SECURING CYBERSPACE: NATO'S CYBER DEFENCE POLICY AS A SECURITY DISPOSITIVE

Carla Spiegel

Student ID: 4113764

Master's Thesis

Thesis Supervisor: Dr. Ozan Ozavci
MA International Relations in Historical Perspective
2016/2017
Utrecht University
Word count: 21,772

TABLE OF CONTENTS

ABSTRACT

Cyberspace is a physically borderless space that challenges the rules and norms of international relations. The cyber attacks on Estonia in 2007, the cyber component of the Russo-Georgian War in 2008, as well as the cyber attacks that accompanied the Russian invasion of Ukrainian Crimea in 2014, are all events that alerted states and international organizations to the role of the cyber domain in interstate conflict and international security. The prospects of cyber war and the cyber attacks in Eastern Europe prompted the North Atlantic Treaty Organization (NATO) to develop norms and regulations to secure the digital infrastructures of its member states. NATO's Cyber Defence Policy has developed into a security dispositive, a combination of practices and discourses that are meant to respond to the cyber threat in the name of cooperative security and collective defence. NATO's cyber security dispositive has evolved from a defence policy concerned with the protection of its internal digital infrastructure in 2002 to a security network embedding cyber attacks into existing discourses of deterrence, information warfare and hybrid warfare in order to normalise cyber threats and incorporating them into existing political discourses of warfare and security. The Alliance has declared cyberspace its fourth domain of military operations, developing practices and discourses of knowledge about cyber threats that could contribute to the legitimization of the use of cyber capabilities in the future of interstate conflict. A historical analysis of NATO's cyber defence policy since 2002 will illustrate what the emerging trends in cyber security are and why the militarisation of cyberspace could endanger the free circulation of information in cyberspace should the use of cyber capabilities in interstate warfare become common practice in the future.

INTRODUCTION

"Cyberspace does not lie within your borders. Do not think that you can build it, as though it were a public construction project. You cannot. It is an act of nature and it grows itself through our collective actions"

- John Perry Barlow, *Declaration of Independence of Cyberspace (1996)*[1]

These are the words of John Perry Barlow, cyber libertarian and co-founder of the Electronic Frontier Foundation, who published the Declaration of Independence of Cyberspace in 1996. He envisioned cyberspace as a free, non-hierarchical and borderless network of ideas and relations, where equality and justice could reign without governments exercising sovereignty over people's virtual lives. A civilisation of the mind in which information could flow without regulation or censorship: that was how John Perry Barlow and other cyber utopians defined cyberspace and the meaning of the Internet in the 1990s. Barlow's written declaration was also one of the first representations of cyberspace as a political notion: it was to become a democratic space in which neither corporations nor governments could limit people's exercise of freedom. Effectively, the availability and free access of information and communication across the global Internet was meant to be an alternative to the traditional system of power held by states and private entities[2].

Since then, cyberspace has become a very different domain than the one imagined by cyber utopians: while the Internet has indeed proven to be a global phenomenon transcending physical boundaries, and societies across the globe have become more digitised and interconnected, cyberspace has also become a place that state and non-state actors can regulate in a myriad of different ways, making use of its technology in military operations, for propaganda and censorship purposes and to for espionage and criminal activity[3]. The cyber component is being incorporated into traditional norms and rules of interstate conflict and international law. What

[1] John Perry Barlow, "A Declaration of the Independence of Cyberspace", *Electronic Frontier Foundation*, 1996, https://www.eff.org/cyberspace-independence, accessed on Aug. 5, 2017.
[2] Evgeny Morozov, *The net delusion: How not to liberate the world*, (London: Penguin, 2011), xiii.
[3] Alexander Klimburg, *The Darkening Web. The War for Cyberspace*, (New York: Penguin, 2017), p. 89.

was hailed as an ungovernable and free space by cyber utopians has been interpreted by some observers as a political domain used to further the interests of states, international organisations, terrorist groups and corporate interests[4]. Threats from cyberspace have also become an item on the political agenda of states and intergovernmental organisations concerned with the security and safety of their digital infrastructures.

The possibility of cyber attacks by enemy nations, individual hackers or insurgent groups and the potentially catastrophic consequences for a nation's economic stability and national security are risks that cannot be ignored as governments increasingly rely on the Internet to operate efficiently. Military facilities, civilian computers and governmental websites are all vulnerable to hacking, the consequences of which can range from economic losses and systems failure to the leaking of information endangering the lives of civilians and state officials. Sometimes cyber attacks can amount to nothing more than 'Weapons of mass annoyance'[5], as hackers can shut a website down for a few hours or send political pictures to the screens of users. However, the potential for disastrous outcomes of cyber attacks is readily imaginable: the loss of life-saving infrastructures, or the collapse of communications technology of a government in crisis, are all scenarios that are at least theoretically possible for an experienced hacker to achieve.

Policy makers can as easily imagine these doomsday scenarios as science-fiction writers. Even though cyberspace might be a recent virtual reality, its importance for our everyday lives and the danger it presents for the security of populations is not virtual. In order to defend digital infrastructures against a variety of cyber attacks, nations and intergovernmental bodies are tasked with developing an effective strategy to secure their information and communications systems. But how do you secure a space that has no physical boundaries, belongs to no sovereign nation in the Westphalian sense of the term, and is accessible by and shared with practically everyone with a computer?[6] Cees J. Hamelink defines cyberspace as "a geographically unlimited, non-physical space, in which - independent of time, distance and location - transactions take place between

[4] Klimburg, *The Darkening Web. The War for Cyberspace*, 18.
[5] PBS Frontline. "Interview with James Lewis (2003)". [2003 Electronic Resource], http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/lewis.html, accessed on Aug. 20, 2017.
[6] Nazli Choucri, "Emerging Trends in Cyberspace: Dimensions & Dilemmas," *Williams and Fiddner, Cyberspace: Malevolent Actors, Criminal Opportunities, and Strategic Competition* (2012): 17.

people, between computers and between people and computers"[7]. Civilians, criminals, corporations and other private parties, as well as governments that are at war with each other or share no common interest all inhabit the same cyberspace in the form of the constant circulation of information and currency, participating daily in the flow of data that is filtered, targeted, protected, hidden from certain actors and revealed to others.

Amongst the several strategies developed to find a way to secure cyberspace despite the challenging interaction between cyberspace and the rules and laws of international relations is the North Atlantic Treaty Organisation's cyber defence policy, which aims to protect the integrity and functionality of the digital infrastructures of member states and their populations[8]. As a collective defence organisation, NATO works to defend the territories of its member states in Europe and North America. Its mandates of collective defence, risk management and cooperative security extend to the organisation's areas of operations in the events of armed conflicts or substantial threats on its member states. In its Warsaw Summit Communiqué in 2016, the Alliance recognised cyberspace as "a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea"[9]. This declaration is the result of fifteen years of a Cyber Defence Policy that has been evolving since cyber threats first made it on the organisation's political agenda in 2002[10]. NATO's cyber defence strategy is producing new practices and discourses about what constitutes a cyber threat and what its role in the future of the organisation's defensive operations will have. Comprised of 29 nations, NATO is one of the most important actors in the debate over the impact of cyber capabilities on interstate conflict and warfare.

NATO's cyber security strategy exposes many dilemmas about the interaction between cyber threats and the organisation's conventional operations that will affect salient issues like war, peace and the protection of digital infrastructures on one hand and compromising the free flow of

[7] Cees J. Hamelink, *The Ethics of Cyberspace*, (London: SAGE Publications, 2001), 9.
[8] North Atlantic Treaty Organization. *Defending the Networks: The NATO Policy on Cyber Defence* (Brussels: North Atlantic Treaty Organization, 2011).
[9] North Atlantic Treaty Organization. *Warsaw Summit Communiqué* (Brussels: North Atlantic Treaty Organization, 2016), 15.
[10] North Atlantic Treaty Organization. "Cyber Defence," http://www.nato.int/cps/en/natohq/topics_78170.htm, accessed on Aug. 16, 2017.

information and communications on the other[11]. Understanding what the fundamental concepts of NATO's Cyber Defence Policy are will contribute to the debate about how to best incorporate cyber threats into current policies and theories of interstate conflict and war. NATO's cyber defence policy is a legitimising practice, which will support a certain conceptual view of cyberspace and neglect others. The need to identify which discourses of cyber threats are becoming legitimate lies in the potentially disastrous effects of getting it wrong: as a collective defence organisation, NATO is tasked with the defence and security of its member states. If the organisation misinterprets the cyber threat or its ability to control it, the way we understand war or interstate relations might change into a direction that will slowly disintegrate existing norms and practices in more conventional relations between actors interacting in the physical and the cyber world[12]. By taking a look at the admittedly short but fast-evolving history of the Alliance's cyber security efforts, I plan to outline why a more profound theoretical analysis of the relationship between cyberspace and traditional strategies of security and war is necessary for both policy makers and academia. Therefore, the research question of this paper is:

What are the practices and discourses of knowledge NATO's cyber defence policy is producing about the future of cyber war and interstate conflict?

I hope to answer this research question through a careful analysis of the evolution of NATO's Cyber Defence Policy since 2002. A historical analysis of NATO's cyber strategy and how it was influenced by the cyber attacks on Estonia in 2007, Georgia in 2008 and Ukraine in 2014 will shed light on the potentially dangerous implications NATO's cyber policy practices might have for the future of cyber war and interstate conflict. NATO is operating in the cyber domain alongside other powerful actors, such as China and Russia. Alexander Klimburg has noted that Russia and NATO have two very different concepts of the role of cyber capabilities in warfare[13]. It reminds us that any security discourse co-exists with other, often contradicting, discourses that are relevant to an effective cyber security strategy for NATO. Especially now that the tensions between Russia and the organisation's member states have found expression in conflicts in Eastern Europe involving the cyber component, it is unlikely that NATO is

[11] Klimburg, *The Darkening Web. The War for Cyberspace*, 18.
[12] Klimburg, *The Darkening Web. The War for Cyberspace*, 12.
[13] Klimburg, *The Darkening Web. The War for Cyberspace*, 17.

developing a cyber security policy unrelated to its more conventional operations in its Eastern area of influence or that it is not informed by the evolution of Russia's use of cyber capabilities in recent years.

The term "cyber war" started to appear in the media and policy debates after it was uncovered that U.S. governmental websites including the Pentagon and NASA had been hacked[14]. The cyber attacks known as *Moonlight Maze* were traced to Russian Internet addresses at the Russian Academy of Sciences in Moscow, but any involvement by the Kremlin could not be proven beyond doubt[15]. The discovery of *Moonlight Maze* illustrated the importance of installing cyber defence mechanisms on both national and multinational levels, but more importantly, it opened up a debate about the future of cyber war and how NATO could secure cyberspace like it secured its other domains of operations.

Key events influenced the direction NATO's cyber defence would take: a disagreement with the Russian government and the Estonian Russian minority in 2007 exposed Estonia, a NATO member state, to a month-long series of cyber attacks to its information and communications technologies. The websites of governmental bodies, media outlets, banks and other Estonian private and public services came under attack in cyberspace, prompting both NATO and Estonia to rethink their cyber security strategies[16]. In August 2008, the war between Georgia and Russia was accompanied by a number of similar cyber attacks on Georgian digital infrastructure[17]. Even though Georgia is not a NATO member state, the event alerted NATO to the real use of cyber capabilities in the context of an armed conflict, further changing the debate over the challenges to cyber security and the role of cyber attacks in interstate conflicts. Finally, the Russian annexation of the Ukrainian region of Crimea in 2014 embedded the cyber security discourse in a context of hybrid warfare, a term to describe Ukraine's experience, namely being the victim of

[14] PR Newswire. "Newsweek Exclusive: 'We're in the Middle of a Cyber War' (September 12, 1999)". [1999 Electronic Resource], http://www.prnewswire.com/news-releases/newsweek-exclusive-were-in-the-middle-of-a-cyberwar-74343007.html, accessed on Aug. 16, 2017.
[15] Alexander Klimburg, "Mobilising cyber power," *Survival* 53.1 (2011): 49.
[16] Christian Czosseck, Rain Ottis, and Anna-Maria Talihärm, "Estonia after the 2007 cyber attacks: Legal, strategic and organisational changes in cyber security," *Case Studies in Information Warfare and Security: For Researchers, Teachers and Students* 72 (2013).
[17] Eneken Tikk et al. "Cyber attacks against Georgia: Legal lessons identified," *NATO Cooperative Cyber Defence Centre of Excellence, Tallinn*, (2008): 3-45.

cyber attacks and propaganda campaigns during an invasion by Russian forces on the ground[18]. In all three cases, NATO had to balance its development of a cyber security strategy with its operations and interests in the organisation's Eastern European area of influence and its tense relationship with Russia. Those processes demonstrated how important the historical and political contexts of conventional interstate conflict are for the development of NATO's cyber security policy, which is often presented as a technical challenge by the Alliance[19]. NATO's cyber policy is heavily influenced by the pre-existing conditions of its more conventional operations and discourses, such as its operations to protect its Eastern European members from further Russian aggression.

The way NATO member states choose to define the nature of the cyber threat and how to respond to it collectively will reveal what the strengths and weaknesses of the organisation's cyber defence policy are and how to improve the Alliance's cyber security. More importantly, a genealogy of the events in Eastern Europe that impacted and changed NATO's cyber defence illustrates that the security of cyberspace is closely interlinked with NATO's other, more conventional security concerns. The practices and discourses the organisation makes use of to conceptualise cyber threats are influenced by practices and discourses already embedded in NATO's strategic history. However, cyberspace presents NATO with a set of challenges that might require new concepts and practices to prepare for a future in which cyber threats will become a part of interstate war.

As many observers have noted, the rules and regulations of interstate warfare often do not apply in cyberspace and NATO's more conventional defence and security strategies might be up against a cyber threat that cannot be defended against through existing practices and discourses[20]. Furthermore, there are a number of concerns about NATO's statement that cyberspace is a domain of military operations, which classifies cyber as a space similar to the physical places NATO operates in. As opposed to the land, air and sea, cyberspace is

[18] Maria Snegovaya, "Russia Report I: Putin's information warfare in Ukraine. Soviet Origins of Russia's Hybrid Warfare," *Institute for the Study of War* (2015).
[19] North Atlantic Treaty Organization. *Defending the Networks: The NATO Policy on Cyber Defence* (Brussels: North Atlantic Treaty Organization, 2011).
[20] Christian Malis, "Unconventional Forms of War," (In *The Oxford Handbook of War*, 185-198. Edited by Julian Lindley-French and Yves Boyen. Oxford: Oxford University Press, 2012): 194.

geographically limitless and traditional hierarchical power relations or concepts such as territorial sovereignty do not function according to the same logic as in the physical world[21]. Cyberspace requires new rules and norms for state and non-state actors to share the virtual domain. NATO's militarisation of cyberspace in the name of cyber defence and security could compromise the freedom of speech and privacy of the population NATO's member states seek to protect, since civil society shares the same virtual space as national militaries.

Entering the Cyber Security Debate: The Legal, Technical and Politico-Strategic Layers of Cyberspace

The secondary literature on NATO's cyber defence policy has mostly focused on two areas: the legal challenges of incorporating cyber threats into international laws and the operational and technical challenges the organisation faces in implementing its strategy effectively. Discussions about NATO's Cyber Defence Policy have to keep up with the rapidly changing nature of the cyber threat. Embedding cyber attacks into the concepts of Russia's current warfare tactics, information and hybrid warfare, as well as the frequent use of deterrence theory applied to cyberspace by NATO and members of academia are all attempts to define cyberspace within the perimeters of existing theories and practices of warfare. However, due to the novelty of the phenomenon there is little literature on the impact such theories and practices can have on the implementation of a cyber security agenda and what consequences the use of certain theoretical frameworks have for the future of cyber activity in interstate conflict.

The danger of letting a cyber defence strategy like NATO's evolve without examining its conceptual framework is best put by Alexander Klimburg, who recognises that studying the responses to the technological advancement of cyberspace is as important as the study of the cyber threat itself:

"The aspirations of states in cyberspace, together with the technical realities of this new artificial world, are creating significant risks for human welfare writ large. These risks are

[21] Nazli Choucri, "Emerging Trends in Cyberspace: Dimensions & Dilemmas," *Williams and Fiddner, Cyberspace: Malevolent Actors, Criminal Opportunities, and Strategic Competition* (2012): 3-4.

associated with new means to not only inflict large-scale destruction in interstate conflict and war but also do catastrophic damage to liberal democratic societies through subtle reframing of information overall as a weapon"[22].

Klimburg's recent book *The Darkening Web* is an in-depth analysis of governments' perceptions and framing of cyberspace through their practices of cyber security. I wish to contribute to the discussions of the legal, technical, operational and politico-strategic layers of cyberspace by placing the interaction between NATO's cyber security and the unique challenges cyberspace poses to the aforementioned layers in a historical analysis of a complex, dynamic and knowledge-producing security strategy in the 21st Century. NATO's cyber security can be seen as a legitimising practice, by which certain practices and discourses of knowledge about cyber threats are employed to defend and secure NATO member states. However, cyberspace presents novel challenges to the Alliance and its mandates of collective defence and cooperative security on all layers. I wish to explore the complexity and interconnectedness between NATO's cyber security and the cyber threats it is exposed to. Examining how NATO has incorporated the ambiguous relationship between cyberspace and security practices in the physical world will point towards challenges from cyberspace that remain unresolved and continue to have an unpredictable impact on the future of interstate war.

I argue that NATO is attempting to secure cyberspace without addressing the interaction and interdependence between the Alliance's security operations in its Eastern area of influence and the strategic ambiguity of cyberspace. The Alliance is producing security practices and discourses that focus primarily on the technical and operational challenges of cyberspace[23], which in turn determine the legal challenges of attribution and the categorisation of cyber attacks as armed attacks. However, political and strategic decisions made in cyber policy by the Alliance are closely linked to its pre-existing practices of deterrence and resilience and embedded in a wider discourse about Russia's modern warfare tactics, namely the emerging theoretical concepts of information warfare and hybrid warfare[24]. Therefore, even though cyberspace might be

[22] Klimburg, *The Darkening Web. The War for Cyberspace*, 2.
[23] Klimburg, *The Darkening Web. The War for Cyberspace*, 17.
[24] - North Atlantic Treaty Organization. *Defending the Networks: The NATO Policy on Cyber Defence* (Brussels: North Atlantic Treaty Organization, 2011).

strategically challenging, NATO's Cyber Defence Policy is a complex set of security mechanisms that could shape the future of interstate conflict, as well as the practices and discourses actors will employ to navigate the cyber domain. The focus of this analysis will therefore be the strategic implications of NATO's Cyber security discourse for the future of interstate war.

Part 1 will be dedicated to the theoretical framework used to analyse the main practices and discourses of NATO's cyber security strategy. In order to be able to conceptualise the problem of cooperative security in cyberspace theoretically I will make use of Michel Foucault's work on security. By embedding NATO's Cyber policy into the theoretical framework of Foucault's concept of a security dispositive, I want to explore the intersubjective relationship between cyber security discourses and practices and the complex structure of cyberspace. I will further present the sources I have chosen to paint a picture of NATO's cyber defence policy since 2002 and explore the limitations of this study.

In Part 2, three cases will be analysed in detail: the cyber attacks on Estonia in 2007, the cyber component of the Russo-Georgian War in 2008, and the cyber component of the Russian annexation of Ukrainian Crimea in 2014. These cases will illustrate which specific challenges from cyberspace prompted NATO to change its cyber defence policy in its Eastern area of influence in Europe and move towards an understanding of cyberspace as a fourth domain of operations that falls under international law.

In Part 3 I will delineate the most important discourses and practices NATO's cyber defence policy has produced about the future of cyber war and interstate conflict in response to the evolution of the cyber threat and Russia's warfare tactics. More importantly, I will map out how NATO's attempt to secure cyberspace might have dangerous consequences for the future of warfare. The militarisation of cyberspace by the Alliance poses many difficult questions about the classification of cyber threats as a weapons technology used in defensive cyber capabilities.

- North Atlantic Treaty Organization. *Warsaw Summit Communiqué* (Brussels: North Atlantic Treaty Organization, 2016), 16.

As we will see in Part 4, several international developments are likely to influence NATO's cyber security strategy and the Alliance's relations with Russia in its Eastern area of influence. These developments are the following: the discovery of the cyber weapon Stuxnet, developed by the United States in conjunction with Israeli experts, could indicate yet another turn towards the use of cyber weapons as offensive capabilities in future interstate wars[25]. Secondly, Russia's participation in international cyber security and digital policy debates since the first Group of Experts (GGE) meeting in 2010 within a UN framework indicates that NATO's cyber security strategy depends on Russia's international cyber discourses and practices, as well as on the international norms and rules that will become legitimised in the UN[26].

In my conclusion I will summarise my findings and offer some thoughts on how to improve the understanding of the cyber component in NATO's future operations, including interstate conflict. Cyber is a space in which civilians and private parties interact with governments on a daily basis. NATO's offensive and defensive cyber capabilities and Russia's current approach to warfare might change the role of civilians in armed conflicts in the future. NATO's existing discourses focus on Russia's hybrid warfare but not on the unique characteristics of cyber threats as more than simply another weapons technology. Furthermore, neither technical nor legal solutions fully grasp the challenge cyberspace poses for collective defence and cooperative security. NATO's challenge in cyberspace is essentially politico-strategic, as the relations of power or the rules of combat in the international arena do not fully translate into cyberspace.

PART 1: THEORETICAL FRAMEWORK – FOUCAULT AND CYBERSPACE

1.1. NATO's cyber defence policy as a security dispositive

NATO is a military organisation tasked with collective defence and cooperative security of its member states and areas of influence[27]. As such, its Cyber Defence Policy serves both as a policy of defence and as a strategy of security, as the concepts and practices NATO employs are

[25] Jon R. Lindsay, "Stuxnet and the limits of cyber warfare," *Security Studies* 22.3 (2013): 365-404.
[26] Tim Maurer, "Cyber norm emergence at the United Nations," *Science, Technology, and Public Policy Program* (2011).
[27] David S. Yost, "NATO's evolving purposes and the next Strategic Concept," *International affairs* 86.2 (2010): 491.

not only meant to serve as a reaction to emerging threats but are also in place to prevent them and protect the population of its member states from any threats to national security in the future. In its cyber strategy, NATO has opted for preventive mechanisms of security as well as defensive capabilities to ensure that member states can protect the public from cyber attacks[28].

Cyber threats are a security threat for NATO because the Internet and cyberspace are being used by NATO member states and militaries, as well as by their citizens and state and non-state actors potentially posing a threat to the Alliance. Any action taken by NATO in cyberspace will inevitably have consequences for the citizens of its member states, presenting to the Alliance the rather difficult task of balancing the need to defend its information and communications infrastructures while at the same time ensuring its population's free access to information guaranteed by Western liberal democracies that make up a large number of NATO member states[29]. NATO must find a way to fulfil its mandate of collective defence and cooperative security in cyberspace without compromising the democratic liberties and rights of its citizens to take part in the free circulation of movement and information. As Myriam Dunn Cavelty writes:

"What becomes exceedingly clear from the developments and lessons of the last decade is that we cannot have both: a strategically exploitable cyberspace full of vulnerabilities—and a secure and resilient cyberspace that all the cyber-security policies call for"[30].

Especially when it comes to the question of 'cyber war' or the use of cyber capabilities in the future of interstate conflict, NATO is tasked with preparing a security agenda that keeps in mind that a variety of actors interact in cyberspace on a daily basis. Can the digital infrastructure of member states be secured without endangering the democratic rights of Internet-using civilians or undermining the trust between liberal governments and their citizens?[31] These security concerns have to be considered in NATO's coordinated approach to cyber attacks. However, security is a dynamic process in which the perception of a threat and the knowledge and practices

[28] North Atlantic Treaty Organization. *Defending the Networks: The NATO Policy on Cyber Defence* (Brussels: North Atlantic Treaty Organization, 2011).
[29] Klimburg, *The Darkening Web. The War for Cyberspace*, 15.
[30] Myriam Dunn Cavelty, "Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities," *Science and Engineering Ethics* 20.3 (2014): 711.
[31] Klimburg, *The Darkening Web. The War for Cyberspace*, 18.

produced in reaction to it determine the direction of a security policy as much or maybe even more than the external threat itself[32]. The cyber attacks on Estonia, Georgia and Ukraine certainly prompted NATO to change its cyber policy. The impact of those attacks and what they revealed about the cyber threat are illustrated in the three case studies to follow. However, the discourses and practices the Alliance has produced in order to give the cyber threats meaning and create counter-acting strategies, a process called 'securitisation', is as important to the study of cyber security as the conceptualising the external threat[33]. A historical analysis of the development of NATO's Cyber Defence Policy will illustrate this intersubjective aspect of cyber security and reveal which discourses and practices have been legitimised by the Alliance.

Cyber security is a fairly recent term in academia and policy-making and refers to "a broad range of practices, tools and concepts related closely to those of information and operational technology security"[34]. Cyber security is conducted by states and intergovernmental organisations that do not only seek to protect their internal information and communications infrastructure, but also make use of cyber capabilities to conduct military operations and create a strategy that includes the cyber component. NATO's cyber defence policy is effectively a strategy of cyber security, in which the future of cyber threats and cyber warfare produce certain practices and discourses its member states will employ to meet the challenges from cyberspace in the future.

In a collection of his lectures at the Collège de France in 1977 and 1978, Michel Foucault describes the mechanisms by which security dispositives anticipate present and future threats and develop strategies to counteract them[35]. A security dispositive is a set of practices and discourses of knowledge put in place to respond to and interact with an emergent threat as it appears in the present, and control how it might evolve in the future. In other words, security dispositives are

[32] Beatrice De Graaf, and Cornel Zwierlein, "Historicizing Security - Entering the Conspiracy Dispositive," *Historical Social Research/Historische Sozialforschung*, 38, no. 1 (143), (2013): 49.
[33] Ibid, 49.
[34] Joe Franscella, "Cybersecurity vs. Cyber Security: When, Why and How to Use the Term." *InfoSec Island* (2013), http://www.infosecisland.com/blogview/23287-Cybersecurity-vs-Cyber-Security-When-Why-and-How-to-Use-the-Term.html, accessed on Aug. 20, 2017. Quoted by: Alexander Klimburg, *The Darkening Web. The War for Cyberspace*, 70,
[35] Michel Foucault, *Security, territory, population: lectures at the Collège de France, 1977-1978*, (New York: Macmillan, 2007).

closely linked to the principles of uncertainty and risk calculation, as the probabilities of a threat's evolution are weighed and analysed in order to develop efficient strategies to regulate it[36]. For an effective cyber security and defence policy, NATO has to determine the nature of the cyber threat and respond to changes in the way the cyber component affects its more conventional operations. Furthermore, NATO's pre-existing discourses and practices are incorporated into the cyber security discourse in order to regulate cyber threats in the context of existing security operations, norms and values the Alliance has established since its conception in 1949. Cyber threats and even the possibility of cyber warfare are woven into the fabric of the status quo, of the existing practices and discourses in foreign relations, interstate conflict and warfare in the other three domains of air, land and sea. Contrary to other theories of security, Foucault's suggests that rather than installing a state of exception to counter cyber threats, suspending rule of law in the name of security, a security dispositive normalises a threat by making it work with the existing conditions of reality, or what is considered "normal":

"[T]he operation of normalization consists in establishing an interplay between these different distributions of normality and [in] acting to bring the most unfavorable in line with the more favorable"[37].

Borrowing from deterrence practices developed in the Cold War, for example, NATO has paid considerable attention to deterring cyber threats. The organisation has also categorised the new cyber threat into existing standards by declaring that like the land, the air and the sea, cyberspace was considered as a domain of military operations in which the alliance would defend itself from cyber threats[38]. NATO's Cyber Security dispositive underlines the urgency and inevitability of cyber threats: urgent because the security of information and communications technology of its member states is essential to the function and exercise of power and governance (and the cases of Estonia, Georgia and Ukraine have served as examples of the nature of the cyber threat), and inevitable because the Alliance and its citizens, as well as potentially hostile actors, are not going to stop making use of cyber capabilities and will possibly

[36] Ibid, 61.
[37] Ibid, 63.
[38] North Atlantic Treaty Organization. *Warsaw Summit Communiqué* (Brussels: North Atlantic Treaty Organization, 2016), 15.

increase their use in the future. NATO's Cyber Security dispositive does not prohibit or limit the cyber domain in an attempt to secure it: it functions through and with the expansion of cyberspace into all areas of political governance, practices of warfare and the everyday lives of citizens.

According to Foucault, "…security will try to plan a milieu in terms of events or series of events or possible elements, of series that will have to be regulated within a multivalent and transformable framework"[39]. A milieu is a space in which a series of uncertain elements can unfold and be regulated by the mechanisms of security in place[40]. Interestingly, Foucault sees security as the process by which freedom of circulation or movement can operate without hindrance, by containing the uncertain and abnormal elements affecting target populations and incorporating them into the normal. A distinctive feature of security dispositive is that they do not limit or enclose spaces in the process of securing; they regulate them by "making possible, guaranteeing, and ensuring circulations; the circulation of people, merchandise, and air, etc"[41]. Emergent threats such as cyber attacks are not phenomena that NATO will aim to defend against by limiting or prohibiting the use of cyber capabilities, as national governments and the organisation itself make use of cyberspace to improve their information and communications capabilities for purposes of governance and military operations. Civil society's use of cyberspace and its many transactions and services might suffer from mechanisms of security employed by NATO to militaries cyberspace and prepare for the event of a hostile cyber attack.

So-called Information Societies, a term used often by the NATO-adjacent CCD COE in its reports on cyber threats, are highly digitalised societies in which many interactions between citizens and the government occur in cyberspace[42]. Nowadays, the circulation of data and information is embedded in the governments of nations and the services they provide to their citizens. This is especially true in liberal Western democracies, where freedom of movement and

[39] Michel Foucault, *Security, territory, population: lectures at the Collège de France, 1977-1978,* (New York: Macmillan, 2007), 20.
[40] Ibid, 20.
[41] Ibid, 29.
[42] Eneken Tikk, Kadri Kaska and Liis Vihul, *International cyber incidents: Legal considerations*, (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2010): 16-17.

circulation is facilitated to match the needs and rights of citizens[43]. NATO's security dispositive must therefore balance the protection of the freedom of circulation in cyberspace with the defence against intrusion into the digital infrastructures of its member states. By imprinting cyberspace with its emerging practices and discourses, NATO is militarising a space that is shared with anyone that owns a computer. This practice might be counterproductive for the free circulation of information and communications that represents the other side of NATO's cyber security dispositive.

The dangers of the emerging practices and discourses of NATO's cyber security dispositive are outlined in Part 3 of this paper. An analysis of the main practices and discourses of cyber security reveals that the external factor, namely the unique and complex structure of cyberspace, challenges the Alliance's attempts to apply existing discourses and practices of security in the cyber domain. However, as security is an intersubjective process, cyberspace and the future of cyber war can equally be altered and embedded in the norms, values and knowledge NATO is producing about cyber threats. In other words, NATO's decision to consider cyberspace a fourth domain of operations seems to indicate that the Alliance is preparing for a future in which cyber war will be common practice and cyberspace will be increasingly militarised. NATO is not alone in determining changes in warfare: actions by highly cyber-advanced nations like Russia and China, as well as insurgent groups or even private actors using cyber capabilities all factor into creating a landscape in which future wars might be fought in cyberspace. However, NATO's discourses and practices are creating a cyber security strategy that contributes to the direction the cyber component of interstate conflict is taking. The ambiguous relation between the challenges of cyberspace and NATO's cyber security practices and discourses lies in their interdependence and their influence on the other. This dynamic is what determines NATO's cyber security dispositive: not only is cyberspace problematised for an effective cyber security strategy, the security practices and discourses themselves can affect the norms, values and knowledge produced about the role of cyber threats in future warfare. Additionally, NATO operates on the premise that the integration of the cyber component into existing forms of conflict and warfare is

[43] Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," *Journal of Strategic Security* 4, no. 2 (2011): 56.

an inevitable process. How it anticipates the actions of cyber advanced nations like Russia will determine its cyber defence policy and prioritise one cyber security discourse over others.

By interpreting NATO's Cyber Defence Policy as a security dispositive, I aim to lay out the practices and discourses the Alliance has produced about cyber threats and what their implications for the future of cyber war are. In order to do so I will analyse fifteen years of NATO Cyber policy, starting in 2002 when the Alliance first put cyber threats on the political agenda. A number of sources are available for analysis: NATO's yearly *Summit Declarations* offer an overview of the Alliance's priorities and strategic steps it seeks to implement in the cyber domain. Furthermore, a Cyber Defence Policy was outlined in 2008 and improved in 2011, which illustrates NATO's practices and discourses specific to cyber threats in reaction to the events in Estonia, Georgia and Ukraine. Perhaps the richest source of information on NATO's cyber strategy comes from the NATO Cooperative Cyber Defence Centre of Excellence, an international military organisation in Tallinn, Estonia, founded on May 14, 2008 after the cyber attacks on Estonia a year earlier.

Accredited by NATO, the CCD COE describes itself as a "multinational and interdisciplinary hub of cyber defence expertise"[44] and focuses on "technology, strategy, operations and law"[45]. Its location in Tallinn is no coincidence, showing once more how much impact the cyber attacks on Estonia had on NATO's conception of the cyber threat and the need to secure cyberspace. As of 2017, the centre is sponsored by Estonia, Germany, Italy, Latvia, Lithuania, Slovakia, Spain, Hungary, Poland, the United States, the Netherlands, the United Kingdom, France, the Czech Republic, Greece and Turkey[46]. Non-NATO members Austria and Finland joined the centre as contributing nations in 2014 and 2015 respectively. Since its conception in 2008 the CCD COE has served NATO in an advisory function, producing a number of publications called the Tallinn Papers, as well as legal and policy papers surrounding the topic of cyber attacks and defence. While the work of the CCD COE does not represent the opinion or official policy of NATO, the centre was founded by the Alliance to research the topic of cyber defence and security and

[44] NATO Cooperative Cyber Defence Centre of Excellence, "NATO Cooperative Cyber Defence Centre of Excellence - Home Page," https://ccdcoe.org/, accessed on Aug. 18, 2017.
[45] Ibid.
[46] NATO Cooperative Cyber Defence Centre of Excellence, "History," https://ccdcoe.org/history.html, accessed on Aug. 18, 2017.

therefore provides a detailed overview of the the main discourses and practices that also appear in NATO's official publications. After the cyber attacks on Estonia and Georgia, the CCD COE published a detailed analysis of the events and their impact on legal proceedings and policy considerations for the Alliance. These analyses are not only informative of the concrete cyber threats, but also of the circulating discourses preoccupying NATO and the CCD COE. Furthermore, while the international community is struggling to determine how international law applies in cyberspace, The Tallinn Manual comes closest to establishing legal standards for cyber attacks: compiled by an international group of experts in 2013, the Manual is a non-binding legal guide for the application of international law to cyber warfare. While the document is not a part of NATO's official documents, members of NATO CCD COE acted as Project Manager and Project Coordinator, amongst others. Together, the sources from NATO's official declarations, the CCD COE's research into cyber security and the legal suggestions made in the Tallinn Manual are indicative of the discourses and practices the Alliance employs to construct its cyber security strategy.

Unfortunately, any undisclosed practices and discourses produced by NATO in the area of cyber security and defence cannot be included in this study for lack of access. However, cyber security is meant to interact with and inform the public about the cyber threat. Therefore, the way the Alliance represents its cyber security practices and discourses to the public is informative of the meaning, norms and values NATO is attaching to the cyber threat and its role in future interstate conflicts. Another limitation of this study is that an analysis of NATO's cyber security dispositive fails to consider the opinions and policies produced by other relevant actors in the field, most notably Russia. The case studies presented in this paper portray three cyber attacks that were embedded in a political context involving a conflict with Russia. The language barrier and the scope of this paper limit the possibilities of analysing and portraying Russia's cyber security approach and legitimising practices. In Part 2 I will provide a brief summary of NATO's dialogue with Russia about international cyber security practices. The terms 'information war' and 'hybrid war' have been incorporated into the discourse of Russia's modern warfare tactics by other actors, including NATO. They are essential to our study of the Alliance's cyber security practices and discourses but another interesting study would be to see how NATO's interpretation and portrayal of Russia's cyber activity contrasts with Russia's own statements and

practices. However, for the purpose of this paper only NATO's interpretations of the events in Eastern Europe will be considered.

In the following sections, we will witness the evolution of NATO's cyber security dispositive, from a defence policy concerned with the protection of its internal digital infrastructure in 2002 to a security network embedding cyber attacks into existing discourses of deterrence, information warfare and hybrid warfare in order to normalise cyber threats by incorporating them into existing political discourses of warfare and strategy. The legal and technical challenges of cyberspace become equally important in NATO's cyber security after the cyber attacks on Estonia in 2007, as the organisation focuses on legal and technical solutions to the security of cyberspace, neglecting the political implications of militarising cyberspace in the name of security. As we will see, the result is a cyber security dispositive that underplays the human consequences of a future in which cyber will be part of interstate conflict in a world in which nations will always share cyberspace and cyber power with private actors and civilians, and overplays the importance of technical solutions to an essentially political problem: governance and security in cyberspace. Russia's approach to cyber warfare as a psychological tool for purposes of propaganda and information campaigns is matched by NATO's technical approach to cyber security, which projects the illusion that the organisation is prepared for the consequences of a world in which cyber warfare is common practice.

Part 2: RUSSIA'S CYBER STRATEGY IN EASTERN EUROPE AND ITS IMPACT ON NATO'S CYBER DEFENCE POLICY

2.1. Cyber Attacks against Estonia in 2007 in the Context of Political Conflict

Historical Context

On April 30, 2007 the Estonian government moved the Bronze Soldier, a memorial from World War II to remember the Soviet liberation of Estonia from the Nazi occupation, from a

central location in the Estonian capital Tallinn to the city's military cemetery[47]. Estonian Russians, the nation's largest minority, viewed the government's decision to move the Bronze Soldier to a more secluded place as an attempt to further marginalise the Russian speaking community in Estonia, while for ethnic Estonians the statue represented Soviet oppression of Estonia in the past.[48] After the collapse of the Soviet Union in 1991, Estonia joined NATO in 2004 along with many other post-Soviet nations. The debate over Russian influence in Eastern European territories and the expansion of institutions like the European Union and NATO into the Eastern parts of Europe have been the subject of contention between Russia and its post-Soviet neighbours.[49] The announcement that the statue would be moved to a less central location in Tallinn sparked violent riots in the streets of Estonia on April 26 and 27, 2007. The rioters were predominantly of ethnic Russian origin and accused the Estonian government of wanting to change the role of the Soviet Union in Estonian history[50]. Following a violent confrontation between police and protesters, the Estonian government moved the Bronze Soldier in the late hours of April 27 and erected it in the Tallinn Military Cemetery on April 30[51].

The Escalation of April 27

That same night a number of cyber attacks targeted Estonian governmental websites, such as the website of political parties and news outlets with Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, which cause websites to become inaccessible to users. A process called ping-flooding was also used as a call to flood websites with so-called ping requests appeared on several Russian-speaking blogs and forums.[52] Ping floods are meant to test the performance of target networks under high-load conditions, resulting in a denial of service (DoS) if the target website is overloaded with ping requests. Other types of cyber attacks included the defacement of websites, as hackers replaced an image of Estonian Prime Minister

[47] Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," *Journal of Strategic Security* 4, no. 2 (2011): 50.
[48] Ibid, 51.
[49] See for example: John J. Mearsheimer, "Why the Ukraine crisis is the West's fault: the liberal delusions that provoked Putin," *Foreign Aff.* 93 (2014): 77-89.
[50] Eneken Tikk, Kadri Kaska and Liis Vihul, *International cyber incidents: Legal considerations*, (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2010): 15.
[51] Ibid, 16.
[52] Ibid, 20, 21.

Ansip with the face of Adolf Hitler on an official government website and conducted similar defacements on other Estonian websites. The cyber attacks lasted until May 18 and targeted websites ranged from governmental websites and Estonian Internet service providers to banks and other services provided by the private sector.[53]

Aftermath: Effects, Investigation and Responses

On April 28th the cyber attacks were declared to be coordinated attacks rather than isolated events[54]. Jack Aaviksoo, who was the Estonian Defence Minister at the time of the attacks, told WIRED Magazine: "This was the first time that a botnet threatened the national security of an entire nation[55]". Estonia is often called eStonia[56] because of its reputation as an information society: in an extensive study of the case of the Estonian cyber attacks on behalf of NATO's Cooperative Cyber Defence Centre of Excellence in Tallinn, Eneken Tikk and his colleagues found that by 2007, 98% of Estonian territory was covered with Internet access, while nearly 50% of Estonians used the Internet. Estonia also made use of digital signatures and governmental digital databases and procedures like citizens' income declarations and council elections were completed online.[57]Estonia's public e-services internet accessibility meant that it was highly dependent on the uninhibited functioning of its communication and information systems, which the cyber attacks in April and May 2007 crippled on a national scale. A report by NATO's CCD COE categorised the cyber attacks against Estonia as a substantial blow to the administrative functions of the country: "Considering that the law governing administrative procedure in Estonia ensures the right of every person to conduct operations with the state via electronic means, crippling the habitual communication channels not only constituted an inconvenience but also harmed the state's ability to carry out its administrative functions in accordance with

[53] Ibid, 20-22.
[54] Christian Czosseck, Rain Ottis, and Anna-Maria Talihärm, "Estonia after the 2007 cyber attacks: Legal, strategic and organisational changes in cyber security," *Case Studies in Information Warfare and Security: For Researchers, Teachers and Students* 72 (2013).
[55] Joshua Davis, "Hackers Take Down The Most Wired Country in Europe." *Wired Online*, August 21, 2007, https://www.wired.com/2007/08/ff-estonia/, accessed on Aug. 10, 2017.
[56] Ibid.
[57] Eneken Tikk, Kadri Kaska and Liis Vihul, *International cyber incidents: Legal considerations*, (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2010): 18.

applicable law"[58]. In other words, Estonia's dependence on information and communications technologies (ICT) made it especially vulnerable to cyber attacks, as many of its administrative and public services and interactions between the Estonian government and its citizen were conducted in cyberspace.

Another aspect of the cyber attacks against Estonia was the use of disinformation campaigns: defacements of websites by replacing the heads of state officials with the head of Hitler, for example, linked Estonia's current government to Nazi Germany, mirroring the argument of Russian nationalists that Estonia was trying to rewrite history by removing the Soviet Statue from the central square in Tallinn. Such techniques are meant to influence the perception and opinion of the public, while at the same time disrupting the information and communications systems of Estonia. The cyber attacks included pro-Russian propaganda that the Russian Federation benefited from while still being able to claim plausible deniability for the crime[59].

As a member of NATO, Estonia had the option to invoke Article 5 of the North Atlantic Treaty (1949) when it was targeted by cyber attacks in 2007. Article 5 states that:

"The Parties agree that an armed attack against one or more of them in Europe or North America shall be *considered an attack against them all* and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, *including the use of armed force,* to restore and maintain the security of the North Atlantic area[60]."

Article 5 is in place to enforce NATO's core task of collective defence, ensuring that member states come to each other's aid in the case of an attack. However, Estonia did not consider the

[58] Eneken Tikk et al. "Cyber attacks against Georgia: Legal lessons identified," *NATO Cooperative Cyber Defence Centre of Excellence, Tallinn,* (2008): 11.
[59] Tim Maurer, "Cyber Proxies and the Crisis in Ukraine," in *Cyber War in Perspective: Russian Aggression against Ukraine*, ed. Kenneth Geers (Tallinn: NATO CCD COE Publications, 2015), 81.
[60] North Atlantic Treaty Organization. *The North Atlantic Treaty* (Washington D.C.: North Atlantic Treaty Organization, 1949), 1. [Emphasis added by me].

cyber attacks on its digital infrastructure to constitute an armed attack[61]. Therefore, Article 5 was not invoked and NATO limited its support to aiding Estonia in the defence of its information and communications system and the subsequent investigation into the actors responsible for the attacks.

Lessons Learned for NATO: Towards a more centralised Cyber Defence Policy

On the technical layer, the nature and execution of the cyber attacks were not new. It was not their technical innovation rather than their scope and use in the given political context that would prove to have a lasting impact on Estonia's national cyber security policy and alert NATO to revise its cyber defence strategy. The cyber attacks exposed Estonia, one of the most digitalised nations in the world, to a new political threat that required categorisation by national authorities and multinational responses by international institutions of collective defence and security. The events in the Spring of 2007 pointed towards many issues of categorisation of the cyber domain in the domain of traditional international relations: when does a cyber attack constitute an armed attack and which conventional international laws apply to the unconventional cyber threat? More specifically, how can NATO incorporate the defence against cyber threats in its core tasks of collective defence, risk management and cooperative security?

In a research paper published by NATO's Defence College, Vincent Joubert argues that the events of Estonia in 2007 marked a considerable change of operational strategy in NATO's cyber defence policy: "The Alliance has long defended its information and communication systems, but has never faced major attacks that represented a critical threat to them. Cyber attacks were until quite recently considered to have limited potential for harm, so that technical responses were thought to be sufficient"[62]. Indeed, a close look at NATO's official declarations on cyber threats reveals an emphasis on technical solutions to cyber threats, such as the protection of NATO's key information systems, while cyber security was largely left in the hands of

[61] Christian Czosseck, Rain Ottis, and Anna-Maria Talihärm, "Estonia after the 2007 cyber attacks: Legal, strategic and organisational changes in cyber security," *Case Studies in Information Warfare and Security: For Researchers, Teachers and Students* 72 (2013): 1.
[62] Vincent Joubert, "Five Years After Estonia's Cyber Attacks: Lessons Learned for NATO?," *NATO Defense College, Research Division* (2012): 2.

individual member states[63]. The absence of a comprehensive cyber defence policy became a practical disadvantage for the organisation when the investigations into the actors behind the cyber attacks on Estonia revealed that there was no official protocol in place to respond to a cyber attack that could cripple the digital infrastructure of a member state. The reports by the Estonian and Allied CERT teams concluded that while some of the attacks could be traced to Russian IP addresses, any involvement by the Kremlin could not be proven[64].

This, however, did not discourage Estonia's foreign minister at the time, Urmas Paet, from accusing the Russian government of having orchestrated the cyber attacks: "The European Union is under attack, because Russia is attacking Estonia"[65]. While members of the Estonian government made similar accusations, NATO did not officially attribute the cyber attacks to the Kremlin. Attribution poses one of the major obstacles to international law and policy on the prosecution of cyber attacks: Attributing a cyber attack to a state actor because the computer from which the attack was launched makes use of its national cyber infrastructure is difficult because computers can be hacked and operated remotely. Jeffrey Carr, who created Project Grey Goose in 2008 to attempt to attribute cyber attacks to specific individuals, writes: "it is neither sufficient nor legally justifiable to simply trace an attack to a server located in a foreign country"[66]. Further efforts to find the people responsible for the cyber attacks were thwarted when Russia refused to cooperate with Estonia's efforts to investigate within Russian territory. By 2009 only one arrest had been made: Dimitri Galushkevich, a student and Estonian national of ethnic Russian origins, was tried and convicted for the illegal blocking of computer data and was fined roughly 1120 euros[67].

[63] North Atlantic Treaty Organization. *Riga Summit Declaration (*Brussels: North Atlantic Treaty Organization, 2006), 7.
Vincent Joubert, "Five Years After Estonia's Cyber Attacks: Lessons Learned for NATO?," *NATO Defense College, Research Division* (2012).
[64] Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," *Journal of Strategic Security* 4, no. 2 (2011): 53.
[65] Joshua Davis, "Hackers Take Down The Most Wired Country in Europe." *Wired Online*, August 21, 2007, https://www.wired.com/2007/08/ff-estonia/, accessed on Aug. 10, 2017.
[66] Jeffrey Carr, "Responsible Attribution: A Prerequisite for Accountability," *NATO Cooperative Cyber Defence Centre of Excellence, Tallinn Paper 6* (2014): 4.
[67] Eneken Tikk, Kadri Kaska and Liis Vihul, *International cyber incidents: Legal considerations*, (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2010): 28.

As a consequence of the difficulty Estonia and NATO faced in the prosecution of the cyber attackers and the lack of accountability of a state actor, Estonia focused on developing a comprehensive Cyber Security Strategy, which was adopted in May 2008, a year after the attacks had occurred[68]. NATO also implemented considerable changes: Following the annual summit meeting in Bucharest on April 2-4 in 2008, NATO devoted many more sections to the cyber threat in comparison to previous years, announcing the creation of a Policy on Cyber Defence that was approved in January 2008[69]. NATO emphasised the need for the protection of the organisation and member states' key information systems, but included a sentence on strengthening the organisation's capacity to assist Allied nations in countering cyber attacks[70]. On May 14, NATO established the Cooperative Cyber Defence Centre of Excellence (CCD COE) in Tallinn, the capital of Estonia. Following the cyber attacks on Estonia, the CCD COE and NATO started work on establishing the laws, rules and norms that were to govern interstate conflict in cyberspace.

The case of Estonia presented the first instance of a cyber attack targeting a nation's digital infrastructure on a large scale as part of a political conflict in NATO's Eastern area of influence. It also exposed limitations in international cooperation on the response and categorisation of cyber attacks within NATO's traditional defence norms and laws, prompting the creation of a centre of research and training that still operates to date. Estonia's national defences against cyber threats were strengthened considerably and NATO's pledge to create a separate policy on cyber defence moved up on the list of priorities on the organisation's political agenda. While the cyber attacks against Estonia revealed that a NATO member state could be crippled economically and socio-politically by cyber attacks, another incident a year later would present an instance of the use of cyber warfare as part of conventional warfare. This instance was the Russo-Georgian War in August 2008. While no NATO member state was directly involved, the role that the cyber component played during the conflict would have tangible implications for NATO's cyber defence strategy.

---

[68] Christian Czosseck, Rain Ottis, and Anna-Maria Talihärm, "Estonia after the 2007 cyber attacks: Legal, strategic and organisational changes in cyber security," *Case Studies in Information Warfare and Security: For Researchers, Teachers and Students* 72 (2013).
[69] North Atlantic Treaty Organization. *Bucharest Summit Declaration* (Brussels: North Atlantic Treaty Organization, 2008).
[70] North Atlantic Treaty Organization. *Bucharest Summit Declaration*, 11.

2.2. Cyber Attacks against Georgia during the Russo-Georgian War in 2008

Historical Context

was the case in Estonia, the cyber attacks against Georgia occurred within a broader historical and political context: these particular tensions between Georgia and Russia had been growing since the Georgian region of South Ossetia declared de facto independence from Georgia in 1991[71]. South Ossetia lies on the border between Georgia and Russia and many South Ossetians are of ethnic Russian origin or consider themselves Russian. The region's independence was not recognised by Georgia or the international community but despite efforts to resolve the conflict in 1991, South Ossetia remained de facto independent, while officially being under the sovereignty of Georgia. In 1992, a peacekeeping force comprising of Russian, Georgian and South Ossetian troops was tasked with maintaining stability in the region, but tensions ran high for the next sixteen years[72].

After an escalation of provocations and tensions in the region, Georgia attacked South Ossetian separatist forces on August 7 2008. A day later on August 8, Russia sent troops into Georgian territory with the stated intent to protect the interests of Russian citizens abroad[73]. Russian troops first remained in the South Ossetian region, but proceeded to move further into Georgian territory no longer considered to be under the mandate of the peacekeeping forces by the OSCE. Georgia considered Russian military presence on its territory as an act of military aggression and declared a state of war on August 9[74]. During the war, South Ossetian separatists proceeded to attack Georgian villages, forcing around 200,000 ethnic Georgians out of their homes in South Ossetia. According to a Human Rights Watch report, 22,000 villagers remained displaced from South Ossetia in 2014[75]. The Georgian government retreated from South Ossetia

[71] Eneken Tikk et al. "Cyber attacks against Georgia: Legal lessons identified," *NATO Cooperative Cyber Defence Centre of Excellence, Tallinn*, (2008): 4.
[72] Ibid, 4.
[73] Eneken Tikk, Kadri Kaska and Liis Vihul, *International cyber incidents: Legal considerations*, (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2010): 67.
[74] Eneken Tikk et al. "Cyber attacks against Georgia: Legal lessons identified," *NATO Cooperative Cyber Defence Centre of Excellence, Tallinn*, (2008): 5.
[75] Human Rights Watch, "Up In Flames Humanitarian Law Violations and Civilian Victims in the Conflict over South Ossetia (2009)." [2009 Electronic File], https://www.hrw.org/sites/default/files/reports/georgia0109web.pdf, accessed on Aug. 20, 2017.

on August 10, followed by a ceasefire negotiated by France on August 12. Russian forces remain in the de facto independent South Ossetia in violation of the ceasefire agreement, recognising the region as independent on August 26[76]. Georgia and Russia severed all diplomatic relations and Russian forces remained in undisputed areas of Georgia until October 2007, after which they retreated from all Georgian regions except Abkhazia and South Ossetia.

Cyber Attacks on Georgia: A New Component of Armed Conflict

Parallel to the physical confrontation, Georgia experienced a number of cyber attacks on governmental, media and financial institutions: just as in the case of Estonia in 2007, DDoS attacks, defacements of websites and ping flooding disrupted Georgia's digital infrastructure throughout the war against Russia[77]. The armed conflict would last until August 12, but the cyber attacks continued to disrupt Georgia's digital infrastructure for the entire month. The first cyber attacks on Georgia were launched a few months before the Russo-Georgian War broke out. So-called defacement of website attacks had already been recorded on July 19, 2008[78]. However, the largest waves of cyber attacks commenced on the same day the Russian invasion into Georgian territory began on August 8. Nonetheless, cyber attacks both preceded and accompanied the war between Georgia and Russia, making the Georgian experience with cyber attacks an important case study in the analysis of the future of cyber warfare.

Aftermath: Effects, Investigations and Responses

As opposed to Estonia, Georgia has limited internet connectivity, mainly being able to access the Internet via land routes to Turkey, Armenia, Azerbaijan and Russia[79]. Many of Georgia's connections to the Internet are interlinked with or pass through Russian infrastructure, constraining the country's ability to seek Internet connectivity outside of Russia. Furthermore, access to the Internet is much less common or spread out as for example in Estonia. However,

[76] Eneken Tikk et al. "Cyber attacks against Georgia: Legal lessons identified," *NATO Cooperative Cyber Defence Centre of Excellence, Tallinn*, (2008): 5.
[77] Ibid, 7-11.
[78] Eneken Tikk, Kadri Kaska and Liis Vihul, *International cyber incidents: Legal considerations*, (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2010): 69.
[79] Eneken Tikk et al. "Cyber attacks against Georgia: Legal lessons identified," *NATO Cooperative Cyber Defence Centre of Excellence, Tallinn*, (2008): 6.

Georgia's limited access to Internet connectivity did not stop hackers from using the same methods that were used in the cyber attacks against Estonia. While the services that were disrupted might not have had the same societal impact because the Georgian population is less dependent on the Internet for public and private services, we must not forget that Georgia's relative dependence on Russia for its Internet access could also have been a factor in the country's vulnerability to cyber attacks[80]. Furthermore, a fibre optic cable connecting Georgia to Western European Internet infrastructure via the Black Sea was nearly completed when Russian forces marched into Georgian territory in August[81]. The armed conflict between Russia and Georgia interrupted the building of that cable. This detail of the cyber conflict serves as a reminder that there is a physical component to cyberspace: the sabotage or destruction of fibre optic cables could become part of warfare in the future, as the Ukrainian case will show.

According to NATO's CCD COE report on the cyber attacks against Georgia, the second phase of cyber attacks that occurred during the war were coordinated and aimed at disrupting the effective communication between the Georgian government and its citizens: "Whereas in Estonia, the core of the damage consisted of obstructed access to socially vital electronic services provided by both the public and private sector, such as e-government and e-banking services, in Georgia, the heart of the damage lied in limiting the nation's options to distribute their point of view about the ongoing military conflict"[82]. The report implies that the individuals or groups behind the cyber attacks against Georgia were employing information blockage tactics, namely interfering with the ability of the Georgian government to communicate with its citizens undisturbed during an armed conflict. Attempts to propagate an anti-Georgian sentiment included the same methods used during the cyber attacks against Estonia, for example replacing the face of Georgian President Mikheil Saakashvili with the face of Adolf Hitler on the website of the President of Georgia and the Ministry of Foreign Affairs[83]. However, as opposed to the Estonian case, the cyber attacks also interfered with the ability of the Georgian state to communicate with its citizen during a war, which begs the question: are the cyber attacks against Georgia an act of war because they occurred during an armed conflict?

[80] Ibid, 6.
[81] Ibid, 6.
[82] Ibid, 15-16.
[83] Ibid, 7.

Georgia tried to secure its digital infrastructure by using the websites of other nations for the unhindered dissemination of information: Poland provided the website of the President of Poland for this purpose, and Georgia's Computer Emergency Response Team (CERT) teams were aided by CERT Poland, CERT France and CERT Estonia[84]. As was the case in Estonia, the cyber attacks could not be traced back to the Russian government. According to Project Grey Goose, a report on the cyber attacks on Georgia compiled by an Open Source Intelligence initiative, an analysis of Russian hacker forums revealed that they found no evidence of a direct involvement by the Kremlin, but nonetheless suggested the possibility that the Russian government could have effectively erased any traces of its involvement:

"We assess with high confidence that the Russian government will likely continue its practice of distancing itself from the Russian nationalistic hacker community thus gaining deniability while passively supporting and enjoying the strategic benefits of their actions"[85].

The CCD COE report, which cites the Project Grey Goose report as a source, also concludes: "The objective facts of the case are too vague to meet the necessary criteria of both state involvement and gravity of effect"[86]. It labels the attacks on Estonia and Georgia as a legal "grey area" and concludes correctly that while the media has once more turned to the catchy term "cyber war" to describe the cyber attacks on Georgia, under the current legal framework a cyber attack is not considered an armed attack and in neither case was it attributed to a state actor or agents of the state[87]. The Law of Armed Conflicts (LOAC) stipulates that an armed conflict is defined as "any difference arising between two States and leading to the intervention of armed forces… even if one of the Parties denies the existence of a state of war"[88]. Failure to attribute the attacks to the Kremlin and the gap in legal literature on whether cyber attacks are considered a weapon and therefore an armed attack therefore exclude any possibility of holding Russia accountable to the international community for the actions of hackers that might have operated

[84] Ibid, 14.
[85] Jeffrey Carr, "Project Grey Goose Phase I Report," *Project Grey Goose* (2008), 3.
[86] Eneken Tikk et al. "Cyber attacks against Georgia: Legal lessons identified," *NATO Cooperative Cyber Defence Centre of Excellence, Tallinn*, (2008): 23.
[87] Ibid, 29.
[88] Ibid, 19.

from within its borders. The case of Georgia illustrates once more that by 2008, cyber attacks had no well-defined place in international law, especially not when it came to its role in armed conflict.

The problem of state attribution is not only a legal challenge for NATO. Strategically, Russia's actions in Eastern Europe are difficult to respond to if no legal framework exists to hold a state responsible for a cyber attack. Should a NATO member state engage in an armed conflict, Article 5 could be invoked according to the rules and regulations of the North Atlantic Treaty[89]. However, the cyber attacks accompanying the armed conflict would be excluded from the definition of armed conflict and no state actor could be made accountable, even if, as it was the case in Georgia, the communication between a government and its public is compromised as a result. On the other hand, failure to prove any involvement by the Russian government doesn't stop the international media and the citizens of the Eastern European nations under attack from suspecting Russia's involvement, putting pressure on NATO to respond to the perceived injustice of its member state Estonia and other Eastern European member states. This dilemma puts NATO in a difficult position, as its operations in the Eastern European area of influence demands that the organisation's relations with Russia be categorised in a certain way for strategic purposes. The case of Georgia demonstrated that cyber attacks could now become active contributors to an armed conflict through information warfare but could not be defined as armed attacks, which would in turn provide the legal ground for NATO's ability to respond with the use of force as a defensive response to a cyber attack on a member state.

Lessons Learned for NATO: Finding A Place for Cyber in Interstate Warfare

The case of Georgia set a dangerous precedent: even though the cyber attacks could not be attributed to the state, Russia was able to benefit from the cyber attacks as Georgia's information and communications infrastructure were compromised during a state of war[90]. The cyber attacks weakened Georgia on a psychological level: the lack of communication and function of the government in times of crisis is a strategic play against the relationship of trust between the

[89] North Atlantic Treaty Organization. *The North Atlantic Treaty* (Washington D.C.: North Atlantic Treaty Organization, 1949), 1-2.
[90] Jeffrey Carr, "Project Grey Goose Phase I Report," *Project Grey Goose* (2008), 3.

Georgian government and its people. Not being able to communicate with the governmental bodies that are supposed to keep you safe can cause fear, panic and disappointment in the Georgian population, as well as weaken the government's ability to warn and inform the public of its progress in the war[91]. Once more Russia's turn towards information campaigns as part of its warfare strategy is directly linked to its cyber capabilities: being able to penetrate the digital infrastructures of Eastern European neighbours, hackers from Russia and other parts of the world have an active role in a war between two nations, with Russia benefiting from the result. Perhaps more daunting than in the case of Estonia is the implication of civilian participation and power in cyberspace: whether the cyber attacks were state-sanctioned or not, Russia tolerates them because it can claim plausible deniability and still reap the fruits of the hackers' labour.

Georgia did not need to be a NATO member to alert the organisation to new threats from cyberspace. Russia's tensions with its Eastern European neighbours had found a new expression in a short war that displaced thousands of Georgians. NATO recognised the dangers implied in the Georgian case and devoted more space to cyber defence in the Strategic Concept, presented at the Lisbon Summit in 2010, stressing the importance of "…bringing all NATO bodies under centralized cyber protection"[92]. However, it wasn't until the Russian annexation of Ukrainian Crimea that the implications of information campaigns and cyber attacks found their way into a new theoretical concept used by NATO: Hybrid Warfare.

2.3. Cyber Attacks against Ukraine during Russia's annexation of Crimea and Sevastopol

Historical Context

In November 2013, Ukrainian President Viktor Yanukovych declared to the public that he would not sign an association agreement with the European Union (EU), an agreement the Ukrainian government had been working towards for several years of negotiations with the EU.

[91] Eneken Tikk et al. "Cyber attacks against Georgia: Legal lessons identified," *NATO Cooperative Cyber Defence Centre of Excellence, Tallinn*, (2008): 16.
[92] North Atlantic Treaty Organization. *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization Adopted by Heads of State and Government at the NATO Summit in Lisbon 19-20 November 2010* (Brussels: North Atlantic Treaty Organization, 2010), 16-17.

Instead, Yanukovych sought closer economic and political ties with Russia, which came with the offer of a lucrative loan of 1.5 billion dollars from its Eastern neighbour[93]. On November 21, 2013, protests filled the streets of Kiev as protesters were angered by the President's sudden turn towards Russia and his abandonment of the Ukrainian-European Union Association Agreement. The protests and upheavals that followed in Ukraine would last until late February, 2014 and would be known as Euromaidan. Over these months, protesters demanding the renegotiation of the association agreement with the European Union were met by police forces and anti-Euromaidan counter-protests across Ukraine[94]. The violent confrontations between pro-European protesters and the police led to President Yanukovych fleeing Kiev on February 22[95]. Six days later, unmarked forces that Vladimir Putin would later admit to be Russian military, marched into Sevastopol in the southwestern region of the Crimean peninsula and took control over a military airfield and the International Airport[96]. More Russian troops entered Crimea on March 2, which constituted an invasion of Ukraine's sovereign territory.

To legitimise Russia's actions in Ukraine, Crimea and Sevastopol held a referendum on March 16, asking its citizens to vote whether or not Crimea should become a federal subject of Russia. 96.77% of the citizens of Crimea voted in favour of becoming a federal subject of the Russian Federation[97]. This decision prompted Russia to justify its actions by claiming to protect its citizens abroad and pointed to their right to self-determination, the same argument that was made by the Russian Federation when its forces marched into Georgian territory in 2008[98]. A further argument made by Russia was that the Crimean constitution of 1992, which states that Crimea falls under the territorial sovereignty of Ukraine, is void[99]. Crimea had been ceded to Russia under Catherine the Great in 1792 and the Union of Soviet Socialist Republics (USSR) had transferred the Crimean region to the Ukrainian Soviet Socialist Republic in 1954. After Ukraine claimed independence from the Soviet Union on 24 August 1991, Crimea remained a

[93] John Biersack, and Shannon O'lear, "The geopolitics of Russia's annexation of Crimea: narratives, identity, silences, and energy," *Eurasian Geography and Economics* 55.3 (to 2014): 248.
[94] Ibid, 248.
[95] Ibid, 248.
[96] Tim Maurer, "Cyber Proxies and the Crisis in Ukraine," in *Cyber War in Perspective: Russian Aggression against Ukraine*, ed. Kenneth Geers (Tallinn: NATO CCD COE Publications, 2015), 80.
[97] Thomas D. Grant, "Annexation of Crimea," *American Journal of International Law* 109.1 (2015): 69.
[98] Roy Allison, "Russian 'deniable' intervention in Ukraine: how and why Russia broke the rules," *International Affairs* 90.6 (2014): 1266.
[99] Ibid.

region of Ukraine, albeit with a large part of the population that considered Russian its first language[100]. The Russian Federation called the legality of the 1954 transfer of Crimea to the Ukrainian Socialist Republic into question, thus claiming that Crimea was legally still a part of Russia[101].

A treaty between the self-proclaimed Republic of Crimea and the Russian Federation was signed on March 18, formally starting the accession process. A day later Ukrainian forces were forced out of the contested regions by Crimean separatists and Russian forces. Despite the several discourses of legitimisation Russia is employing to justify the annexation of Crimea, neither Ukraine nor the international community have accepted Crimea and Sevastopol's de facto independence from Crimea. The annexation of Crimea was met by the international community with protest, economic sanctions imposed on Russia and the termination of its membership in the Group of Eight (G8).[102] However, to this day Crimea remains de facto independent from Ukraine and Russia maintains its presence in the region.

Cyber attacks against Ukraine: Disrupting the Communication Systems between Ukraine and the region of Crimea

Russia's invasion into Ukrainian territory was accompanied by the types of cyber attacks that the international community had already observed in the cases of Estonia and Georgia. Alongside DDoS and defacement of website attacks on the website of the Ukrainian government and others, hackers infected the computers of the Ukrainian Prime Minister's office and several embassies in Ukraine with a malicious computer worm called Snake and hacked the cell phones of several Ukrainian officials and politicians[103]. Parallel to the confrontations between the armed forces of Russia and Ukraine in Crimea, an exchange of attacks took place in cyberspace.

[100] State Statistics Committee of Ukraine. "About number and composition population of AUTONOMOUS REPUBLIC OF CRIMEA by All-Ukrainian population census' 2001 data (2003-2004)," [2003-2004 Electronic Resource], http://2001.ukrcensus.gov.ua/eng/results/general/language/Crimea/, accessed on Aug. 20, 2017.
[101] Roy Allison, "Russian 'deniable' intervention in Ukraine: how and why Russia broke the rules," *International Affairs* 90.6 (2014): 1286.
[102] John Biersack, and Shannon O'lear, "The geopolitics of Russia's annexation of Crimea: narratives, identity, silences, and energy," *Eurasian Geography and Economics* 55.3 (to 2014): 251.
[103] Tim Maurer, "Cyber Proxies and the Crisis in Ukraine," in *Cyber War in Perspective: Russian Aggression against Ukraine*, ed. Kenneth Geers (Tallinn: NATO CCD COE Publications, 2015), 80.

However, in the case of Ukraine another element of cyber warfare became visible: the Ukrainian Telecommunications Company Ukrtelecom reported that a fibre-optic cable belonging to the company had been damaged by unknown individuals[104]. According to the company, the damage to the fibre-optic cable had endangered the communication services provided by Ukrtelecom. Fibre-optic cables are one of the more physical targets of cyber attacks that can cause the Internet in certain regions to collapse if the right fibre-optic cables are destroyed. Tampering with these cables blurs the line between cyber attacks and armed attacks in the physical world, begging the question of how to classify them. If anything, the report alerted observers to the possibility of achieving considerable disruptions or even the complete loss of services provided in cyberspace through an attack on land and sea, as well as through the air, such as missile or drone attacks targeting these fibre-optic cables.

The cyber attacks against Ukraine were met by resistance in cyberspace in the form of Ukrainian hacker groups, such as the Ukrainian Cyber Force. The hacker group is led by Eugene Dokukin, which reportedly threatened to shut down Crimea's internet access during the conflict and has routinely leaked sensitive data from the Russian Ministry of Interior[105]. The Ukrainian government itself attempted to defend against the incoming cyber attacks through official channels, but several experts have pointed out that the country's cyber power is predominantly found in Ukraine's private sector[106].

Aftermath: Effects, investigations and responses

While Ukraine enjoys many ties with Western Europe, it is not a member of NATO. However, the heart of the conflict between the Euromaidan protesters, the Ukrainian government and the Crimean separatists was essentially a conflict between a part of the population favouring closer economic and political ties with Europe and a part of the population looking to Russia for assistance and cooperation. NATO's operations in Eastern Europe are also a part of this ideological divide: NATO set up a Cyber Defence Trust Fund to increase Ukraine's cyber defence capabilities post-conflict. Therefore, even though Ukraine does not fall under the

[104] Ibid, 81.
[105] Ibid, 82.
[106] Ibid, 82.

purview of Article 5 of the North Atlantic Treaty, NATO has a vested interest in providing Ukraine with cyber-related assistance because of the country's strategic and political situation in relation to Russia. Once more we see that NATO's cyber defence is closely related to its existing interests in its Eastern area of influence.

As was the case in Estonia and Georgia, the Russian government claimed plausible deniability when it was accused of involvement in the cyber attacks on Ukraine. Firmly embedded in its information campaigns, cyber attacks were launched by Russian nationalists and sympathisers who had no discernible links to the Kremlin[107]. The same element of uncertainty that Russia had used in its grey area discourse of legitimising the annexation of Crimea, was once again seen in its tolerance of anti-Ukrainian cyber attacks, which showed similar patterns of coordination and planning as the cyber attacks against Georgia in 2008. The effect of the cyber attacks on Ukraine were not merely the disruption of communications and information services, which might explain why they once again refrained from causing catastrophic damage. Russia's information campaign benefits from cyber attacks less because of their direct consequences to computers and digital infrastructures but because they are an important contribution to the dissemination of information that creates uncertainty and confusion, pushing pro-Russian narratives and manipulating the perception of the public in Ukraine and the world. As Maria Snegovaya from Columbia University points out in a report of Russia's warfare tactics in Ukraine:

"The goal, […], is to weaken the West, create divisions between NATO member states, and to undermine the U.S. in the eyes of the world, especially the developing world[108]."

The destructive potential of cyber attacks has been subject to many debates surrounding the potential of cyber war. Provided that hackers have the cyber capability to shut down the Internet, hack into websites crucial to the digital infrastructure of countries, from traffic lights, to hospitals and banks to nuclear weapons facilities, why do they often limit their cyber attacks to the defacement of websites and malicious software? The attacks on Estonia, Georgia and Ukraine

[107] Maria Snegovaya, "Russia Report I: Putin's information warfare in Ukraine. Soviet Origins of Russia's Hybrid Warfare," *Institute for the Study of War* (2015): 16.
[108] Ibid, 14.

indicate that private groups, state-sponsored or not, do have the know-how and the technology to hack into banks to disable ATMs or bring down essential websites. The cyber technology is out there; and yet the primary aim of the cyber attacks on Estonia, Georgia and Ukraine was to disrupt communication systems on one hand and to disseminate information on the other.

Why, then, did the cyber attacks on these three Eastern European countries remain at relatively low to mid levels of disruptive force? According to Maria Snegovaya, cyber attacks are a part of Information Warfare, a way to influence civil society and create strife amongst NATO allies[109]. Cyber attacks are distinguished from nuclear weapons and other conventional military operations by the high level of civilian involvement, as private hacker groups, companies and other non-state actors are the perpetrators and victims of cyber attacks during an interstate conflict. The case of Ukraine shows once more that cyberspace complicates the traditional hierarchies of power in international relations, giving civil society a much more crucial role than in conventional conflicts. The opinion of the masses is therefore crucial to the information campaign of Russia, as it encourages the participation of hacker groups and individuals wishing to express their ideological and political opinions in the form of cyber attacks[110]. Whether or not the Russian government directly coordinated the attacks or not is irrelevant to this aspect of information war, as it still achieves the same effect: influencing the perception of target groups through information campaigns that serve the purposes of the Russian federation.

Lessons Learned for NATO: The Hybrid Warfare Theory

Russia's annexation of Crimea received much more attention from the international community and the Western media than the war against Georgia in 2008. While the cyber component was only one of many aspects of the invasion that captivated policy-makers and the public about the Ukrainian conflict, as the ideological divide between pro-European and pro-Russian discourses took centre stage, the combination of cyber attacks, information campaigns and military force legitimised by an identity discourse prompted NATO to find a new term to

[109] Ibid, 7.
[110] Ibid, 7.

explain Russia's recent actions in Eastern Europe: *Hybrid Warfare* would become a new attempt for NATO to understand how to counter the cyber threat in combination with Russia's other warfare tactics[111]. Along with Deterrence, information warfare, legal discourses surrounding the applicability of Article 5, and the centralisation of a more coordinated defence of the digital infrastructures of member states, NATO has answered the challenges posed by the cases of Estonia in 2007, Georgia in 2008 and Ukraine in 2014 by developing a comprehensive security and defence dispositive, in which its relations with Russia are as central as the cyber component. In the next section I will analyse the main discourses and practices arising out of NATO's lessons learned in its Eastern area of influence and determine what the implication of its current cyber policy has for the future of cyber warfare and interstate conflict.

PART 3: ANALYSING NATO's PRACTICES AND DISCOURSES ABOUT THE FUTURE OF CYBER WAR

The cyber attacks against Estonia caused a fundamental change in NATO's approach to cyber defence from the protection of its internal information and communication systems to the first development of a Policy on Cyber Defence in 2008. The Policy "emphasises the need for NATO and nations to protect key information systems in accordance with their respective responsibilities; share best practices; *and provide a capability to assist Allied nations, upon request, to counter a cyber attack"*[112]. The Alliance recognised the need for a more coordinated and sophisticated response rate in the event of a cyber attack on a member state. Existing discourses on the application of Article 5 in the event of a cyber attack were amplified, as Estonia had refrained from invoking Article 5 because it didn't consider them to constitute an armed attack. In the context of Georgia in 2008 and Ukraine in 2014, the question was not whether NATO had to step in according to Article 5 because neither countries were member states. The challenge for NATO lay in a fundamental question for future operations: How should NATO operate in the event of an armed conflict involving the cyber domain and asymmetric warfare tactics?

[111] Keir Giles, "Russia's 'New' Tools for Confronting the West Continuity and Innovation in Moscow's Exercise of Power," *Russia and Eurasia, Programme, London: Chatham House* (2016): 6.
[112] North Atlantic Treaty Organization. *Bucharest Summit Declaration* (Brussels: North Atlantic Treaty Organization, 2008), 11.

3.1. The Legal Layer: Establishing military operations without existing legal standards of cyber warfare

There are a few approaches to the categorisation of cyber attacks as armed attacks: some experts claim that the intent of a cyber attack should determine whether or not it is considered to constitute "use of force", which under the U.N. Charter would be the equivalent of an armed attack[113]. Others favour the approach of letting the impact of a cyber attack decide its legal category, distinguishing between the disruption of essential information and communication services necessary for a government to function and the hacking of a website, for example[114]. However, no consensus exists on whether or not cyber attacks constitute armed attacks, whether they cause physical harm indirectly or whether certain disruptive cyber attacks could be described as an act of war directed against a state and its population. Article 5 of the North Atlantic Treaty cannot be called into effect if the legal framework doesn't classify any type of cyber attack as an armed attack. However, adding to the legal debate over the use of force in the cyber domain, the difficulty of tracing cyber attacks to the responsible actors presents another obstacle to the application of Article 5:

The investigations after the cyber attacks on Estonia, Georgia and Ukraine showed that attribution was a major obstacle to the application of international law to cyber threats: in neither case could the cyber attacks be traced back to the Russian government, making the laws of interstate conflict difficult to apply without a state that could be held accountable for the actions of civilian hackers, even when some of them had Russian IP addresses[115]. Russia has categorically denied any involvement in the cyber attacks against Estonia, Georgia and Ukraine. If civilian actors were responsible for the attacks and a state cannot be held accountable under international law, NATO faces the difficulty of not knowing how to respond. Should the cyber component continue to be used in future interstate conflicts and war, identifying the responsible actors will be essential for NATO and its member states. Until then, the Russian government and

[113] Wolfgang McGavran, "Intended consequences: regulating cyber attacks," *Tul. J. Tech. & Intell. Prop.* 12 (2009): 261.
[114] Ibid, 261.
[115] Jeffrey Carr, "Project Grey Goose Phase I Report," *Project Grey Goose* (2008), 3-4.

other state actors continue to benefit from cyber attacks disseminating pro-Russian information and disrupting the digital infrastructure of other nations, without the fear of being held accountable for them[116].

Cyber attacks are being used in the context of armed conflict, as was the case during the Russo-Georgian War in August 2008, and during the invasion of Crimea in 2014. The legal challenge continues to be the incorporation of cyber attacks into the existing legal paradigm, a process that is impeded by the problem of attribution and the hesitation to give cyber attacks the status of armed attacks. Without clear legal standards regulating cyber activity in interstate conflict, future warfare could include the unchecked use of cyber attacks in this current legal grey zone.

NATO declared in its Wales Summit Communiqué in 2014 that International Law would apply in cyberspace[117]. It classified cyber threats as "non-conventional" and decreed that the invocation of Article 5 in the event of a cyber attack would be decided on a case-by-case basis. However, neither the issues of attribution and accountability, nor a clear-cut decision on whether cyber attacks constitute an armed attack are solved by this decision. Deciding on the application of Article 5 on a case-by-case basis provides the organisation with enough flexibility to make ad hoc decisions based on the severity of the case. As previously mentioned, the Tallinn Manual comes closest to establishing legal standards for cyber attacks: compiled by an international group of experts in 2013, the Manual is a non-binding legal guide for the application of international law to cyber warfare. The Manual recommended that "A cyber operation by a State directed against cyber infrastructure located in another State may violate the latter's sovereignty. It certainly does so if it causes damage"[118]. What the experts could not agree on, however, was "whether the placement of malware that causes no physical damage (as with malware used to monitor activities) constitutes a violation of sovereignty"[119]. So-called coercive cyber operations directed against governments are to be categorised as illegal "intervention" or a prohibited "use

[116] Ibid, 3.
[117] North Atlantic Treaty Organization. *Warsaw Summit Communiqué* (Brussels: North Atlantic Treaty Organization, 2016), 16.
[118] Michael N. Schmitt and Vihul, Liis, "The Nature of International Law Cyber Norms," *NATO Cooperative Cyber Defence Centre of Excellence, Tallinn Paper 5* (2014): 16.
[119] Ibid, 16.

of force", while a cyber operation considered an armed attack would trigger the right to self-defence, individual or collective[120]. Under the United Nations Charter, a cyber attack that causes physical damage might indeed qualify as an armed attack, supporting the guidelines of the Tallinn Manual[121]. However, the North Atlantic Council is the authority in NATO's command structure that decides whether an attack on a member state considers an armed attack[122]. Furthermore, in the North Atlantic Treaty, an armed attack is merely described as an armed attack on the territory and forces of Parties to the treaty, including vessels[123]. Without a clear classification of cyber attacks, the question of when a cyber attack triggers Article 5 has not been solved by NATO.

One important implication for the future of cyber warfare is that in order to constitute an armed attack, certain cyber attacks must be qualified as weapons. Realistically, the majority of cyber attacks do not cause physical damage directly but might nonetheless have disastrous economic, social and individual consequences for individuals, not excluding the loss of life. If the North Atlantic Council has the authority to decide what constitutes an armed attack, what will be the standards by which cyber attacks will be categorised? Will it be the intent of the cyber attack or the actual damage it has caused? The reason why not all cyber attacks are declared armed attacks is because there are many actors, state and non-state, individual and collective, that make use of their cyber capabilities in their military operations or for private gain. One NATO member, the United States, for example, reportedly developed the Stuxnet worm, a malicious botnet designed to sabotage Iran's Nuclear Programme[124]. Classifying cyber attacks as weapons would limit the possibilities of state actors to expand their cyber capabilities for a number of uses. The use of cyber capabilities by NATO members and potential enemies is complicating a definite incorporation of cyber attacks into established rules and norms. In this case, NATO has been given a lot of flexibility by declaring cyberspace as a domain of military operations without a clear legal framework for the future of cyber war. What will the collective response to an armed attack under Article 5 look like? Will it include kinetic and cyber attacks or

[120] Ibid, 17.
[121] Stephen W. Korns and Joshua E. Kastenberg, "Georgia's cyber left hook," *Parameters* 38.4 (2008): 63.
[122] David P. Fidler, Richard Pregent, and Alex Vandurme, "NATO, Cyber Defense, and International Law," *Journal of International and Comparative Law* 4.1 (2016): 7.
[123] North Atlantic Treaty Organization. *The North Atlantic Treaty* (Washington D.C.: North Atlantic Treaty Organization, 1949), 2.
[124] Jon R. Lindsay, "Stuxnet and the limits of cyber warfare," *Security Studies* 22.3 (2013): 366.

only one of the two? How much state involvement will be considered evidence of attribution and thus accountability for cyber attacks in the future?

None of these questions have been answered by NATO, but the legal discourse continues. The CCD COE has published several long reports on the legal challenges exposed to the organisation by the events in Estonia and Georgia. More recently, NATO has declared in its Cyber Defence Pledge of July 8, 2016 that it will continue to integrate cyber defence into its existing operations[125]. Despite the organisation's hard work on the legal challenges from cyberspace, its premature decision to apply international law to a space that doesn't allow for attribution or a clear definition of an armed attack means that the next cyber attack on a NATO member state could trigger an interstate conflict without the necessary legal framework to ensure that the organisation's actions are in line with the international norms and rules it adheres to.

3.2. The Technical Layer: Centralised Coordination and Sharing of Best Practices - Presenting Technical Solutions to a Political Problem

Besides the focus on legal challenges, the literature on NATO's cyber defence has thematised the improvement of the organisation's technical and operational capabilities. NATO defines 'cyber defence' as "the ability to safeguard the delivery and management of services in an operational CIS (Communication and Information Systems) in response to potential and imminent as well as actual malicious actions that originate in cyberspace[126]." Before 2007, NATO's cyber defence was limited to the strengthening and protection of its internal digital infrastructure while member states were tasked with the security of their own information and communications systems[127]. However, since the cyber attacks on Estonia, experts have suggested a more coordinated and centralised approach to cyber defence, addressing "operational needs for

[125] North Atlantic Treaty Organization. *Cyber Defence Pledge* (Brussels: North Atlantic Treaty Organization, 2016).
[126] Alexander Klimburg (Ed.), "National Cyber Security Framework Manual," *NATO CCD COE Publications, Tallinn* (2012): 13. (brackets added by me)
[127] Vincent Joubert, "Five Years After Estonia's Cyber Attacks: Lessons Learned for NATO?," *NATO Defense College, Research Division* (2012): 4.

speed, secrecy, and mobility with risk management, data security, and information sharing—all tasks that characterize effective cybersecurity[128]".

Locked Shields is a training exercise organised by NATO CCD COE since 2010 and is meant to train these operational characteristics, in which NATO member states and Allies compete to determine how advanced the cyber capabilities of participating nations are[129]. The yearly exercise is meant to share best practices and identify existing weaknesses in the cyber defence capabilities of all members. Furthermore, NATO's Allies, academia, international organisations and the private sector are forming a growing network to address the fast-evolving cyber threats as they appear on the international arena. Experts focusing on the technical dimension of NATO's cyber defence suggest a faster response rate, a better command structure and the avoidance of duplication through information sharing in a more coordinated and centralised cyber defence of critical communication infrastructure[130].

NATO CCD COE published a Framework Manual for National Cyber Security in 2012, in which five cyber security dilemmas are identified for member states:

1) Stimulate the Economy vs. Improve National Security Infrastructure
2) Modernisation vs. Critical Infrastructure Protection
3) Private Sector vs. Public Sector
4) Data Protection vs. Information Sharing
5) Freedom of Expression vs. Political Stability[131]

These five considerations reflect NATO's effort to balance the technical and operational changes to Cyber Defence with the political and strategical consequences of implementing these

[128] David P. Fidler, Richard Pregent, and Alex Vandurme, "NATO, Cyber Defense, and International Law," *Journal of International and Comparative Law* 4.1 (2016): 8.
[129] NATO Cooperative Cyber Defence Centre of Excellence. "*Events: Cyber Defence Exercises/Locked Shields 2017,"* https://ccdcoe.org/locked-shields-2017.html, accessed on Aug. 18, 2017.
[130] Hannes Krause, "NATO on Its Way Towards a Comfort Zone in Cyber Defence," *NATO Cooperative Cyber Defence Centre of Excellence, Tallinn Paper 3* (2014): 6.
David P. Fidler, Richard Pregent, and Alex Vandurme, "NATO, Cyber Defense, and International Law," *Journal of International and Comparative Law* 4.1 (2016): 18.
[131] Alexander Klimburg (Ed.), "National Cyber Security Framework Manual," *NATO CCD COE Publications, Tallinn* (2012): 34-42.

changes. NATO's move towards a more centralised cyber defence system means that national cyber security approaches will be increasingly integrated with each other, creating cyber practices that will be very similar across the Alliance. Such a coordinated approach to cyber security will enable NATO to exercise better command over national cyber policies of member states in the future. However, the attempt to solve all five cyber security dilemmas equally for all 29 member states will prove difficult. Not only do the different national security frameworks have diverging logics and priorities, the rules and norms governing the relationship between governments and their civilian population varies as well[132]. The five cyber security dilemmas listed in the Framework Manual for National Cyber Security pose some crucial questions for the Alliance to consider in its cyber defence approach. The Alliance is moving towards a system of information sharing and close cooperation with the private sector through its NATO Industry Cyber Partnership[133].

The more NATO centralises these practices in its member states' cyber security frameworks, the more alternative cyber security practices and discourses will fade into the background. In their Cyber Defence Pledge of 2016, the Allies write: "We will ensure that strong and resilient cyber defences enable the Alliance to fulfil its core tasks. Our interconnectedness means that we are only as strong as our weakest link. We will work together to better protect our networks and thereby contribute to the success of Allied operations"[134]. While the Alliance's member states might enjoy a more robust cyber defence in the technical sense through a centralised coordination of cyber operations and the sharing of best practices with industry, this approach underplays the unique structure of cyber as a decentralised space[135]. In cyberspace, power and capability lie with several actors that NATO will depend on to share best practices in the field of cyber security. The fundamental tension between the protection of national digital infrastructure and the sharing of best practices has not been discussed in enough detail by the Alliance. In the future, the political implications of an over-reliance on technical solutions will expose these tensions. The role of Industry, civil society and individuals in the development of a nation's cyber capabilities means that cyberspace is not merely a domain of operations for NATO, but a

[132] Ibid, 35.
[133] North Atlantic Treaty Organization. *Cyber Defence Pledge* (Brussels: North Atlantic Treaty Organization, 2016).
[134] Ibid.
[135] Nazli Choucri, "Emerging Trends in Cyberspace: Dimensions & Dilemmas," *Williams and Fiddner, Cyberspace: Malevolent Actors, Criminal Opportunities, and Strategic Competition* (2012): 3-4.

platform shared with the civilians it seeks to protect. The technical and operational dimensions are essential to an effective cyber defence policy for NATO. However, cyberspace's technical challenges to national defence and security considerations are only one aspect of a collective cyber strategy. Preparing for future cyber attacks might necessitate good technical and operational strategies to protect software and hardware, but the political aspects of NATO's strategy in cyberspace are crucial for an effective cyber security. Current literature on the prospects of Cyber War and how NATO can prepare for all eventualities is embedded in three different discourses: nuclear warfare, information warfare and hybrid warfare.

3.3. The Political and Strategical Layers: Nuclear Warfare, Information Warfare, Hybrid Warfare…Cyber Warfare?

There is much speculation about the future of cyber warfare: some authors like Thomas Rid argue that cyber war is unlikely to take place because cyber attacks are versions of existing warfare activities, namely subversion, espionage and sabotage[136]. In his view, cases of cyber attacks that have materialised in the past have not constituted an armed attack in themselves and, as Rid predicts, won't qualify as such in the future. However, other authors posit that cyber war is no longer an outrageous or inflammatory term: John Arquilla and David Ronfeldt from the RAND cooperation tie cyber war to the emergence of a so-called Information Age, in which information and the capabilities to disrupt the enemy's communication network will not only shape but transform future of warfare[137]. Adam Liff and Timothy J. Junio each point out that theorising about an event that has not occurred requires a strong theoretical framework to define what constitutes cyber warfare and why it is (im)probable that it will happen[138]. It is not only important to study whether or not a cyber war is probable. Understanding how NATO conceptualises the probabilities of a cyber war occurring in the future reveals which underlying security practices and norms will be produced by NATO in response to the future its experts

[136] Thomas Rid, "Cyber war will not take place," *Journal of strategic studies* 35.1 (2012): 6.
[137] John Arquilla, and David Ronfeldt. "Cyberwar is coming!," *Comparative Strategy* 12.2 (1993): 142.
[138] -Timothy J Junio, "How probable is cyber war? Bringing IR theory back in to the cyber conflict debate," *Journal of Strategic Studies* 36.1 (2013): 126.
-Adam P. Liff, "Cyberwar: a new 'absolute weapon'? The proliferation of cyberwarfare capabilities and interstate war," *Journal of Strategic Studies* 35.3 (2012): 403.

predict. The three main theories circulating about cyber defence and its role in interstate conflict and war are Deterrence, Information Warfare and Hybrid Warfare.

Defence and Deterrence: Why Cyber Attacks are not like Nuclear Weapons

Deterrence against security threats is one of NATO's founding principles[139]. Experts and policy makers have drawn the analogy between nuclear weapons and cyber attacks, arguing that the destructive potential of cyber attacks are comparable to the catastrophic consequences of nuclear warfare[140]. To continue the analogy, some experts assume that the same formula of deterrence and proliferation applies in cyberspace: as rational actors, states will refrain from using cyber threats that might cause the collapse of entire economies or digital infrastructures because they fear retaliation of the same kind. This formula was applied to predict that nuclear warfare is not of advantage to the actor holding nuclear weapons[141]. It is also being applied to the possibility of cyber warfare, as many actors argue that deterring against cyber attacks will follow the same logic as it did in nuclear deterrence theories[142]. However, some authors point out that deterring an enemy from using destructive weapons technology for fear of the opponent's retaliatory ability works differently in cyberspace[143]. Once again the issue of attributing cyber attacks to certain actors comes into play: a cyber attack may be launched by a national government or insurgent group confident enough that its traces can be erased. Furthermore, as opposed to nuclear technology, cyber technology is decentralised and dispersed over a vast virtual space and held by many actors besides state actors traditionally holding the decision-making capabilities to launch a nuclear attack[144]. According to this argument an individual hacker with the right skills and equipment can do as much damage as a government and any

[139] David S. Yost, "NATO's evolving purposes and the next Strategic Concept," *International affairs* 86.2 (2010): 491.
[140] Jon R. Lindsay, "Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack," *Journal of Cybersecurity* 1.1 (2015): 63. Note: Lindsay quotes a comment by U.S. President Barack Obama, which can be found at: Barack H. Obama, "Remarks by the President to the Business Roundtable." *The White House* (2015), https://www.whitehouse.gov/the-press-ofce/(2015)/09/16/remarks-president-business-roundtable, accessed on Aug. 8, 2017.
[141] Klimburg, *The Darkening Web. The War for Cyberspace,* 5-7.
[142] Ibid, 5-7.
[143] Jon R. Lindsay, "Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack," 63.
[144] Christian Malis, "Unconventional Forms of War," (In *The Oxford Handbook of War,* 185-198. Edited by Julian Lindley-French and Yves Boyen. Oxford: Oxford University Press, 2012), 194.

links to a state actor can be hidden from subsequent investigations, as was the case in Estonia, Georgia and Ukraine. Deterrence theory is a consistent aspect of NATO's cyber policy, despite these theoretical challenges to its effectiveness in cyberspace.

In its Strategic Concept of 2010, NATO devoted a section of its strategy to Defence and Deterrence, pledging to "develop further our ability to prevent, detect, defend against and recover from cyberattacks, including by using the NATO planning process to enhance and coordinate national cyber-defence capabilities, bringing all NATO bodies under centralized cyber protection"[145]. NATO's first deterrence capability begins with Article 5 of the North Atlantic Treaty of 1949, stipulating that an attack against one member of the alliance is an attack against al members, which is also the premise for the organisation's core premise of enabling cooperative security through collective defence in the case of an armed attack[146]. The deterrent factor of Article 5 lies in the consequences of such an attack on a member state, which posits that the Alliance will intervene on behalf of a member state in case of armed attack[147]". Hostile actors considering an armed attack against a NATO member state must therefore calculate the possibility of an armed defensive response by the Alliance.

James A. Lewis published the eighth Tallinn Paper for NATO's CCD COE in 2015 titled 'The Role of Offensive Cyber Operations in NATO's Collective Defence'. In it he argues that in order to meet the advanced military capabilities of hostile nations like Russia, who have developed offensive cyber strategies, NATO has to "publicly embrace offensive cyber capabilities in planning and exercises"[148]. Lewis posits that an offensive cyber doctrine is essential for NATO to be able to deter and defend against cyber attacks in the future. In this line of reasoning, Russia's cyber capabilities and more importantly its information warfare tactics to use propaganda and gather intelligence through cyber means present a danger to NATO that

[145] North Atlantic Treaty Organization. *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization Adopted by Heads of State and Government at the NATO Summit in Lisbon 19-20 November 2010* (Brussels: North Atlantic Treaty Organization, 2010), 16-17.
[146] David P. Fidler, Richard Pregent, and Alex Vandurme, "NATO, Cyber Defense, and International Law," *Journal of International and Comparative Law* 4.1 (2016): 2.
[147] North Atlantic Treaty Organization. *The North Atlantic Treaty* (Washington D.C.: North Atlantic Treaty Organization, 1949), 1.
[148] James A. Lewis, "The Role of Offensive Cyber Operations In NATO's Collective Defence," *NATO Cooperative Cyber Defence Centre of Excellence, Tallinn Paper 8* (2015): 12.

cannot be met with a purely defensive cyber strategy. Lewis is not alone in his analysis of NATO's cyber defence policy: since the cyber attacks on Estonia and Georgia prompted NATO's policy makers, consultants and academia to consider the possibility of a future including cyber conflict and war more seriously, another discourse started to emerge: Cyber attacks were not only inevitable aspects of the future of interstate conflict, they could also become offensive capabilities for NATO and its members[149].

NATO's Cyber security isn't confined to the defence against cyber attacks that have already taken place, but it includes the development of a strategy to defend against, deter and counter cyber threats if necessary. In order to create an effective cyber security strategy, NATO must develop defensive capabilities to protect its network and coordinate the protection of the digital infrastructures of member states, as well as offensive capabilities to prepare for a number of scenarios in the future that include the use of cyber capabilities in interstate conflict and war[150]. In other words, in order to uphold its mandate of collective defence, its cyber capabilities must match the offensive capabilities of other actors.

NATO's current cyber defence policy focuses on its ability to withstand cyber attacks through enhanced cyber capabilities protecting the digital infrastructures of member states, a strategy described as 'resilience', and its ability to deter hostile actors from launching cyber attacks in the first place[151]. The nuclear arms race caused deterrence to become a fundamental strategy for NATO member states, most importantly the U.S., to avoid a nuclear war[152]. In the cyber domain, deterrence by denial ensures that a breach of defences is made technically difficult because NATO's internal information and communications networks and those of its members are robust enough to withstand a cyber attack[153]. Before the attacks on Estonia in 2007, deterrence by denial, denying the attacker's objective to launch a successful cyber attack, was the

[149] David P. Fidler, Richard Pregent, and Alex Vandurme, "NATO, Cyber Defense, and International Law," *Journal of International and Comparative Law* 4.1 (2016): 12.
[150] Ibid, 12.
[151] North Atlantic Treaty Organization. *Warsaw Summit Communiqué* (Brussels: North Atlantic Treaty Organization, 2016), 16.
[152] Vincent Joubert, "Five Years After Estonia's Cyber Attacks: Lessons Learned for NATO?," *NATO Defense College, Research Division* (2012): 3.
[153] Ibid, 3.

fundamental aspect of NATO's cyber defence strategy[154]. However, the Estonian case revealed once more that the national infrastructure and defence mechanisms of a member state could be penetrated by a cyber attack without being detected in time. While the attacks on Estonia did not present the first case of a cyber attack, the specific political context, Russia's tensions and conflicts with an Eastern European NATO member, as well as Estonia's reliance on e-services, demonstrated the digital infrastructure of NATO members was vulnerable to cyber attacks after all, with both technical and political implications for the Alliance.

In the Strategic Concept of 2010, NATO described cyber attacks as "becoming more frequent, more organised and more costly in the damage that they inflict, […]; they can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability[155]". With an increased awareness of the potential of cyber attacks to penetrate the cyber defences of member states, NATO has moved closer to an approach called deterrence by punishment[156], deterring actors from launching cyber attacks against NATO because they fear retaliation. This brings us back to the discussion of collective defence, which NATO has firmly embedded in its official cyber defence policy since it declared that it would decide whether or not a cyber attack could invoke Article 5 on a case-by-case basis.

Despite the legal concerns of this decision outlined above, invoking Article 5 in the case of a cyber attack would also have important consequences for deterrence, since potential cyber attacks could have retaliatory consequences if the North Atlantic Council decides that they constitute an armed attack. The threat of invoking Article 5 in cyberspace does serve as a deterrent factor for actors that are unsure whether or not they can successfully hide their traces after launching a cyber attack. However, there are no rules or procedures in place to regulate whether NATO can defend against cyber attacks with cyber or kinetic force. Should a state actor be found responsible for a cyber attack, would it be possible for NATO to attack the critical digital infrastructure of the opponent as a defensive mechanism? Or would it use kinetic force to

[154] Ibid, 3.
[155] North Atlantic Treaty Organization. *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization Adopted by Heads of State and Government at the NATO Summit in Lisbon 19-20 November 2010* (Brussels: North Atlantic Treaty Organization, 2010), 11.
[156] Vincent Joubert, "Five Years After Estonia's Cyber Attacks: Lessons Learned for NATO?," *NATO Defense College, Research Division* (2012): 3.

defend member states? “Use of force” is so ill-defined in the cyber realm that the line between defence and offensive is especially blurred. The potential danger of NATO’s cyber approach to deterrence by punishment doesn't lie in the effectiveness of the approach but in the consequences of increasing cyber capabilities to the point where defensive cyber operations could cause the same destructive damage on civilian populations of target states as an offensive cyber attack.

3.4. Information Warfare and Hybrid Warfare as the theories for modeling Cyber Warfare: Strengths and Weaknesses

As we have seen in the cases of Estonia, Georgia and Ukraine, cyber attacks include the disruption of an opponent’s information and communications structure and the gathering of information and knowledge about the opponent through cyber means. The emphasis on information in cyber war resonates with the literature that links information warfare with the emerging cyber threat. The term ‘information warfare’ is closely related to discussions about Russia’s modern warfare tactics, described by Maria Snegovaya as a tactic to obscure Russia’s goals through disinformation campaigns, confuse and influence the perception of onlookers and opponents through information in peace times as well as during an armed conflict[157]. Russia’s modern information war makes use of different platforms available, such as social media and cyber operations, to win wars of public opinion as well as on the ground. Combined with armed attacks, diplomatic relations and other more conventional means of warfare, Russia’s information war includes “deliberate disinformation campaign supported by actions of the intelligence organs designed to confuse the enemy and achieve strategic advantage at minimal cost[158]”.

Snegovaya views information war as a method of a more recent term to describe Russia’s warfare tactics in Ukraine in 2014, Hybrid Warfare.[159]The concept of hybridity in warfare was coined by political scientist Frank Hoffman, describing it as a “blend of the lethality of state

[157] Maria Snegovaya, "Russia Report I: Putin’s information warfare in Ukraine. Soviet Origins of Russia’s Hybrid Warfare,” *Institute for the Study of War* (2015): 9.
[158] Ibid, 9.
[159] Ibid, 9.

conflict with the fanatical and protracted fervor of irregular war"[160]. Hybrid warfare refers to the use of both conventional and so-called unconventional or irregular forces in combat, but the term is heavily contested, as there are many definitions for what constitutes irregular or asymmetric warfare[161]. Many authors like Keir Giles consider cyber attacks to be important aspects of Russia's disinformation campaigns[162]. The cyber element in Russia's confrontation with Estonia, Georgia and Ukraine was deeply embedded with the dissemination of pro-Russian and anti-Estonian, anti-Georgian or anti-Ukrainian propaganda and the manipulation of the opinion of the public watching the events in Eastern Europe.

In 2016, NATO declared in its Warsaw Summit Communiqué that it is working on developing quick responses to cyber attacks, "including in hybrid contexts[163]". The term hybrid warfare has become popular in academic literature in an effort to categorise changes in warfare tactics in the 21st Century. The term has also become embedded in NATO's strategical discourse describing Russian operations in Ukraine in 2014[164]. NATO has embedded cyber threats in the context of hybrid warfare tactics for two reasons: first, Russia's use of information warfare tactics combined with the cyber attacks by Russian nationalists and sympathisers in the Estonian, Georgian and Ukrainian cases required a theoretical framework for the organisation to analyse and respond to Russia's actions. The specific combination of armed forces on the ground in Georgia while the country's digital infrastructure came under attack forced NATO to find a pattern in the new way Russia seemed to be approaching conflicts in Eastern Europe. Secondly, the case of Ukraine in 2014 showed that a full invasion of Russian forces into Ukrainian sovereign territory of Crimea could be carried out with the support of 96.77% of the Crimean population, which had previously called for an annexation of Crimea by Russia in a referendum[165]. From an armed conflict in Georgia to a full-out invasion in Crimea, Russia made

[160] Frank G. Hoffman, *Conflict in the 21st century: The rise of hybrid wars*, (Arlington: Potomac Institute for Policy Studies, 2007), quoted by: Keir Giles, "Russia's 'New'Tools for Confronting the West Continuity and Innovation in Moscow's Exercise of Power," *Russia and Eurasia, Programme, London: Chatham House* (2016): 6.
[161] Keir Giles, "Russia's 'New'Tools for Confronting the West Continuity and Innovation in Moscow's Exercise of Power," *Russia and Eurasia, Programme, London: Chatham House* (2016): 7.
[162] Ibid, 44.
[163] Ibid, 15.
[164] Ibid, 6.
[165] Thomas D. Grant, "Annexation of Crimea," *American Journal of International Law* 109.1 (2015): 69.

use of cyber attacks, information campaigns on the ground and in social media and the Internet to influence the perception of the parties involved.

Conventional military power was no longer the only indicator of success - and NATO had to prepare for a new way of waging war[166]. Hybrid warfare was a term that not only described a new form of warfare and campaigns in the eyes of NATO, it represented the ambiguity of victory in asymmetric warfare. Success is no longer measured only in the number and strength of a military. Just as cyberspace is by nature a space shared by anyone with a computer, cyber war will be equally inclusive of non-state and civilian actors. The participation of civil society and the private sector starts with public opinion and ends with cyber attacks: hackers that do not necessarily have to be recruited by governments to support their cause in a conflict will be able to do so in cyberspace if they have the necessary skills. Russia's information campaigns are so difficult to measure in terms of winning or losing a war because a large portion of the cyber capabilities and decisions are not made by the government. They are made by individuals with their own private interests and ideologies, aligned with the state's interest through years of state activity in the field of propaganda, information and censorship of alternative discourses[167]. Cyber attacks are not merely another weapon; they are tools by which non-state actors can actively and quite easily participate in warfare, armed conflicts and disputes between states. NATO has not yet found a way to counteract this aspect of cyber warfare in its current cyber security framework. The lessons learned in Estonia, Georgia and Ukraine should have alerted NATO to consider the implications of cyberspace on the relationship between governments and civilians more, rather than focusing on a technical solution to cyber threats.

The psychological aspects of the cyber attacks on Estonia, Georgia and Ukraine are not limited to influencing the perception of civilians and governments involved in the conflicts. The damage to the target is not confined to the economic or bureaucratic spheres: when the communication between a government and civilians is under attack, for example when Georgia's official governmental and media platforms do not function during an armed conflict with Russia,

[166] Keir Giles, "Russia's 'New'Tools for Confronting the West Continuity and Innovation in Moscow's Exercise of Power," *Russia and Eurasia, Programme, London: Chatham House* (2016): 42.
[167] Maria Snegovaya, "Russia Report I: Putin's information warfare in Ukraine. Soviet Origins of Russia's Hybrid Warfare," *Institute for the Study of War* (2015).

there can be societal ramifications too. Let us not forget that the digital infrastructure of a nation includes information *and* communications technology, the disruption of which can compromise the relationship of trust between government and citizens [168]. Furthermore, individual psychological remnants of a cyber attack can include the fear of intrusion into one's privacy and freedom of speech.

The response time of the Estonian, Georgian or Ukrainian governments is also crucial to this trust relationship, as the first wave of cyber attacks surprised national defence mechanisms. More importantly, NATO's ability to respond in time to defend member states against cyber attacks has been subject to doubt by experts of the Russian conflict with its Eastern European neighbours [169]. NATO has met the technical challenge of cyber attacks with a number of extensive exercises, such as Locked Shields, as well as the development of a more centralised and coordinated approach to the sharing of information and best practices of cyber security between NATO members[170]. However, more than the technical challenges of responding to a cyber attack promptly, NATO must understand the implications of the use of cyber capabilities in the context of information campaigns[171]. An awareness of the politico-strategic layer of cyber campaigns, which include the psychological effects of disrupting information and perception of management through information campaigns on the websites of target nations, will aid NATO in developing responses to the cyber threat that are not limited to the technical or legal layer of cyberspace.

Maria Snegovaya points out that the novelty of Russia's information war tactics is being exaggerated: "Russian information operations in Ukraine do not herald a new era of theoretical or doctrinal advances, although they aim, in part, to create precisely this impression. Russia's information warfare is thus a significant challenge to the West, but not a particularly novel or

[168] Klimburg, *The Darkening Web. The War for Cyberspace.* 18.
[169] Keir Giles, "Russia's 'New'Tools for Confronting the West Continuity and Innovation in Moscow's Exercise of Power," *Russia and Eurasia, Programme, London: Chatham House* (2016): 50.
[170] North Atlantic Treaty Organization. *Defending the Networks: The NATO Policy on Cyber Defence* (Brussels: North Atlantic Treaty Organization, 2011).
[171] Keir Giles, "Russia's 'New'Tools for Confronting the West Continuity and Innovation in Moscow's Exercise of Power," *Russia and Eurasia, Programme, London: Chatham House* (2016): 62.

insuperable one"[172]. What makes Russia's modern information warfare so dangerous to NATO's current cyber defence is that its current strategy doesn't offer an effective strategy to counter Russian disinformation campaigns. NATO faces the choice of adopting a similar hybrid warfare strategy that will inevitably include cyber attacks in the future, or continue to focus on the technical and legal challenges of cyber threats in the hopes that increased cyber defence capabilities and a more centralised response structure will be enough to deter enemies from attacking its Eastern European member states through cyberspace. NATO has shown no signs of wanting to limit the use of cyber capabilities in its military operations[173]. It might be an indication that the Alliance is moving towards a security approach to cyberspace that incorporates the cyber threat itself into the core of its defence mechanism. By not limiting the use of cyber capabilities in military operations, NATO will instead prepare for cyber war by building its member states' own cyber capabilities in the name of security and defence[174]. The Alliance is still faced with the dilemma of countering Russia's information warfare approach with a strategy that does not compromise the democratic ideals that ensure the freedom of circulation and information in cyberspace.

3.5. The Role of Civil Society in Cyberspace: 'The Whole of Nation' Security Approach and its implications for the circulation of freedom and information

Perhaps the most pressing concern for the future of warfare is the role of civilians. The Law of Armed Conflict (LOAC) stipulates that civilians that make a "direct contribution to a war effort may be subject to attack"[175]. If civilians are indeed identified as the perpetrators of cyber attacks, will they be considered combatants in the case of an Article 5 invocation? States will have to share their cyber capabilities with the private sector and civil society in the future. Does that mean that civilians will have an active role in wars to come? The Georgian and Ukrainian cases certainly suggest it. How will NATO react to the hybrid approaches incorporating civilian action through information campaigns on social media and hacking initiatives? NATO has

[172] Maria Snegovaya, "Russia Report I: Putin's information warfare in Ukraine. Soviet Origins of Russia's Hybrid Warfare," *Institute for the Study of War* (2015): 7.
[173] North Atlantic Treaty Organization. *Warsaw Summit Communiqué* (Brussels: North Atlantic Treaty Organization, 2016).
[174] Alexander Klimburg (Ed.), "National Cyber Security Framework Manual," *NATO CCD COE Publications, Tallinn* (2012): 1-195.
[175] Stephen W. Korns and Joshua E. Kastenberg, "Georgia's cyber left hook," *Parameters* 38.4 (2008): 72.

already announced that it will increase cooperation with the private sector and other intergovernmental bodies like the European Union and the United Nations: "NATO and Allies will work with partners, international organisations, academia and the private sector in a way that promotes complementarity and avoids duplication"[176]. The organisation is aware that in order to counter the evolving cyber threats, it requires the expertise of the private sector, the home of technological innovation and the development of best cyber security practices. What role will these contributors to NATO's cyber defence have in the future o interstate conflicts that include the cyber component?

The inclusion of society into the operations of member states is described as the 'Whole of Nation' approach in NATO CCD COE's Framework Manual for National Cyber Security: "More recently, states have begun looking at better methods for cooperating with their 'national' non-state actors, ranging from aid and humanitarian groups to critical infrastructure providers (sometimes called the Whole of Nation approach or WoN) or even, more generally, their national civil society"[177]. One of NATO's founding member states, The Netherlands, has already enlisted the help of the Organisation for Applied Scientific Research (TNO), which is neither a private company nor a governmental body and enjoys a special constitutional status, to coordinate the relationship between public and private efforts to secure The Netherlands in the cyber domain[178]. The incorporation of society into a state's national security and defence efforts is not new per-se. However, in cyberspace the actors holding cyber power are very differently distributed than in the physical world. The complexity of cyberspace for international relations and governance often lies in the ability of any individual with a computer and the right skills to influence events in the cyber domain. NATO's cooperation with the private sector in cyberspace is a much less regulated partnership than it might perhaps be in the so-called "meat-space". Corporations hold considerable power when it comes to the newest cyber capabilities and methods, which means that NATO states will undoubtedly enlist their aid to fulfil their pledge to increase their cyber defence capabilities and share best practices as they appear on the market.

[176] North Atlantic Treaty Organization. *Defending the Networks: The NATO Policy on Cyber Defence* (Brussels: North Atlantic Treaty Organization, 2011).
[177] Alexander Klimburg (Ed.), "National Cyber Security Framework Manual," *NATO CCD COE Publications, Tallinn* (2012): 30.
[178] Ibid, 93.

NATO admits: "Cyber threats transcend state borders and organisational boundaries"[179]. However, so do NATO's own cyber operations, as they depend on the innovations in cyber security that primarily emerge out of the private sector. Defending the Alliance in cyberspace will not be possible without these non-state actors. Currently, NATO's cyber policy has not implemented any regulations or guidelines determining how the new power structures of cyberspace will translate into further war scenarios.

3.6. NATO's Cyber Security Dispositive: Normalising Cyber Threats and the Consequences for Interstate Conflict

Foucault wrote that security dispositives are distinguished by mechanisms of discipline by their ability to make security threats work within a framework flexible enough to respond to a certain degree of uncertainty[180]. NATO's cyber defence policy has attempted just that by embedding the cyber attacks against Estonia in 2007, Georgia in 2008 and Ukraine in 2014 in existing practices, such as deterrence, and in existing discourses aimed at explaining the political context of Russia's actions in Eastern Europe, namely Information and Hybrid Warfare. The Alliance's response has been an improved and more coordinated technical system of collective defence and increased cooperation with the private sector and other intergovernmental organisations like the European Union and the United Nations. The legal challenges of attribution and the classification of cyber attacks as armed attacks have not been solved by the international community, giving the Alliance more authority to make ad hoc decisions about the applicability of Article 5 in cyberspace. NATO acknowledges that cyber threats are new and fast-evolving, but ultimately normalises the threat they pose to the future of warfare by focusing on improving its technical ability to defend the digital infrastructures of member states.

NATO and its member states are operating within a complex structure of relations with all other sectors of society in cyberspace. The continued evolution of cyber capabilities brought on the market by hackers, companies and other actors outside of NATO's control might become an

[179] North Atlantic Treaty Organization. *Defending the Networks: The NATO Policy on Cyber Defence* (Brussels: North Atlantic Treaty Organization, 2011), page number.
[180] Michel Foucault, *Security, territory, population: lectures at the Collège de France, 1977-1978,* (New York: Macmillan, 2007), 20.

inevitable part of warfare in the future too. In fact, the reliance on deterrence by the Alliance will leave member states vulnerable to a scenario in which civil society can participate in cyber attacks capable of breaching cyber defences. NATO's current cyber defence policy is moving towards an increasing reliance on the Industry, which holds considerable cyber power. However, in the event of an attack in cyberspace all sectors of society could be affected. This is a scenario that NATO has not prepared for in its discourse of deterrence and resilience.

Cyber threats are unlike nuclear weapons or kinetic attacks. As Christian Malis writes: "The cyberworld is as intrinsically decentralized as the nuclear world was centralized: aggression can come from everywhere, the principle of 'only one finger on the nuclear trigger' […] does not apply, the technical entrance barrier is terribly low, much of the defence has to be supported by the civilian/private sector, etc"[181]. The current practices and discourses NATO has produced to incorporate cyber threats into existing military operations and war theories have had the distinctive effect of normalising a phenomenon that requires new theoretical frameworks and practical approaches. As a security dispositive NATO's cyber policy is constructed for maximum flexibility in future scenarios of cyber war: rather than prohibiting the use of cyber capabilities in military operations, it is racing to share best practices and prepare for a time in which a cyber-enhanced nation like Russia might strike. However, while the nuclear arms race was limited to specific governments holding the keys to detonation, no specific state or non-state actor can completely control cyberspace – and NATO is no exception.

NATO responded to a threat in cyberspace by incorporating it into the discourse of Russia's information and hybrid warfare. The hybrid context is a helpful paradigm for understanding the cyber attacks on Estonia, Georgia and Ukraine. The psychological aspects of cyber attacks are as important as their physical or technical damage. One could even argue that Russia's approach to warfare has found a place for the new complex structures of power in cyberspace: the work of hackers during conflicts and wars against its Eastern European neighbours benefits the interests and aims of the Russian government and its military operations. Influencing public opinion has also found a new platform in cyberspace and it can cause considerable damage. NATO has

[181] Christian Malis, "Unconventional Forms of War," (In *The Oxford Handbook of War*, 185-198. Edited by Julian Lindley-French and Yves Boyen. Oxford: Oxford University Press, 2012): 194.

adopted a theory to explain this phenomenon. However, its own practices of cyber defence might endanger the relationship between governments and their citizens: if cyberspace is considered a domain of military operations and if cyber attacks, along with information, will be considered weapons, what exactly will the regulation of cyberspace by NATO mean for freedom of speech and the free circulation of information?[182]

The political subject of security dispositivees, Foucault tells us, is the population[183]. The security of the population is the primary concern of NATO's cyber defence policy and the practices and discourses it has created to fulfil its mandate are ultimately mechanisms aimed at protecting civilians from cyber attacks. In an attempt to ensure cyber security, NATO has militarised a space that is shared on a global level and presented the challenges of cyberspace as technical and legal, when in fact they are political and influenced by meat-space events and relations, such as Russia's tense relations with NATO. The cyber domain offers more challenges to collective defence and cooperative security than simply its technological innovation. Combined with information campaigns, cyber threatens societal structures as much as digital infrastructures. NATO's current Cyber Defence Policy doesn't sufficiently incorporate the uniqueness of cyberspace and the reshuffling of cyber power in assymetric warfare. As a result, the future of armed conflict will be met with pre-existing notions of warfare that might not help NATO member states to understand or respond to cyber attacks as challenges to societal stability.

By categorising cyberspace as the fourth domain of operations, NATO is effectively expanding its military operations into a borderless space shared with a global civil society and other actors holding the power to influence events. Lacking the proper legal framework to hold perpetrators of cyber attacks accountable during a war, NATO either underestimates or neglects the political impact of continuing to enhance its cyber capabilities. Consider the possibility of cyber war involving a NATO member state in the future: not only will NATO possess the most innovative cyber capabilities to defend its digital infrastructure, in the event of a breach of a member state's information and communications system the same capabilities will offer

[182] Klimburg, *The Darkening Web. The War for Cyberspace.* 18.
[183] Michel Foucault, *Security, territory, population: lectures at the Collège de France, 1977-1978,* (New York: Macmillan, 2007), 42.

offensive options. An example of a cyber weapon used by a NATO member state was revealed in 2010:

PART 4: INTERNATIONAL DEVELOPMENTS IN CYBER SECURITY - PREDICTIONS FOR THE FUTURE OF NATO'S CYBER DEFENCE POLICY

Part 4.1. Stuxnet - The Cyber Weapon that will change warfare?

In 2010, a malicious computer worm targeting industrial computer systems was discovered to have been causing damage to Iran's Nuclear Enrichment Program for years[184]. The computer worm was named *Stuxnet* and was allegedly built by a joint U.S.-Israeli task force as part of the U.S. Cyber campaign "Olympic Games", an operation targeting Iran. *Stuxnet* damaged several centrifuges in Iran's uranium enrichment facility, reportedly setting Iran's enrichment programme back a year[185]. *Stuxnet* is widely described as the first cyber weapon, ushering in a new era of warfare[186]. Neither Israel nor the United States of America have claimed responsibility for the attack. Reports by The New York Times and the Washington Post, however, speak of anonymous state officials confirming that *Stuxnet* was part of a U.S. campaign to disrupt Iran's nuclear capabilities[187]. The discovery of *Stuxnet* reveals that the weaponisation of cyber capabilities by state actors is no longer a far-fetched scenario. Reportedly the first known cyber attack to target infrastructure in the physical world, in this case Iran's uranium enrichment facility, *Stuxnet* was described by German cyber security expert Ralph Langner as "the key for a very specific lock"[188]. According to his analysis, the malicious worm was not

[184] Jon R. Lindsay, "Stuxnet and the limits of cyber warfare," *Security Studies* 22.3 (2013): 365.
[185] Ibid, 365.
[186] Ibid, 366.
[187]- David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran". *The New York Times*, June 1, 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=2&_r=1&seid=auto&smid=tw-nytimespolitics&pagewanted=all, accessed on Aug. 20, 2017.

-Ellen Nakashima and Joby Warrick, "Stuxnet was work of U.S. and Israeli experts, officials say". *The Washington Post*, June 2, 2012, https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?utm_term=.17291ad0aff2, accessed on Aug. 20, 2017.

[188] Mary Ellen O'Connell, "Cyber security without cyber war," *Journal of Conflict and Security Law* 17.2 (2012): 194.

designed for purposes of espionage, nor was the target random: "It is about destroying its targets with utmost determination in military style[189]."

The group of experts that compiled the *Tallinn manual on the international law applicable to cyber warfare* concluded that *Stuxnet* qualified as "act of force", but did not specify whether they considered it to be an armed attack[190]. James A. Lewis from the Center for Strategic and International Studies in Washington, D.C. warned that the experts' legal opinion would have difficult consequences for the classification of cyber attacks in the future, referring to the cyber attacks on Estonia to make the point that most cyber attacks did not constitute armed attacks[191]. The debate over *Stuxnet* is necessary for policy-makers and academics to understand the possibilities of cyber weapons being used in war and in peace. As one of the most influential members of NATO, the United States has contributed to the development of a collective cyber policy over the past fifteen years. Its actions do not reflect the actions or policies of the Alliance, but they are an example of an offensive cyber capability approach taken by a member state. Offensive cyber capabilities are being incorporated into military operations without a definite legal standard to judge these uses by: the unmonitored weaponisation of the cyber domain is essentially a matter of societal importance, endangering the free flow of information and communication on a global platform through the actions of national militaries. Failing to address these issues in its Cyber Defence Policy, NATO might be doing a disservice to its mandate to keep citizens of its member states secure in cyberspace.

4.2. In Dialogue with Russia: Two Philosophical Approaches to Cyber Security

This paper has been largely concerned with changes in NATO's Cyber Defence Policy following Russia's actions in three Eastern European countries. However, NATO Allies have also been in dialogue with Russia with the intent of establishing international rules and measures to secure cyberspace. Draft resolutions on cyber security have been presented at the United Nations General Assembly as far back as 2001, when Russia proposed to set up a group of

[189] Ibid, 194.
[190] Kim Zetter, "Legal Experts: Stuxnet Attack on Iran was illegal 'Act of Force'". *WIRED Online*, March 25, 2013, https://www.wired.com/2013/03/stuxnet-act-of-force/, accessed on: Aug. 20, 2017.
[191] Ibid.

governmental experts (GGE) on threats in the areas of cyber and information security[192]. After failing to agree on a definition of cyber attacks in 2004, the GGE settled on a non-binding report positing that international law should apply to cyber conflicts[193]. However, both Russia and China later distanced themselves from the application of the entire UN Charter to cyberspace, especially any reference to Article 51, which gives UN member states the inherent right to defend themselves through use of force should an armed attack occur against them[194]. In the GGE meeting of 2015, the United States attempted to include a reference to Article 51, but Russia, China and a number of other nations feared that the clause would give countries more legitimacy to militarise cyberspace in the name of national security and defence[195].

Even though any mention of Article 51 was excluded from the final report, the fourth GGE meeting further cemented the following norms of state conduct in cyberspace: states should refrain from using or allowing ICT from being used for wrongful acts, let CERT teams operate without hindrance and act cooperatively in the event of CERT investigations into cyber crimes[196]. The norms were described as a breakthrough for U.S. Cyber foreign policy, as they established non-binding measures for state conduct in cyberspace during peace times[197]. Russia remained cautious about the inclusion of Article 51, as Andrei Krutskikh, the Russian presidential special envoy for international cooperation and information security, stated: "…if we did not hesitate to write that the Article 51 of the UN Charter is applicable to the field of ICT, we would have given a strong opportunity for countries to use any hacker attack as a pretext for a retaliatory use of force, that is, for a war[198]." Russia has pushed for stronger governmental oversight over cyberspace, the application of humanitarian laws prohibiting attacks on non-

[192] Klimburg, *The Darkening Web. The War for Cyberspace,* 120.
[193] Ibid, 121.
[194] United Nations. *Charter of the United Nations*. (San Francisco: United Nations, 1945).
[195] Joseph Marks, "U.N. body agrees to U.S. norms in cyberspace". *POLITICO*, September 7, 2015, http://www.politico.com/story/2015/07/un-body-agrees-to-us-norms-in-cyberspace-119900, accessed on Aug. 19, 2017.
[196] NATO Cooperative Cyber Defence Centre of Excellence. "2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law". *Incyder News,* August 31, 2015, https://ccdcoe.org/2015-un-gge-report-major-players-recommending-norms-behaviour-highlighting-aspects-international-l-0.html, accessed on: Aug. 19, 2017.
[197] Ibid.
[198] Sputnik International. "UN Cybersecurity Report Compromises on Self-Defense Issue - Russian Official (August 17, 2015)", [2015 Electronic Resource], https://sputniknews.com/politics/201508171025819426-UN-cybersecurity-report-compromises-on-self-defence/, accessed on Aug. 19, 2017.

combatants, as well as opening the dialogue for cyber arms control and possibly disarmament treaties, which the United States has reportedly continued to oppose[199].

The GGE meetings served to establish international norms and rules about security and defence in cyberspace that included cyber-advanced nations like Russia and China at the negotiation table. The reports that emerged from these meetings reflect the clash between two different approaches to cyber security, backed by equally different strategic interests. By declaring cyberspace as a space in which international laws apply, the United Nations is moving towards the regulation of cyberspace through legal and military means. On the other hand, Russia is amongst the nations pushing for more state control over its national infrastructure in cyberspace, a suggestion that could limit Internet freedom if it was ever implemented in practice. Interestingly, Russia's fears of militarisation and U.S. hegemony in cyberspace has led it to support disarmament or some form of arms control, proposing the signing of international treaties to that effect. The United States and other nations are instead more concerned with national security and defence against cyber attacks, favouring the military approach of strengthening cyber capabilities and regulating their use through international laws and norms. Russia's approach to cyber and information security is geared towards protecting its national sovereignty from international intrusion, while the United Nations is moving closer to a cyber security policy resembling NATO's[200]: in order to secure the free movement of goods and information in cyberspace, the emerging UN norms seem to stress the need for international laws governing cyber crime to protect the economic and political interests of member states, and emphasizes the building of cyber capabilities in order to strengthen cyber defence and security in anticipation of a cyber attack[201].

After meeting for the fifth UN GGE sessions from September 2016 to June 2017, participating nations were unable to reach a consensus on the final report. The future of the group's cooperation is currently in question and both Russia's and the United States' support for

[199] John Markoff and Andrew E. Kramer, "U.S. and Russia Differ on a Treaty for Cyberspace". *The New York Times*, June 27, 2009, http://www.nytimes.com/2009/06/28/world/28cyber.html, accessed on Aug. 20, 2017.
[200] Tim Maurer, "Cyber norm emergence at the United Nations," *Science, Technology, and Public Policy Program* (2011).
[201] Tim Maurer, "Cyber Proxies and the Crisis in Ukraine," in *Cyber War in Perspective: Russian Aggression against Ukraine*, ed. Kenneth Geers (Tallinn: NATO CCD COE Publications, 2015).

the meetings seems to be declining[202]. Further complicating a consensus between Russia's information security approach and cyber defence and security strategies like NATO's is the new role of Industry in the creation of cyber norms and regulations, as corporations like Google and Microsoft have drafted their own proposals for cyber security legislation[203]. Incorporating these new private actors in cyber security discourses or reaching consensus with cyber-advanced nations like Russia with a different philosophical and political approach to state conduct in cyberspace should be a priority for NATO and the United Nations. Without including other practices and discourses in its cyber defence policy, the legal limitations of applying international laws to cyberspace will continue to pose a threat for future uses of cyber capabilities in wars. Furthermore, the diverging philosophies of NATO states, most prominently the United States, and Russia once more show that the rules and norms in cyberspace are being determined by the politico-strategic interests of individual nations.

While the space itself requires new theoretical concepts and practices due to its international, borderless and expansive nature, cyberspace is being regulated and secured by the interests of states and the security and defence strategies that are already known to them. The frequent application of deterrence analogies and legal debates over cyber attacks reveal that there is little space for an interpretation of cyberspace as an entirely different phenomenon than nuclear weapons, terrorism or technological innovations. Ultimately, the militarisation of cyberspace in the name of cooperative security and collective defence that NATO is pursuing is being determined by national security interests, not by an understanding of cyberspace as a truly global space without a single state sovereign. Paradoxically, it might be precisely NATO's

[202] Klimburg, *The Darkening Web. The War for Cyberspace*, 121.
[203] For a transcript of Microsoft Corporation's President Brad Smith's proposal for a Digital Geneva Convention see:

Brad Smith, "Transcript of Keynote Address at the RSA Conference 2017 "The Need for a Digital Geneva Convention"". *Microsoft Corporation*, February 14, 2017, https://mscorpmedia.azureedge.net/mscorpmedia/2017/03/Transcript-of-Brad-Smiths-Keynote-Address-at-the-RSA-Conference-2017.pdf, accessed on Aug. 19, 2017.

For Google's proposal for cross-border access standards in digital security, see:

Google, "Digital Security & Due Process: Modernizing Cross-Border Government Access Standards for the Cloud Era (2017)." [2017 Electronic File], https://www.blog.google/documents/2/CrossBorderLawEnforcementRequestsWhitePaper_2.pdf, accessed on Aug. 19, 2017.

normalisation of cyber security and its militarisation of a global space that could limit the free circulation of movement and information in cyberspace: by insisting that traditional norms and rules of international conflict apply in cyberspace, NATO legitimises the use of national security strategies traditionally embedded into the theoretical framework of territorial sovereignty in a space that was designed to circulate information and goods independent of physical constraints.

CONCLUSION

Any reader of Foucault's work might wonder what he would have to say about security mechanisms in cyberspace. Fortunately, the French philosopher left us with an interesting theory of security dispositives as regulators of threats that ensure the freedom of circulation and movement. In this paper we sought to determine which main practices and discourses of knowledge NATO has been producing for the past fifteen years about the future of cyber threats and their role in interstate conflict. The cyber component in the confrontations between Estonia and Russia in 2007, Georgia and Russia in 2008 and finally Ukraine and Russia in 2014 prompted NATO to expand its cyber defence policy by developing a more centralised cyber security strategy. Its interpretation of Russia's cyber doctrine and warfare methods has shaped its cyber policy as much as the events in Eastern Europe. NATO's cyber security has neither constructed a threat that didn't exist nor has it reacted solely to the technical advances in cyber capabilities. NATO's cyber security dispositive is informed by and adjusted to a calculation of probabilities, namely that of Russia's use of cyber weapons in the context of hybrid warfare in future operations, and the move towards an understanding of cyber capabilities as a weapon and cyberspace as a domain of military operations like the land, air and sea. The assumption that cyber threats will be a part of future warfare has led NATO to develop a strategy that focuses on deterrence analogous to the strategy used to prevent mutually assured destruction through nuclear weapons in the Cold War. Cyber attacks have been incorporated into NATO's existing practices and discourses to find a place for the cyber domain, which is often difficult to define in the context of international relations. As a consequence, NATO's current cyber policy is geared towards the defensive and offensive use of cyber operations in future conflicts and war.

The militarisation of cyberspace by NATO harbours several dangers for the role of cyberspace in international relations. While cyber utopians in the 1990s viewed it as the antidote to governmental power and intervention, the truth is that traditional hierarchies of state power have simply shifted towards more complex structures of power in cyberspace, in which the private sector, international organisations and civil society can all participate and operate in. NATO's partnerships with the private sector suggest that future cyber security strategies will require the Alliance's reliance on industry expertise to respond to the rapid evolution of cyber threats. The possibility that Russia, China, insurgent groups or actors that are hostile to NATO member states might win the cyber arms race influences NATO's decision-making as much as the technical challenges from cyberspace. The strategic implications of NATO's cyber security can therefore not be analysed solely from a technical perspective: the Alliance is establishing a number of legitimising practices, including its partnership with the private sector, that encourage trust in technical solutions to essentially political and ethical problems of cyber warfare[204]. The impact of cyberspace on interstate conflict cannot be reduced to technological progress and innovation.

Cyberspace is a truly global and borderless space, in which information circulates and transactions take place between people and computers independent of physical distances and time[205]. While it may seem that it is an ungovernable space, one mustn't forget that it is still a human-made domain. States and corporations might have difficulty navigating it, but that doesn't mean that it is impossible to exercise power and regulate cyberspace according to human-made norms and rules[206]. Especially in the practice of international security, organisations like NATO must simulate the possibilities and probabilities of different futures in a virtual space that can be used to forge cyber weapons and utilise them in interstate conflict. While experts disagree about the possibility of Cyber War, organisations like NATO must respond to cyber threats as they present themselves entangled with existing tensions in the political arena.

The cyber domain is more than just a new tool for attacking nations or a weapon analogous to nuclear threats. It is a space in which new rules and norms emerge and that can be used to

[204] Hamelink, *The Ethics of Cyberspace*, 7.
[205] Hamelink, *The Ethics of Cyberspace*, 9.
[206] Klimburg, *The Darkening Web. The War for Cyberspace*, 9.

create new practices and discourses, that can be regulated, militarised and normalised to become what powerful actors want it to be. It isn't the ungovernable assurance of freedom that cyber utopians hoped for, nor is it a physical space that states can control and defend like they do physical territories. As opposed to nuclear weapons technology, cyber technology is something most individuals on this planet interact *with and in* on a daily basis. Its complexity doesn't imply ungovernability but a completely new and undefined network of actors that can influence and shape cyberspace, from a single civilian hacker to institutions like NATO.

There are no easy answers - the dilemma of securing cyberspace on one hand and becoming a subversive force limiting the free circulation of information on the other is difficult to incorporate into a cyber defence policy that has to adopt the threat of cyber attacks looming over NATO and its member states. Especially its Eastern European members are threatened by existing and long-lasting tensions with Russia, a country that has been shown to use a completely different approach to cyber capabilities than NATO. Understanding the power and influence of the politico-strategic layer of cyberspace on the technical and legal layers might contribute to a cyber security strategy that is more aware of the new power structures in cyberspace. NATO must accept that it has greater responsibility as an intergovernmental military organisation in cyberspace than coordinating the defence of national digital infrastructures. In order to protect its member states, especially Eastern European countries fearing Russian intervention into their political affairs or territorial integrity, NATO must understand that cyber wars will always be embedded in the human decision-making processes of national militaries, civil society, the private sector and hackers.

Opening a new dialogue about the impact of the cyber domain on warfare practice and the free circulation of information must necessarily include nations with advanced cyber capabilities like Russia and China. The norms and values produced during these discussions will undoubtedly shape the way cyberspace will be regulated by the different actors, state or non-state, in the future. The dangers of NATO’s current cyber security dispositive have been the subject of this paper. However, any attempt to securitise the cyber domain will prioritise some practices and discourses over others. Therefore, it is imperative to continue the discussion of the

socio-political implications of cyber security strategies in the international arena by critically analysing the relation between security, cyberspace and power. As Foucault once said:

"My point is not that everything is bad, but that everything is dangerous, which is not exactly the same as bad. If everything is dangerous, then we always have something to do."[207]

Current word count: 22,400 words (excluding bibliography)

LIST OF ABBREVIATIONS

CCD COE - Cooperative Cyber Defence Centre of Excellence

CERT - Computer Emergency Response Team

CIS - Communications and Information Systems

DDoS - Distributed Denial of Service

DoS - Denial of Service

ICT - Information and Communications Technology

NATO - North Atlantic Treaty Organization

UN - United Nations

UN GGE - United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

[207] Foucault, Michel. *The subject and power*. 1983. In: H. Dreyfus & P. Rabinow (Eds.), *Michel Foucault: Beyond structuralism and hermeneutics, 2nd ed.* Chicago: University Of Chicago Press, 2014, pp. 231-232.

BIBLIOGRAPHY

Primary Literature

Geers, Kenneth, (ed). *Cyber war in perspective: Russian aggression against Ukraine*. Tallinn: NATO CCD COE Publications, 2015.

Joubert, Vincent. “Five Years After Estonia's Cyber Attacks: Lessons Learned for NATO?”. *NATO Defense College, Research Division*, (2012): 1-8.

Klimburg, Alexander (Ed.). “National Cyber Security Framework Manual.” *NATO CCD COE Publications, Tallinn* (2012): 1-195.

Maurer, Tim. "Cyber Proxies and the Crisis in Ukraine." In *Cyber War in Perspective: Russian Aggression against Ukraine*, 79-87. Edited by Kenneth Geers. Tallinn: NATO CCD COE Publications, 2015.

North Atlantic Treaty Organization. *Bucharest Summit Declaration*. Brussels: North Atlantic Treaty Organization, 2008.

North Atlantic Treaty Organization, *Chicago Summit Declaration.* Brussels: North Atlantic Treaty Organization, 2012.

North Atlantic Treaty Organization. *Commitment to Enhance Resilience Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw, 8-9 July 2016.* Brussels: North Atlantic Treaty Organization, 2016.

North Atlantic Treaty Organization. “Cyber Defence,” http://www.nato.int/cps/en/natohq/topics_78170.htm, accessed on Aug. 16, 2017.

North Atlantic Treaty Organization. *Cyber Defence Pledge*. Brussels: North Atlantic Treaty Organization, 2016.

North Atlantic Treaty Organization. *Defending the Networks: The NATO Policy on Cyber Defence.* Brussels: North Atlantic Treaty Organization, 2011.

North Atlantic Treaty Organization. *Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization.* Brussels: North Atlantic Treaty Organization, 2016.

North Atlantic Treaty Organization. *Lisbon Summit Declaration*. Brussels: North Atlantic Treaty Organization, 2010.

North Atlantic Treaty Organization. *Prague Summit Declaration*. Brussels: North Atlantic Treaty Organization, 2002.

North Atlantic Treaty Organization. *Riga Summit Declaration*. Brussels: North Atlantic Treaty Organization, 2006.

North Atlantic Treaty Organization. *Strasbourg/Kehl Summit Declaration*. Brussels: North Atlantic Treaty Organization, 2009.

North Atlantic Treaty Organization. *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization Adopted by Heads of State and Government at the NATO Summit in Lisbon 19-20 November 2010.* Brussels: North Atlantic Treaty Organization, 2010.

North Atlantic Treaty Organization. *The North Atlantic Treaty*. Washington D.C.: North Atlantic Treaty Organization, 1949.

North Atlantic Treaty Organization. *The Warsaw declaration on Transatlantic Security Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016.* Brussels: North Atlantic Treaty Organization, 2016.

North Atlantic Treaty Organization. *Wales Summit Declaration*. Brussels: North Atlantic Treaty Organization, 2014.

North Atlantic Treaty Organization. *Warsaw Summit Communiqué*. Brussels: North Atlantic Treaty Organization, 2016.

NATO Cooperative Cyber Defence Centre of Excellence, “NATO Cooperative Cyber Defence Centre of Excellence - Home Page,” https://ccdcoe.org/, accessed on Aug. 18, 2017.

NATO Cooperative Cyber Defence Centre of Excellence. “*Events: Cyber Defence Exercises/Locked Shields 2017,”*. https://ccdcoe.org/locked-shields-2017.html, accessed on Aug. 18, 2017.

NATO Cooperative Cyber Defence Centre of Excellence, “History,” https://ccdcoe.org/history.html, accessed on Aug. 18, 2017.

NATO Cooperative Cyber Defence Centre of Excellence. “2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law”. *Incyder News,* August 31, 2015, https://ccdcoe.org/2015-un-gge-report-major-players-recommending-norms-behaviour-highlighting-aspects-international-l-0.html, accessed on: Aug. 19, 2017.

Schmitt, Michael N (ed). *Tallinn manual on the international law applicable to cyber warfare*. Cambridge: Cambridge University Press, 2013.

Tikk, Eneken, Kaska,Kadri, Rünnimeri, Kristel, Kert, Mari, Talihärm, Anna-Maria, Vihul, Liis. "Cyber attacks against Georgia: Legal lessons identified." *NATO Cooperative Cyber Defence Centre of Excellence, Tallinn* (2008): 3-45.

Tikk, Eneken, Kaska, Kadri and Vihul, Liis. *International cyber incidents: Legal considerations*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2010.

NATO Cooperative Cyber Defence Centre of Excellence, Tallinn Papers:

Geers, Kenneth. “Pandemonium: Nation States, National Security, and the Internet”. *NATO Cooperative Cyber Defence Centre of Excellence, Tallinn Paper 1* (2014): 1-13.

Vihul, Liis. “The Liability of Software Manufacturers for Defective Products”. *NATO Cooperative Cyber Defence Centre of Excellence, Tallinn Paper 2* (2014): 1-14.

Krause, Hannes. “NATO on Its Way Towards a Comfort Zone in Cyber Defence”. *NATO Cooperative Cyber Defence Centre of Excellence, Tallinn Paper 3* (2014): 1-6.

Areng, Liina. “Lilliputian States in Digital Affairs and Cyber Security”. *NATO Cooperative Cyber Defence Centre of Excellence, Tallinn Paper 4* (2014): 1-12.

Schmitt, Michael N. and Vihul, Liis. “The Nature of International Law Cyber Norms”. *NATO Cooperative Cyber Defence Centre of Excellence, Tallinn Paper 5* (2014): 1-31.

Carr, Jeffrey. “Responsible Attribution: A Prerequisite for Accountability”. *NATO Cooperative Cyber Defence Centre of Excellence, Tallinn Paper 6* (2014): 1-8.

Schmitt, Michael N. “The Law of Cyber Targeting.” *NATO Cooperative Cyber Defence Centre of Excellence, Tallinn Paper 7* (2015): 1-20.

Lewis, James A. “The Role of Offensive Cyber Operations In NATO’s Collective Defence.” *NATO Cooperative Cyber Defence Centre of Excellence, Tallinn Paper 8* (2015): 1-12.

Secondary Literature

Allison, Roy. "Russian ‘deniable’ intervention in Ukraine: how and why Russia broke the rules." *International Affairs* 90.6 (2014): 1255-1297.

Arquilla, John, and David Ronfeldt. "Cyberwar is coming!." *Comparative Strategy* 12.2 (1993): 141-165.

Barlow, John Perry, "A Declaration of the Independence of Cyberspace”, *Electronic Frontier Foundation (*1996), https://www.eff.org/cyberspace-independence, accessed on Aug. 5, 2017.

Biersack, John, and Shannon O’lear. "The geopolitics of Russia's annexation of Crimea: narratives, identity, silences, and energy." *Eurasian Geography and Economics* 55.3 (2014): 247-269.

Carr, Jeffrey. *Cyber Warfare.* Sebastopol: O’Reily, 2011.

Carr, Jeffrey. "Project Grey Goose Phase I Report." *Project Grey Goose* (2008).

Cavelty, Myriam Dunn. "Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities." *Science and Engineering Ethics* 20.3 (2014): 701-715.

Cavelty, Myriam Dunn. "Critical information infrastructure: vulnerabilities, threats, and responses." *Disarmament Forum* 9:3 (2007): 15-20.

Choucri, Nazli. "Emerging Trends in Cyberspace: Dimensions & Dilemmas." *Williams and Fiddner, Cyberspace: Malevolent Actors, Criminal Opportunities, and Strategic Competition* (2012): 1-18.

Czosseck, Christian, Rain Ottis, and Anna-Maria Talihärm. "Estonia after the 2007 cyber attacks: Legal, strategic and organisational changes in cyber security." *Case Studies in Information Warfare and Security: For Researchers, Teachers and Students* 72 (2013).

Davis, Joshua. “Hackers Take Down The Most Wired Country in Europe”. *Wired Online*, August 21, 2007, https://www.wired.com/2007/08/ff-estonia/, accessed on Aug. 10, 2017.

De Graaf, Beatrice, and Cornel Zwierlein. “Historicizing Security - Entering the Conspiracy Dispositive.” *Historical Social Research/Historische Sozialforschung*, 38, no. 1 (143), (2013): 46–64.

Dillon, Michael, and Andrew Neal (eds). *Foucault on politics, security and war*. Basingstoke: Palgrave Macmillan, 2008.

Dreyfus, Hubert L.. And Paul Rabinow. *Michel Foucault: Beyond structuralism and hermeneutics*. Chicago: University of Chicago Press, 1983.

Evans, Brad. "Foucault’s legacy: Security, war and violence in the 21st century." *Security Dialogue* 41.4 (2010): 413-433.

Farwell, James P., and Rafal Rohozinski. "The new reality of cyber war." *Survival* 54.4 (2012): 107-120.

Fidler, David P., Richard Pregent, and Alex Vandurme. "NATO, Cyber Defense, and International Law." *Journal of International and Comparative Law* 4.1 (2016): 1-25.

Foucault, Michel. *Security, territory, population: lectures at the Collège de France, 1977-1978.* New York: Macmillan, 2007.

Foucault, Michel. "The subject and power." In *Michel Foucault: Beyond structuralism and hermeneutics*, 208-226. Edited by Hubert L. Dreyfus and Paul Rabinow. Chicago: University of Chicago Press, 1983.

Franscella, Joe. "Cybersecurity vs. Cyber Security: When, Why and How to Use the Term." *InfoSec Island* (2013), http://www.infosecisland.com/blogview/23287-Cybersecurity-vs-Cyber-Security-When-Why-and-How-to-Use-the-Term.html, accessed on Aug. 20, 2017.

Gartzke, Erik, and Jon R. Lindsay. "Weaving tangled webs: offense, defense, and deception in cyberspace." *Security Studies* 24.2 (2015): 316-348.

Giles, Keir. "Russia's 'New'Tools for Confronting the West Continuity and Innovation in Moscow's Exercise of Power." *Russia and Eurasia, Programme, London: Chatham House* (2016): 4-71.

Google, "Digital Security & Due Process: Modernizing Cross-Border Government Access Standards for the Cloud Era (2017)." [2017 Electronic File], https://www.blog.google/documents/2/CrossBorderLawEnforcementRequestsWhitePaper_2.pdf, accessed on Aug. 19, 2017.

Grant, Thomas D. "Annexation of Crimea." *American Journal of International Law* 109.1 (2015): 68-95.

Hamelink, Cees J. *The Ethics of Cyberspace.* London: SAGE Publications, 2001.

Hansen, Lene, and Helen Nissenbaum. "Digital disaster, cyber security, and the Copenhagen School." *International studies quarterly* 53.4 (2009): 1155-1175.

Herzog, Stephen. "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses." *Journal of Strategic Security* 4, no. 2 (2011): : 49-60.

Hoffman, Frank G. *Conflict in the 21st century: The rise of hybrid wars.* Arlington: Potomac Institute for Policy Studies, 2007.

Human Rights Watch. “Up In Flames Humanitarian Law Violations and Civilian Victims in the Conflict over South Ossetia (2009)”. [2009 Electronic File], https://www.hrw.org/sites/default/files/reports/georgia0109web.pdf, accessed on Aug. 20, 2017.

Junio, Timothy J. "How probable is cyber war? Bringing IR theory back in to the cyber conflict debate." *Journal of Strategic Studies* 36.1 (2013): 125-133.

Klimburg, Alexander. "Mobilising cyber power." *Survival* 53.1 (2011): 41-60.

Klimburg, Alexander. *The Darkening Web. The War for Cyberspace.* New York: Penguin, 2017.

Korns, Stephen W., and Joshua E. Kastenberg. "Georgia's cyber left hook." *Parameters* 38.4 (2008): 60-76.

Liff, Adam P. "Cyberwar: a new ‘absolute weapon’? The proliferation of cyberwarfare capabilities and interstate war." *Journal of Strategic Studies* 35.3 (2012): 401-428.

Lindsay, Jon R. "Stuxnet and the limits of cyber warfare." *Security Studies* 22.3 (2013): 365-404.

Lindsay, Jon R. "Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack." *Journal of Cybersecurity* 1.1 (2015): 53-67.

Malis, Christian. “Unconventional Forms of War.” In *The Oxford Handbook of War,* 185-198. Edited by Julian Lindley-French and Yves Boyen. Oxford: Oxford University Press, 2012.

Markoff, John, and Andrew E. Kramer. “U.S. and Russia Differ on a Treaty for Cyberspace”. *The New York Times,* June 27, 2009, http://www.nytimes.com/2009/06/28/world/28cyber.html, accessed on Aug. 20, 2017.

Marks, Joseph. “U.N. body agrees to U.S. norms in cyberspace”. *POLITICO*, September 7, 2015, http://www.politico.com/story/2015/07/un-body-agrees-to-us-norms-in-cyberspace-119900, accessed on Aug. 19, 2017.

Maurer, Tim. "Cyber norm emergence at the United Nations." *Science, Technology, and Public Policy Program* (2011).

Maurer, Tim, and Scott Janz. "The Russian-Ukraine Conflict: Cyber and Information Warfare in a Regional Context." *The International Relations and Security Network* 17 (2014).

McGavran, Wolfgang. "Intended consequences: regulating cyber attacks." *Tul. J. Tech. & Intell. Prop.* 12 (2009): 259-275.

Mearsheimer, John J. "Why the Ukraine crisis is the West's fault: the liberal delusions that provoked Putin." *Foreign Aff.* 93 (2014): 77-89.

Morozov, Evgeny. *The net delusion: How not to liberate the world*. London: Penguin, 2011.

Nakashima, Ellen, and Joby Warrick. “Stuxnet was work of U.S. and Israeli experts, officials say”. *The Washington Post*, June 2, 2012, https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?utm_term=.17291ad0aff2, accessed on Aug. 20, 2017.

O’Connell, Mary Ellen. "Cyber security without cyber war." *Journal of Conflict and Security Law* 17.2 (2012): 187-209.

Obama, Barack H. “Remarks by the President to the Business Roundtable (2015)”. [2015 Electronic Resource], https://www.whitehouse.gov/the-press-ofce/(2015)/09/16/remarks-president-business-roundtable, accessed on Aug. 18, 2017.

PBS Frontline. “Interview with James Lewis (2003)”. [2003 Electronic Resource], http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/lewis.html, accessed on Aug. 20, 2017.

PR Newswire. “Newsweek Exclusive: ‘We’re in the Middle of a Cyber War’ (September 12, 1999)”. [1999 Electronic Resource], http://www.prnewswire.com/news-releases/newsweek-exclusive-were-in-the-middle-of-a-cyberwar-74343007.html, accessed on Aug. 16, 2017.

Rid, Thomas, and Ben Buchanan. "Attributing cyber attacks." *Journal of Strategic Studies* 38.1-2 (2015): 4-37.

Rid, Thomas. "Cyber war will not take place." *Journal of strategic studies* 35.1 (2012): 5-32.

Ruus, Kertu. "Cyber war I: Estonia attacked from Russia." *European Affairs* 9.1-2 (2008).

Sanger, David E. “Obama Order Sped Up Wave of Cyberattacks Against Iran”. *The New York Times*, June 1, 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=2&_r=1&seid=auto&smid=tw-nytimespolitics&pagewanted=all, accessed on Aug. 20, 2017.

Smith, Brad. “Transcript of Keynote Address at the RSA Conference 2017 “The Need for a Digital Geneva Convention””. *Microsoft Corporation*, February 14, 2017, https://mscorpmedia.azureedge.net/mscorpmedia/2017/03/Transcript-of-Brad-Smiths-Keynote-Address-at-the-RSA-Conference-2017.pdf, accessed on Aug. 19, 2017.

Snegovaya, Maria. "Russia Report I: Putin’s information warfare in Ukraine. Soviet Origins of Russia’s Hybrid Warfare”, *Institute for the Study of War* (2015).

Sputnik International. “UN Cybersecurity Report Compromises on Self-Defense Issue - Russian Official (August 17, 2015)”, [2015 Electronic Resource], https://sputniknews.com/politics/201508171025819426-UN-cybersecurity-report-compromises-on-self-defence/, accessed on Aug. 19, 2017.

State Statistics Committee of Ukraine. “About number and composition population of AUTONOMOUS REPUBLIC OF CRIMEA by All-Ukrainian population census’ 2001 data (2003-2004),” [2003-2004 Electronic Resource], http://2001.ukrcensus.gov.ua/eng/results/general/language/Crimea/, accessed on Aug. 20, 2017.

Swanson, Lesley. "The era of cyber warfare: Applying international humanitarian law to the 2008 Russian-Georgian cyber conflict." *Loy. LA Int'l & Comp. L. Rev.* 32 (2010): 303-333.

Tikk, Eneken. "Global Cybersecurity–Thinking About the Niche for NATO." *SAIS Review of International Affairs* 30.2 (2010): 105-119.

United Nations. *Charter of the United Nations*. San Francisco: United Nations, 1945.

Wichum, Ricky. "Security as dispositif: Michel Foucault in the field of security." *Foucault Studies* 15 (2013): 164-171.

Willcocks, Leslie P. "Michel Foucault in the social study of ICTs: Critique and reappraisal." *Social science computer review* 24.3 (2006): 274-295.

Woltag, Johann-Christoph. *Cyber Warfare: Military Cross-Border Computer Network Operations under International Law*. Cambridge: Intersentia, 2014.

Yost, David S. "NATO's evolving purposes and the next Strategic Concept." *International affairs* 86.2 (2010): 489-522.

Zetter, Kim. “Legal Experts: Stuxnet Attack on Iran was illegal ‘Act of Force’”. *WIRED Online*, March 25, 2013, https://www.wired.com/2013/03/stuxnet-act-of-force/, accessed on: Aug. 20, 2017.