the 2007 attacks with the realization that cyber attack occurrences had increased as an extension of non-cyber conflict in the European region. As such, the discourse of these public documents largely operates in a securitizing framework.

However, as was referenced numerous times throughout the analysis and discussion of the documents, the application of the theoretical conceptualization of descuritization (especially the delineations of the manifestations of desecuritization made by Hansen) to the discourse of the documents reveals exemplifications of how the issue of cyber conflict can be reframed so as to not attribute existential threat to a referent object. In this sense, the claim that desecuritization can be used as a legitimate frame of analysis for the study of cyber conflict is evident, but contemporary exemplifications of this are still sparse. Such examples of desecuritization within the documents lay only in the rearticulation of a threat and the subsequent politicization of the issue in order to mitigate the threat. Other such delineations of desecuritization were incompatible with the policy recommendations and initiatives found within the documents' discourse. With these principle findings being said, the concluding sentiments of this research study will be further expounded upon within the conclusion chapter, as well as recommendations for future research based on the analysis and findings of this study.

Finally, a discussion relating to the possibility of bridging the gap between cyber securitization and the conceptualization of cyber peace serves as a potential starting point from which a future study of cyber conflict to focus. The initial connection between these two concepts is found in the 2012 and 2013 Annual Reports in which they discuss the level of peace within Estonian cyberspace for the year. Little analysis is offered beyond just briefly assessing the perceived level of peace in the cyber theater of operation. In this respect, the measure of peace used in the documents is only the quantifiable assessment of the attacks that were measured and recorded during the given year. From the perspective of Peace Research, this stands as a gap in the frame of reference in which one can assess the concept of peace in cyber space. In short, the conceptualization of cyber space exists as paradigmatic shift within the greater academic study of cyber interaction

from a social sciences standpoint, particularly from a peace and conflict research perspective. The following chapter will contain the concluding remarks of this research study regarding securitization and desecuritization in Estonia's political discourse surrounding cyber conflict, as well as take into consideration the questions raised by the perceived gaps in research on cyber desecuritization and the conceptualization of cyber peace.

6.0 Conclusion

The seven-year period between 2007 and 2014 saw significant changes in the way in which the international community viewed the issue of the cyber capacity for conflict. Beginning with the 2007 Estonian attacks and continuing with attacks on Georgia in 2008, the 2010 Stuxnet attack on Iran the occurrences high-profile attacks continue. More recently at the time of writing this thesis cyber attacks have been exemplified as extensions of greater conflicts in the 2014 Ukrainian conflict and 2014 Hong Kong protests.[188] The emergence of new challenges like cyber conflict potentially represents a large threat to states, depending on the scale of the attack. In this regard, the security of the state and the existentialism of various referent objects within the military, economic, political, and societal sectors may be pushed forward by legislators in order to take effective action against the cyber threat, effectively securitizing the issue.

What has been done in this research study is looking beyond the securitizing movement of the cyber issue, and attempted to either evidence movements of desecuritization wherein the cyber issue is changed in its presentation to the audience so as to bring it back into the politicized realm of resolution, or if no exact examples of applying desecuritization can be directly referenced as applicable cases, at least promote a further conceptualization of desecuritization. Both such cases are discussed in the concluding remarks of the previous chapter in which the various initiatives and policy recommendations put forth operate in a similar vein to desecuritization through a rearticulative methodology on the part of the Estonian ministries and NATO. The main caveat for the findings regarding securitization and desecuritization in the analyzed documents is that the apparent trend in discourse is indicative of securitization rather than desecuritization of the cyber issue.

The apparent Securitization of the cyber issue in Estonia stems from the continued insistence of major imminent threat to the state's ability to operate or even exist in some aspects, and the subsequent policy objectives that look to alleviate this issue. This of course, does not necessary indicate that exceptional measures are being taken by NATO or Estonia, but this directive element was most apparent within the final document that

[188] See Fox-Brewster: 2014, Healy: 2014

laid the framework for the cyber security strategy for the Estonian state going forward from 2014 to 2017.

The phrase 'paradigmatic shift' has been used in conjunction with the pursuit of studying cyber-related discourse through the lens of the desecuritization concept within this thesis. This has been in reference to the under-employed use of desecuritization as a guiding theoretical concept in research on cyber security and cyber conflict. Academically speaking, the contribution made by this research study lies in the initiative to further attempt to apply this concept to a case study based on cyber security strategy policy recommendations. It is understandable that there is still much work to do in shifting the security focus of this field of study, as the general study of cyber conflict is relatively a theoretical zygote.

Hansen's delineations of desecuritzation were a great step in this direction, but the application of these delineations do not have a clean application to the field of cyber conflict, and one of the primary research considerations that can be derived from this particular study is that attempts to further apply the concept to other case studies of post-cyber conflict discourse and rhetoric must be made, and even if there are no contemporary examples of desecuritization in practice then there is still the possibility of proposing policy directives that lead towards deeper elucidations of actual delineations of cyber desecuritization. Furthermore, a proposal to come from the findings of this research study is the development of a new delineation of desecuritization, which can be more accurately used in conjunction with cyber security analysis. The realization that rearticulative desecuritization did not completely fit with what was observed in the analyzed documents leads to a opportunity for adopting the 'proliferation of epistemic authority amongst the all levels of the international community' as a new way of envisioning cyber desecuritization. This stems from the permeation of the promotion of cyber-related knowledge advancement throughout the analyzed documents as a substantial factor in the mitigation of perceived cyber threat in the future.

To return to the topic of developing the potentiality for the conceptualization of cyber peace, it must first be said that this too falls into the category of being generally

under researched.[189] Perhaps one of the more important findings in this research study is the permeation of equating low levels of cyber attack instances in the EISA annual reports with quasi-measurable levels of peace in Estonian cyber space. This gives credence to the idea that cyber peace represents more than just a theoretical proposition without any basis. The future of this conceptualization is two-fold. First, the field of peace research stands to make significant contributions to this topic through the application of perspectives like Galtungian theory to the study of cyber interaction. For instance there are bigger questions to be asked of the cyber peace concept such as "What constitutes Cyber Peace building" and "How do you delineate between positive and negative cyber peace." Questions such as these move the line of thinking in a direction that demands more of blanket statements claiming peaceful years in cyber space as seen in the aforementioned annual reports.

The second part of the future of cyber peace conceptualization is the potentiality for creating links between the initiatives and policies that result in the desecuritization of an issue and the elements ultimately representing moves towards cyber peace. As evidenced in the analysis of the Estonian documents, many of the initiatives that were associated with moves towards desecuritization of aspects of cyber conflict were aimed at attack deterrence. By moving the issue of cyber attacks back into the politicized spectrum in order to ultimately mitigate the employment of the current known methodology of cyber attacks, there may be a link to the creation of peace. In the political process of mitigating the persistence of cyber attacks to a point where attacks cease, has a state actually created a situation of peace? This is a question that has the potentiality for exploration after more work has been made in relation to the previously discussed recommendations for future research on conceptualizing cyber peace.

As with the tradition of academic research, this thesis uncovered more questions in its conclusion than it was able to effectively answer. This is a positive for fledging fields of study like cyber conflict / cyber security / cyber peace as more questions need to be asked in order for the development of our collective knowledge of the issue. Lack of technical computer-related knowledge cannot be used as an inhibition to apply new

[189] See footnote 69 for contempory examples of literature promoting the development of conceptualizing cyber peace.

concepts and theories to this field. If nothing else, this must be the main take-away from this thesis. The international community is working to better understand the nature of cyber interaction whether it be for positive or negative purposes. There is a vast wealth of pre-existing theories and methodologies already used to research other fields of study that can ultimately be re-applied to the cyber theater of operation, and in doing so, can formulate a new paradigm in which cyber-related research is conducted.

7.0 References

Alvestrand, Harald. "A Mission Statement for the IETF." October 1, 2004. Accessed March 12, 2015. https://www.ietf.org/rfc/rfc3935.txt.

Anderson, Nate. "Massive DDoS Attacks Target Estonia; Russia Accused." Arstechnica. May 14, 2007. Accessed March 12, 2015. http://arstechnica.com/security/2007/05/massive-ddos-attacks-target-estonia-russia-accused/.

Balzacq, Thierry. "The Three Faces Of Securitization: Political Agency, Audience And Context." *European Journal of International Relations* 11 (2005): 171-201.

Bartelson, Jens. *A Genealogy of Sovereignty*. Cambridge: Cambridge University Press, 1995.

Bendrath, Ralf. ”The American Cyber-Angst and the Real World – Any Link?”. In Robert Latham (Ed.): Bombs and Bandwidth: The Emerging Relationship between IT and Security, New York: The New Press, 2003

Blank, Andrew. *TCP/IP Foundations*. San Francisco, California: Sybex, 2004.

Broad, William, John Markoff, and David Sanger. "Israeli Test on Worm Called Crucial in Iran Nuclear Delay." The New York Times. January 15, 2011. Accessed March 22, 2015. http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all&_r=0.

Buzan, Barry. "Rethinking Security After The Cold War." *Cooperation and Conflict* 32 (1997): 5-28.

Buzan, Barry, and Ole Waever. "Macrosecuritization and Security Constellations: Reconsidering Scale in Securitization Theory." *Review of International Studies* 35, no. 2 (2009): 253-76.

Buzan, Barry, Ole Waever, and Jaap De Wilde. *Security: A New Framework for Analysis*. Boulder, Colorado: Lynne Rienner Pub., 1998.

Collins, Sean, and Stephen Mccombie. "Stuxnet: The Emergence of a New Cyber Weapon and Its Implications." *Journal of Policing, Intelligence and Counter Terrorism* 7, no. 1 (2012): 80-91.

Connolly, Dan. "The 'text/html' Media Type." June 1, 2000. Accessed March 12, 2015. http://www.ietf.org/rfc/rfc2854.

Deibert, Ronald. *Circuits of Power* in Rosenau, James N. *Information Technologies and*

Global Politics the Changing Scope of Power and Governance. Albany, New York: State University of New York Press, 2002.

Eddy, W. "RFC 4987 - TCP SYN Flooding Attacks and Common Mitigations." RFC 4987 - TCP SYN Flooding Attacks and Common Mitigations. August 1, 2007. Accessed March 21, 2015. https://tools.ietf.org/html/rfc4987.

Finn, Peter. "Cyber Assaults on Estonia Typify a New Battle Tactic." Washington Post Foreign Service. May 19, 2007. Accessed March 10, 2015. http://msl1.mit.edu/furdlog/docs/washpost/2007-05-19_washpost_estonia_cyberattacked.pdf.

Fox-Brewster, Thomas. "Did China Order Hackers to Cripple the Hong Kong Protest?" Motherboard. November 5, 2014. Accessed November 6, 2014. http://motherboard.vice.com/read/inside-the-unending-cyber-siege-of-hong-kong?utm_source=vicenewsfb.

Foucault, Michel. *The Archaeology of Knowledge*. New York, New York: Pantheon Books, 1972.

G., Tim. "Renting a Zombie Farm: Botnets and the Hacker Economy." Renting a Zombie Farm: Botnets and the Hacker Economy. August 8, 2014. Accessed March 21, 2015. http://www.symantec.com/connect/blogs/renting-zombie-farm-botnets-and-hacker-economy.

George, Alexander, and Andrew Bennett. *Case Studies and Theory Development in the Social Sciences*. Cambridge, Massachusetts: MIT Press, 2005.

Hansen, Lene. "Reconstructing Desecuritisation: The Normative-political in the Copenhagen School and Directions for How to Apply It." *Review of International Studies* 38, no. 3 (2012): 525-46.

Hansen, Lene & Helen Nissenbaum. “Digital Disaster, Cyber Security, and the Copenhagen School” *International Studies Quarterly*, 53: (2009): 1155-1175.

Hansen, Lene, and Ole Waever. *European Integration and National Identity the Challenge of the Nordic States*. 1st ed. London: Routledge, 2003.

Healy, Jason. "Russia vs. Ukraine: The Cyber Front Unfolds." Atlantic Council. April 2, 2014. Accessed November 18, 2014. http://www.atlanticcouncil.org/blogs/new-atlanticist/russia-vs-ukraine-the-cyber-front-unfolds.

Huysmans, Jef. "The Question of the Limit: Desecuritization and the Aesthetics of Horror in Political Realism." *Journal of International Studies* 27 (1998): 569-89.

Laclau, Ernesto, and Chantal Mouffe. *Hegemony and Socialist Strategy: Towards a Radical Democratic Politics*. London: Verso, 1985.

Langer, Ralph. "Cracking Stuxnet, a 21st-century Cyber Weapon." TED. March, 2011. Accessed March 22, 2015. http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyber weapon?language=en#t-256497.

Liff, Adam P. "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War." *Journal of Strategic Studies* 35, no. 3 (2012): 401-28.

Luiijf, Eric & Healey, Jason. *Organizational Structures Considerations*. In Klimburg, Alexander. "National Cyber Security Framework Manual." NATO CCDCOE. 2012.

Marsh, Robert. "Critical Foundations Protecting America's Infrastructures." The Report of the President's Commission on Critical Infrastructure Protection. October 13, 1997. Accessed March 14, 2015. https://fas.org/sgp/library/pccip.pdf.

Microsoft Support. "Explanation of the Three-Way Handshake via TCP/IP." Explanation of the Three-Way Handshake via TCP/IP. February 12, 2010. Accessed March 21, 2015. https://support.microsoft.com/en-us/kb/172983.

Moses, Asher. "The Aussie Who Blitzed Visa, MasterCard and PayPal with the Low Orbit Ion Cannon." The Age. December 9, 2010. Accessed March 21, 2015. http://www.theage.com.au/technology/security/the-aussie-who-blitzed-visa-mastercard-and-paypal-with-the-low-orbit-ion-cannon-20101209-18qr1.html.

Murray, Andrew. *Information Technology Law: The Law and Society*. Oxford: Oxford University Press, 2010.

Nazario, Jose. "Estonian DDoS Attacks – A Summary to Date." Arbor Networks DDoS & Security Reports: The Arbor Networks IT Security Blog. May 17, 2007. Accessed March 11, 2015. http://www.arbornetworks.com/asert/2007/05/estonian-ddos-attacks-a-summary-to-date/.

Richards, Jason. "Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security." International Affairs Review. Accessed March 21, 2015. http://www.iar-gwu.org/node/65.

Rid, Thomas. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35, no. 1 (2012): 1-28.

Shackelford, Scott. *Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace.* Cambridge: Cambridge University Press, 2014.

Shapiro, Michael J. *Methods and Nations: Cultural Governance and the Indigenous Subject*. New York, New York: Routledge, 2004.

Taureck, Rita. "Securitization Theory And Securitization Studies." *Journal of International Relations and Development* 9 (2006): 53-61.

Tikk, Eneken, Kadri Kaska, and Liis Vihul. "International Cyber Incidents: Legal Considerations." Cooperative Cyber Defence Centre of Excellence (CCD COE). 2010.

Touré, Hamadoun. "The Quest for Cyber Peace." International Telecommunications Union. 2011. http://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-E.pdf.

Traynor, Ian. "Russia Accused of Unleashing Cyberwar to Disable Estonia." *The Guardian*, May 17, 2007, World News sec. Accessed March 12, 2007. http://www.theguardian.com/world/2007/may/17/topstories3.russia.

Wæver, Ole. *Securitization and Desecuritization"*, in Ronnie D. Lipschutz. *On Security*: 1995.

Primary Documents

Estonian Ministry of Defense. "Cyber Security Strategy." Cyber Security Strategy Committee. 2008.

Klimburg, Alexander., ed. "National Cyber Security Framework Manual." NATO CCDCOE. 2012.

Ministry of Economic Affairs and Communication."2014–2017 Cyber Security Strategy." 2014.

Schmitt, Michael N., ed. *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*. Cambridge University Press, 2013.

Vaks, Toomas., ed. "Summary of the Estonian Information System's Authority on Ensuring Cyber Security in 2012." 2012.

Vaks, Toomas., ed. "2013 Annual Report Cyber Security Branch of the Estonian Information System Authority." 2013.

Vaks, Toomas., ed. "2014 Annual Report Cyber Security Branch Of the Estonian Information System Authority." 2014.