CHARLES UNIVERSITY IN PRAGUE

FACULTY OF SOCIAL SCIENCES

Master Thesis

2018 **André Viana**

CHARLES UNIVERSITY IN PRAGUE

FACULTY OF SOCIAL SCIENCES

Institute of Political Studies

André Viana

NATO and Offensive Cybersecurity: A Strategic Analysis

Master thesis

Prague 2018

Author: BSc. André Lopes Carvalho Viana

Supervisor: PhDr. Vít Střítecký, Ph.D., M.Phil.

External Advisor: PhDr. André Inácio, Ph.D., LL.M.

Bibliographic Note

Viana, André Lopes C. *NATO and Offensive Cybersecurity: A Strategic Analysis*, [number of pages]p. Master Thesis. Charles University, Faculty of Social Sciences, Institute of Political Studies. Supervisor PhDr. Vít Střítecký, M.Phil., Ph.D.

Abstract

This thesis presents a strategic analysis on the possibility of use of offensive cyber capabilities by NATO in its defensive efforts. There is a vast array of academic literature regarding the strategic value of the use of offensive capabilities in cybersecurity, and NATO's cyber posture, however, there is little available regarding the relationship between both. Through the use of tools borrowed from Strategic Studies, this thesis attempts to determine whether it is possible to formulate valid cybersecurity strategies for the use of offensive cyber capabilities from the combination of known academic concepts with current NATO capabilities. The thesis also analyzes the possible implications of using such strategies as well as the underlying causes of their potential success or failure.

Keywords

NATO, Cybersecurity, Cyber Defense, Cyberstrategy, Cyber Capabilities, Strategic Studies, Offensive Capabilities

Range of thesis:

106 pages, 190'790 keystrokes, incl. spaces. Thesis text only: 86 pages, 21'316 words, 139'841 keystrokes, incl. spaces.

Declaration of Authorship

1. The author hereby declares that he compiled this thesis independently, using only the listed resources and literature.

2. The author hereby declares that all the sources and literature used have been properly cited.

3. The author hereby declares that the thesis has not been used to obtain a different or the same degree.

Lisbon, Portugal, 30 July 2018

André Viana

Acknowledgements

I would like to take the opportunity to thank my supervisor, Vít Střítecký, for guiding me during the entire writing process, and being extremely kind and understanding. I also want to thank my advisor, André Inácio, for helping me shape the idea that became the starting point of this thesis. I am thankful to Lucie Kadlecová for allowing me to attend her classes and being kind enough to take the time for after-class discussions with me, as well as reviewing my theoretical background chapters. These sessions gave me crucial insight that helped shape my thesis. Finally, I am also indebted to my partner, Dorota Kusiak, who supported my writing efforts the entire way. She went out of her way to continuously read my drafts and discuss them with me, which helped improve my writing style.

TABLE OF CONTENTS

Abstract iii

Declaration of Authorship iv

Acknowledgements v

Introduction 1

1. Defining Cyberspace 6

   1.1. Cybersecurity and NATO 8

2. The Offense vs. Defense Discourse in Cyberspace 14

   2.1 Does Cyberspace Favor an Offensive or Defensive Approach? 15

3. NATO Cyber Posture 20

   3.1 NATO's Shortcomings 28

4. Strategic Analysis: The Lykke Model 32

   4.1 Lykke Model 33

   4.2. Components 35

      4.2.1. Component 1: Objectives 35

      4.2.2. Component 2: Resources 36

      4.2.3. Component 3: Concepts 37

      4.3.3. Component 4: Risk Assessment 47

5. Methodology 51

6. Analysis 55

   6.1. Objectives 55

   6.2. Resources 56

6.3. Strategy of Punctuated Deterrence 58

6.3.1. Risk Assessment.. 59

6.3.2. Evaluation.. 61

6.4. Strategy of Cyber Persistence 66

6.4.1. Risk Assessment.. 67

6.4.2. Evaluation.. 69

6.5. Strategy of Cyber Deception... 72

6.5.1. Risk Assessment.. 73

6.5.2. Evaluation.. 75

7. Summary of Results 79

8. Conclusion.. 81

Bibliography 87

Introduction

In the beginning of November 2017, the meeting between the Defense Ministers from the various nations that make up NATO produced an unprecedented result: the adoption of the allied members' cyber capabilities by the organization for its missions and operations. However, no confirmation or denial was provided by NATO Secretary General Jens Stoltenberg regarding the possible adoption and use of these capabilities as offensive tools when directly asked by Europa Press during the press conference:

> "What we have done today is to agree the framework and the principles for how to integrate cyber capabilities into NATO missions and operations. Then it will be a decision by nations what kind of capabilities they are willing integrate and to use in specific missions and operations (…) regardless of whether we speak about a plane or a tank or a cyber capability, the use of these capabilities is going to be in accordance with international law and it's going to be part of the defensive posture of NATO"[1]

While advances in Information and Communication Technology (ICT) since the turn of the century have allowed societies across the globe to become increasingly interconnected and digitalized, these advances have also facilitated the use of the technology for propaganda, espionage and an astounding array of criminal activity.[2] This has propelled states to consider cyberspace a national security concern as well as an effective tool for foreign policy, leading to its militarization. As the world's largest military alliance, NATO needs to remain at the forefront of this phenomenon. Its failure to help protect its member states from major hostile cyber operations or rally a collective response afterwards, such as in the cases of the operations against Estonia in

[1] North Atlantic Treaty Organization. "Press conference by NATO Secretary General Jens Stoltenberg following the meeting of the North Atlantic Council at the level of Defence Ministers." North Atlantic Treaty Organization Newsroom (2017).

[2] Klimburg, Alexander. 2017. The Darkening Web: The War for Cyberspace. New York: Penguin, 89.

2007[3], Lithuania in 2008[4], and the U.S. in 2016[5], have exposed NATO's deficiencies in cyberspace at a legal, institutional and operational level. The adoption of the allied members’ cyber capabilities by the organization, which was the result of the NATO Defense Ministers' meeting in 2017, was an unprecedented step in the field of cybersecurity in the context of the Alliance’s policies. U.S. Navy Commander Michael Widmann at the NATO Cooperative Cyber Defense Centre of Excellence made this rationale clearer later that month: “There’s a change in the (NATO) mindset to accept that computers, just like aircraft and ships, have an offensive capability.”[6]

These events led to some initial questions that sparked and guided this thesis' research: how exactly would NATO be able to use offensive capabilities as part of its defensive posture? With what objective(s) would NATO use these capabilities? What consequences could this have for NATO’s relationship with its Allies, partners and external nations?

The topic of offensive capabilities was also addressed during last year’s symposium on cybersecurity, the Third International Cyber Operations Symposium, organized by the Dutch Ministry of Defense. In a recap of the discussions, Max Smeets from Stanford University Center for International Security and Cooperation (CISAC), pointed out:

> “Every scholar or policymaker at the conference noted that deterrence was a flawed strategy to pursue in cyberspace - either partially or completely. Yet, there remains a lack of alternatives and policymakers at the conference seemed unaware of ideas raised in the academic literature about the strategic value of offensive

[3] Saltzman, Ilai. 2013. “Cyber Posturing and the Offense-Defense Balance, Contemporary Security Policy”, Vol. 34:1, 54.

[4] Burton, Joe. 2015. "NATO's cyber defence: strategic challenges and institutional adaptation", Defense Studies, Vol. 15:4, 306-307.

[5] Kello, Lucas. 2017. *The Virtual Weapon and International Order*. New Haven: Yale University Press, 212-229.

[6]Emmott,Robin. 2017. “NATO mulls 'offensive defence' with cyber warfare rules”.[NATO CCDCE Head of Strategy Michael Widmann, interview with REUTERS], REUTERS.

> cyber capabilities, such as Kello's cumulative deterrence, Harknett's notion of persistence, or Lindsay and Gartzke's discussion of deception."[7]

Whereas the aforementioned conference focused solely on European countries, the majority of literature from scholars and experts alike surrounding NATO and cybersecurity shares the view that the Alliance also faces the need of a new approach towards the value of offensive capabilities in light of recent developments, as it will be shown in more detail in chapter three. Surprisingly enough, the available academic literature seems to be centered on the organization's currently inadequate cyber posture, the consequential necessity of adopting offensive cyber capabilities or its implications in warfare[8], but the possibility of a study on how these capabilities could be integrated into the alliance to address threats below the armed threshold is still largely unexplored, with only "The Virtual Weapon and International Order"[9] by Lukas Kello providing new insights into cyberstrategy by applying international relations theory. There have been similar studies to this thesis, such as "Strategic Cyber Security"[10] by Kenneth Geers, in which he analyzes four strategies formulated from categorically divergent nation-state approaches to threat mitigation. In "Strategic Cyber Deterrence: The Active Cyber Defense Option"[11], Scott Jasper extensively analyzes current strategic practices in cyberspace, and introduces his own hybridized alternative. Despite this, no notable research of this kind was found related to NATO and the possible use of cyber offensive

[7] Segal, Adam. 2017. "Europe Slowly Starts to Talk Openly About Offensive Cyber Operations", Council on Foreign Relations.

[8] See Saltzman, Ilai. 2013. "Cyber Posturing and the Offense-Defense Balance", Contemporary Security Policy, Vol. 34:1, 40-63; Szentgáli, Gergely, 2013. "The NATO Policy on Cyber Defense: The Road so Far". AARMS Vol. 12:1, 83-91; Rühle, Michael. 2011. "NATO and Emerging Security Challenges: Beyond the Deterrence Paradigm". American Foreign Policy Interests, Vol. 33:6, 278-282; Canbolat, Mustafa and Emrah Sezgin. 2016. "Is NATO Ready For a Cyber War?". Master Thesis, Naval Postgraduate School, Monterey.

[9] Kello, Lucas. 2017. The Virtual Weapon and International Order. New Haven: Yale University Press.

[10] Geers, Kenneth. 2017. Strategic Cyber Security. Tallinn: NATO Cooperative Cyber Defense Centre of Excellence.

[11] Jasper, Scott. 2017. Strategic Deterrence: The Active Cyber Defense Option. New York: Rowman & Littlefield.

capabilities. To be able to fill this gap, further research was conducted to select at least three diverging theoretical concepts on the use of offensive cyber capabilities in cybersecurity, along with an appropriate method that could help analyze and operationalize them. The selection was based on how known and reputable the concepts and their authors are, the date at which it they were published, and the divergence between them. Coincidentally, the same three concepts mentioned by Smeets were found to be the most recent (2015-2017), well-founded and diverging, all three from known scholars in the field of cybersecurity. During this period, it was observed that the field of Strategic Studies offered the required framework to both analyze the concepts and measure the results of their integration with NATO capabilities. The answer to the necessity of a proper methodological approach came in the form of the Lykke Strategic Model, extensively used in American military strategic planning.

In an attempt to narrow down this thesis' research question while still retaining the ability to integrate these concepts from academic literature and satisfy the initial queries created, the final research question was formulated:

> *Can emerging concepts on the use of offensive cyber capabilities in the context of cybersecurity become valid, operational strategies for NATO and retain their theoretical strategic value?*

Answering this question will determine if it is possible for NATO, in its current state, to draw upon recent academic literature on offensive cyber capabilities to complement its strategic efforts in cybersecurity, which can open the door for future policy improvements in the Alliance. To support its argumentation, the thesis relies on extensive theoretical and historical background, which is presented in the first four chapters. Chapter one will approach the conceptualizations of cyberspace and cybersecurity, and contextualizes them within NATO's policies. This part of the paper is crucial to understand the kind of threats the Alliance faces in cyberspace, and the role it can play in each of them within this domain. Chapter two will discuss the debate on whether cyberspace leans more towards offensive or defensive tendencies in order to ascertain what each concept encompasses and to locate where NATO's own practices fit. Supported by the previous two chapters, chapter three will provide the relevant historical background of the Alliance's posture in cyberspace to comprehend the current shortcomings in Allied cyber defense strategy. Among the most important theoretical parts of the thesis, chapter four will explain the workings of the model, its originating field of study, and introduce the academic concepts that will be used for the analysis. This background information and theoretical aspects of the research will be followed by the methodology chapter, where the model will be related to the research question and the limitations of this approach discussed.. Chapters six and seven will cover the analysis and the results. Here, the model will draw upon the data presented throughout the thesis to formulate operational strategies and evaluate them. In the last step, the conclusion, the insights acquired during the analysis, as well as reflecting on potential improvements to the strategies and the research conducted will be discussed. The strategies formulated in this paper are intended to respond to threats within cyberspace that could compromise the Alliance's networks, and by extension sabotage its military and political efforts.

1. Defining Cyberspace

The continuous evolution of cyberspace has hardened scholarly attempts to define it, along with its associated terms and concepts. Peter W. Singer and Allan Friedman attempt to address this issue in their book “Cybersecurity and Cyberwar: What Everyone Needs to Know” by informing and educating the public about this area. Citing definition attempts by the Pentagon since the advent of the internet, the authors recognize that “not only in its expansive, global nature, but also in the fact that the cyberspace of today is almost unrecognizable compared to its humble beginnings„[12] make the term so difficult to define. They opt for a simple definition and treat cyberspace as “the realm of computer networks (and user behind them) in which information is stored, shared, and communicated online„[13]. They add that although it is primarily an information environment, it is not purely virtual but requires presence in the physical realm in the form of infrastructure and systems that store the data and allow it to flow.[14]

Several definitions have surfaced from sovereign states and international organizations alike by necessity, a reflection of the importance this realm has acquired regarding security-related activities.[15]The International Telecommunications Union (ITU) of the United Nations has coined cyberspace as "the physical and non-physical terrain created by and/or composed of some or all of the following: computers, computer systems, networks and their computer programs, computer data, content data,

[12] Friedman, Allan and Peter W. Singer. 2014. Cybersecurity and Cyberwar: What Everyone Needs to Know. New York : Oxford University Press, 13.

[13] Ibid.

[14] Ibid, 12-16.

[15] Even, Shmuel and David Siman-Tov; Rosen, Judith (ed.). 2012. Cyber Warfare: Concepts and Strategic Trends. Memorandum 117. Tel Aviv: Institute for National Security Studies, 10-35.

traffic data, and users."[16]. The NATO Cooperative Cyber Defense Centre of Excellence in Estonia (CCDCOE) contains a vast compilation of cyberspace definitions taken from their respective cybersecurity strategy documents, all of which - albeit in different terms - acknowledge the existence of different layers interconnected with one another.[17] While the number of layers recognized by each state varies, the most commonly accepted are the human, logical and physical layers. The most inner layer is the physical layer. Comprised by the large network of IT infrastructures, this includes all the existent hardware found at land, sea, air or space such as satellites, signal towers, routers, IT devices, and transatlantic cables. The middle layer - called logical or virtual layer - encompasses the software, firmware, and all data that is present and sustained through hardware (including the internet). The final and most distinguishing layer is the human (or cognitive)layer, which involves the users themselves.[18] USAF Lieutenant Colonel Trujillo highlighted the relevance of this major element in cyberspace in the Joint Force Quarterly:

> “Whereas other domains are solely part of the physical environment, cyberspace, as the only man-made domain, is shaped and used by humans. Cognitive personas interact with the virtual environment and each other. (...) this human personal can be reflective, multiplicative, or anonymous. Cognitive users of the cyberspace environment can be nation-state or nonstate actors (such as users, hackers, criminals, or terrorists).”[19]

Cyberspace has enabled both state and nonstate actors to perform actions without traditional geographical limitations at incredible speeds, throwing conventional

[16] International Telecommunications Union. 2010. "ITU Toolkit for Cybercrime Legislation", Report commissioned by ITU Development Sector of Cybersecurity. Geneva: ITU, 12.

[17] For example: the "Nationale Cyber-Sicherheitsstrategie" (Germany) and the "Cybersecurity Strategy of the United Kingdom" both provide definitions that recognize the different layers of cyberspace, however their definitions are narrowed and centered around the logical layer. In: NATO Cooperative Cyber Defense Centre of Excellence. " Cyber Definitions".

[18] Even, Shmuel and David Siman-Tov; Rosen, Judith (ed.). 2012. Cyber Warfare: Concepts and Strategic Trends. Memorandum 117. Tel Aviv: Institute for National Security Studies, 10-13.

[19] Trujillo, Clorinda. 2014. "The Limits of Cyberspace Deterrence". Joint Force Quarterly, Issue 75. Washington, D.C.: National Defense University Press.

security concepts in disarray. The ability to act in anonymity, the low threshold of entry and the extent at which devices operating in other domains[20] are connected to cyberspace also made it an extremely attractive place for malicious use, prompting states and organizations like NATO to address it.

1.1. Cybersecurity and NATO

Just as with cyberspace, scholars have consistently struggled with conceptual challenges regarding cybersecurity. While the CCDCOE compiled a list of definitions from several states, these vary according to respective national interests, thus keeping the fundamental terminology regarding cybersecurity and its categories a subject of constant debate.[21] Instead, a rather simplified definition can be used to introduce the term. Cybersecurity expert Joe Burton wrote:

> „Cybersecurity, at its most basic level, is about being secure from (a) cyber attacks - efforts to disrupt, delay or destroy computer networks, and (b) cyber exploitation - efforts to covertly obtain information from computer networks."[22]

Burton continues his analysis by considering the motivations and choice of target of the attacker. This leads to his division of cybersecurity into four main threats and NATO's role in each of them: cyber crime, cyber espionage, cyber terrorism and cyber warfare. The author designates cyber crime as attacks carried out by private individuals or groups against other individuals and businesses, usually in the form of

[20] Most modern military assets are connected to communication networks. This connectivity also refers to the possibility of converting data from the physical domain (thermal, geographical, directional) into the cyber domain. *See:* Even, Shmuel and David Siman-Tov; Rosen, Judith (ed.). 2012. Cyber Warfare: Concepts and Strategic Trends. Memorandum 117. Tel Aviv: Institute for National Security Studies, 16-17.

[21] NATO Cooperative Cyber Defense Centre of Excellence. " Cyber Definitions".

[22] Burton, Joe. 2015. "NATO's cyber defence: strategic challenges and institutional adaptation", Defense Studies, Vol. 15:4, 299.

financial fraud and identity theft.[23]While not a military threat, the sheer financial losses caused by these actions and its exponential growth have made cyber crime a recognized threat to the national security of NATO members. The Alliance itself however is neither a criminal justice body nor a police organization to be able to develop both legal and civil responses required and therefore does not have an active role, relying instead on its member states and international agreements to pursue internal cybersecurity issues.[24]

The cyber realm has also changed the dynamics of espionage: cyber OAAs[25] (Operations, Attacks, Actions) of this type target private businesses and foreign states with the purpose of stealing "sensitive information for commercial, political and military gain.„[26] Although connected to cyber crime[27], cyber espionage is overseen by a state either directly or indirectly. This threat is one of the most relevant of the four as NATO's networks and infrastructure keep sensitive and confidential information that could be used by states outside the organization for political and military gains.[28]According to the Tallinn Manuals, however, peacetime cyber espionage does not *per se* violate customary international law, only the method through which it is pursued might.[29]

Cyber Terrorism is defined as „unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives."[30]

[23] Ibid.

[24] Ibid, 299-300.

[25] The word "attack" in cyberspace is often used as a general term to refer to all kinds of hostile actions, but to avoid any confusion the term "OAA" has been adopted in this thesis to include other expressions that can represent hostile actions in cyberspace. Dr. Richard J. Harknett coined this term in 2017.

[26] Ibid.

[27] Use of criminal/activist groups by a state for cyber OAAs enables the latter to claim plausible deniability.

[28] Ibid.

[29] Schmitt, Michael N.(g.e.). 2017. Tallinn Manual 2.0 On The International Law Applicable To Cyber Operations. Tallinn: Cambridge University Press, 168-174.

[30] D. C., Alexander.2014. "Cyber Threats against the North Atlantic Treaty Organization (NATO) and Selected Responses". Istanbul: Gelisim University Social Sciences Journal, Issue 1, p 3.

NATO members have suffered various forms of terrorism throughout history, even invoking Article 5 of the Washington Treaty in response to the 9/11 attacks. Article 5 exists to enforce NATO's core task of collective defense, and states that an armed attack on any member state constitutes an attack against all Allied nations.[31]

Perhaps the most discussed category, cyber warfare has seen renewed prominence since cyberspace was declared an operational domain by NATO in 2016.[32]Burton stresses that despite the debate surrounding the term itself, it is the political nature of the cyber attacks against NATO and the involvement of foreign states that distinguishes the term from other online activity.[33] Stephen Walt attempts to bypass this debate by separating different dangers grouped under the term itself. Walt distinguishes four issues in his work: cyber espionage, degradation of enemy military capabilities, shutdown of civilian infrastructure by network penetration and web-based criminal activity.[34] Following Walt's footsteps, Gartzke states that this division helps to „frame cyber warfare as an evolving, nuance set of issues, each amenable to its own cost-benefit analysis."[35]NATO forces have been deployed into several conflicts throughout the post-cold war era, and cyber operations are increasingly becoming an integral part of modern conflicts. As a military organization, NATO's priority role in cyberspace during a conflict would be the protection of its military networks and assistance to allied networks.

It is important to note that while cybersecurity is an area of great interest for NATO, the Alliance does not practice cybersecurity in its totality. In an effort to address

[31] North Atlantic Treaty Organization. The North Atlantic Treaty. Washington D.C.: North Atlantic Treaty Organization, 1949, 1.

[32] North Atlantic Treaty Organization. Last updated: 16 Jul. 2018. "Cyber Defence".

[33] Burton, Joe. 2015. "NATO's cyber defence: strategic challenges and institutional adaptation", Defense Studies, Vol. 15:4, 300-301.

[34] Walt, Stephen M. 2010. "Is the Cyber Threat Overblown?" Foreign Policy.

[35] Gartzke, Erik. 2013. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth". Massachusetts: International Security, Vol. 38:2, MIT Press, 49.

cyber threats as a defensive organization, NATO practices cyber defense. Just as with previous concepts, several definitions exist and the CCDCOE database covers a number of them.[36] If one skips the conceptual debate, the practice of cyber defense in NATO encompasses the concentration of the organization's efforts in cybersecurity into effective defenses[37] through prevention and resilience in cyberspace, two key components that add to NATO's strategic approach of deterrence by denial. NATO's path is reflective of the Alliance's commitment to legal principles and the rule of law, as well as the complex legal ecosystem through which its cyber activities have to navigate through.[38] In a joint work that analyses the implementation of Croatia's 2015 cybersecurity Strategy and Action Plan, Galinec states that cyber defense “focuses on preventing, detecting and providing timely responses to attacks or threats so that no infrastructure or information is tampered with.”[39] NATO's strategic approach in cyberspace will be discussed with greater detail in chapter three of this thesis.

What NATO classifies as cyber defense can be seen as the partial practice of the field of cybersecurity. The SANS (SysAdmin, Audit, Network, Security) Institute's scaling model created by analyst Robert Lee provides a clear and practical explanation of this view.[40]“The Sliding Scale of Cybersecurity” serves as a framework to discern what actions contribute to cybersecurity. The model is structured into five categories: architecture, passive defense, active defense, intelligence, and offense. Architecture

[36] The most complete is Belgium's definition of cyber defense: "the application of effective protective measures to obtain an appropriate level of Cybersecurity in order to guarantee defensive operations and functionalities. This is achieved by applying appropriate protective measures to reduce the security risk to an acceptable level. Cyber Defense consists of following duties: Protect, Detect, Respond, and Recover." In: NATO Cooperative Cyber Defense Centre of Excellence. " Cyber Definitions".

[37] P. Fidler, David; Pregent, Richard and Alex Vandurme. 2013. "NATO, Cyber Defense, and International Law". Indiana: Articles by Maurer Faculty, Paper 1672, 13.

[38] Ibid.

[39] Galinec, Darko; Moznik, Darko and Boris Guberina. 2018. "Cybersecurity and cyber defence: national level strategic approach". London: Informa UK Limited. Automatika vol. 58:3, 274.

[40] As a discussion surrounding this model and cyber defense/security goes beyond the scope of this thesis, this paragraph is meant to help the reader differentiate different aspects within cybersecurity.

involves the “planning, establishing and upkeep of systems with security in mind.”[41] Passive defense refers to any systems added to the previous category that provide a reliable defense without continuous human interaction (high level of automation). Active defense[42] includes major human interaction through monitoring for intrusions, response to an attack and learning from previous incidents, all of this within the defendant's own network. Intelligence, as the name suggests, consists in the collection data from previous incidents and production of assessments that fill identified knowledge gaps, and is crucial to active defense. The final element - offense - is a key term in this thesis. According to the model, offense represents direct action against an adversary outside the defendant's network and can be undertaken for reasons other than cybersecurity, such as an ongoing conflict or national policy. Within the context of cybersecurity, offensive actions must respect both national and international laws when applicable, and so the SANS analyst defines them as “legal countermeasures and counterstrike actions taken against an adversary outside of friendly systems for the purpose of self-defense.”[43] The term 'cyber offensive capabilities' - often mentioned in this thesis - refers to these legal countermeasures and specific counterstrike tools that enable the disruption or even destruction of the intruder's network.[44]

NATO's cybersecurity efforts through cyber defense can be seen to some extent in the first four categories of the SANS Institute model. The architecture is established as a pre-requisite and therefore present, while both defense categories can be represented by the NATO Computer Incident Response Capability (NCIRC), the organ within NATO that is tasked with protecting the organization’s own networks. Following

[41] Lee, Robert M. 2015. "The Sliding Scale of Cybersecurity". SANS Analyst Whitepaper. Swansea: SANS Institute, 5.

[42] Lee considers that this term is misused due to attempts to apply concepts from traditional warfare into cyberspace and by extension to cybersecurity, such as 'counterattack' for 'hack-back'.

[43] Ibid, 18-19.

[44] Specific examples cannot be given due to the sensitive nature of cyber capabilities.

the SANS model, the NCIRC employs both passive (autonomous detection systems) and active (rapid reaction teams, analysts) defense in cyberspace. The intelligence element is present through NATO's CCDCOE and multiple partnerships with the purpose of sharing information and technical aid.[45]

[45] North Atlantic Treaty Organization. 2016. "NATO Cyber Defense".

2. The Offense vs. Defense Discourse in Cyberspace

The perception that a determined security environment is better suited to the offensive side or the defensive side can be traced back to the 1930s League of Nations discussions on limiting arms[46] and further back to the First World War, where overconfidence in the advantages of offense created a „cult of offensive" and resulted in one of the bloodiest conflicts in History.[47] Originally introduced in the 1970's by Robert Jervis and George Quester, the Offense-Defense Theory asserted that the „orientation of different military capabilities and weaponry systems may influence interstate security dilemmas[48] and therefore the prevalence of war or peace."[49] This theory has since then been heavily criticized for not properly distinguishing the offensive and defensive natures of military capabilities, spurring various attempts to improve it. Analysts Charles Glaser and Chaim Kaufmann wrote in 1998 what would become the dominant interpretation in academic literature[50]: that the cornerstone of the theory (the offense-defense balance) should be considered as the „ratio of the cost of the forces the attacker requires to take territory to the cost of the forces the defender has deployed."[51] This view takes into consideration two major factors that can alter the costs and tilt the

[46] Slayton, Rebecca. 2017. "What is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment". Massachusetts: MIT Press. International Security, Vol. 41:3,

[47] Evera, Stephen Van. 1984. "The Cult of the Offensive and the Origins of the First World War". Massachusetts: MIT Press. International Security, Vol. 9:1, 58-107.

[48] Term coined by John Herz in 1950 in which a state's efforts to increase their security threatens other states, prompting them to do the same and beginning a dangerous sequence of events. *In* Herz, John H. 1950. "Idealist Internationalism and the Security Dilemma". Princeton: Cambridge University Press. World Politics, Vol. 2:2, 157-180.

[49] Saltzman, Ilai. 2013. "Cyber Posturing and the Offense-Defense Balance", Contemporary Security Policy, Vol. 34:1, 42.

[50] Ibid.

[51] Glaser, Charles L. and Chaim Kaufmann. 1998. "What is the Offense-Defense Balance and Can We Measure it?". Massachusetts: MIT Press. International Security, Vol. 22:4, 50.

balance, those being geography (terrain, obstacles, mobility)and technology (degree of destructiveness of capabilities).[52]

These factors follow the presumption that conflict develops according to a territorial logic and kinetic basis, making them to some extent obsolete when the cyber offense-defense balance. Cyberspace does not have defined territory or borders in the same way as the physical domain, there is no physical mobility, and cyber capabilities are too divergent from conventional weapons to be approached in a similar fashion.[53] Several academics have tried to address this issue in recent years by adapting the theory's conceptual basis, with a focus on technological affordances.[54] Instead of geographical and technological aspects such as mobility and firepower, Satzman argued that the versatility derived from the interconnectivity in critical infrastructure and the degree of technological damage that can be inflicted should be the deciding factors.[55]

2.1 Does Cyberspace Favor an Offensive or Defensive Approach?

Saltzman's assessment lead him to conclude that „cyber capabilities tilt the Offense-Defense balance in favor of the offense".[56] Former US Deputy Secretary of Defense William Lynn cemented in 2010 what remains as conventional wisdom[57] regarding cybersecurity among policy makers, scholars and military officials alike: "In cyberspace, the offense has the upper hand."[58] Only a minority of scholars contest this

[52] Buchanan, Ben. 2017. The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations. New York: Oxford University Press, 103-106.

[53] Saltzman, Ilai. 2013. "Cyber Posturing and the Offense-Defense Balance", Contemporary Security Policy, Vol. 34:1, 42-43.

[54] Slayton, Rebecca. 2017. "What is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment". Massachusetts: MIT Press. International Security, Vol. 41:3, 82.

[55] Saltzman, 43-45.

[56]Ibid, 44.

[57]Slayton, 72.

[58] Lynn, William J. 2010. "Defending a New Domain: The Pentagon's Cyberstrategy", Foreign Affairs, Vol. 89:5, 98.

offensive orientation however and have argued that cyberspace may favor defense. Most arguments in favor of offense revolve around the features of the technology itself: the attribution problem, the ease of use, and the inevitable existence of software vulnerabilities. The attribution problem can be summed up in William Lynn's words:

> „Whereas a missile comes with a return address, a computer virus generally does not. The forensic work necessary to identify an attacker may take months, if identification is possible at all."[59]

Even if the forensic work is successful and the geographical source of an Internet Protocol (IP) address is obtained, there is still no certainty as to who the perpetrators are and if they acted on their own behalf.[60] This remains a key issue due to the borderless nature of the Internet, as well as the need for public acceptance of evidence and methods used to obtain it. US Navy Lieutenant Commander Z'hra M. Ghavam gives a practical example in his postgraduate thesis:

> „If a website that contains malware is owned in China but has a Polish address and a Danish host, holding the proper party accountable becomes a daunting challenge."[61]

Legal complications aside, if either the evidence acquired or the means used remain classified, security experts and the international community alike may be skeptical of the attribution's accuracy. The state from which the attackers operated can thus easily deny responsibility, and any punitive responses may risk escalation.[62]The 2007 attacks on Estonian websites, for example, were traced back to Russia, and while Estonian authorities argue that the Kremlin was directly involved, no publicly accepted

[59] Ibid, 99.

[60] Ghavam, Z'hra M. 2016. "NATO's Preparedness For Cyberwar". Master Thesis, Naval Postgraduate School, Monterey, 28.

[61] Ibid.

[62] Edwards, Benjamin; et al. 2017. "Strategic aspects of cyberattack, attribution, and blame", Proceedings of the National Academy of Sciences of the United States of America, Vol. 114:11, 2825-2830.

evidence exists to this day.[63] While not directly affecting the balance, the difficulty in attributing OAAs in cyberspace encourages offensive behavior, as adversaries are much more likely to strike if the ability to retaliate is remote.

The 'ease of use' refers to the low costs of entry and operation at a skill and financial levels for the offensive actor when compared with the defender. While the defense must account for all possible venues of attack, offense only needs to find a single route to explore those defenses. The increasing number of cyber OAAs carried out by none-state actors also supports the notion that one does not require state-level resources to produce results that threaten even great powers.[64] As Martin Libicki from RAND put it, „another dollar's worth of offense requires far more than another dollar's worth of defense to restore prior levels of security".[65]

A vulnerability can be considered as „an aspect of the IT that can be used to compromise it (...) accidentally introduced through a design or implementation flaw, or introduced intentionally"[66], and fall into two categories: zero day vulnerabilities (not discovered prior to its use) and known vulnerabilities (fixed once software is updated).[67] Most network intrusions rely on these vulnerabilities to be present within the adversary's software, and while defenders constantly attempt to find and fix them, it's technically impossible to rule out flaws in constantly evolving software designs.[68] The significant advantage these exploits might seem to give is often a short-lived one, as once a vulnerability is used or revealed, other actors will update their network defenses

[63] Locatelli, Andrea. 2013. "The Offense/Defense Balance In Cyberspace". Milano: Istituto per gli Studi di Politica Internazionale, Analysis No. 203, 9.

[64] Knapp, Kenneth and William Boulton. 2006. "Cyber-Warfare Threatens Corporations: Expansion to Commercial Environments" Information Systems Management Journal, Vol. 23:2, 76-87.

[65] Libicki, Martin C. 2009. Cyberdeterrence and Cyberwar. Santa Monica: Research ANd Development Corporation (RAND), 32.

[66] Lin, Herbert. 2014. "Cyber Conflict and National Security", In: Art, Robert J. and Robert Jervis (Eds.). International Politics: Enduring Concepts and Contemporary Issues. Pearson. Boston: Pearson 12th Edition, 476-489.

[67] Buchanan, Ben. 2017. The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations. New York: Oxford University Press, 105-106.

[68] Locatelli, Andrea, 8.

accordingly for the most part. There is also the possibility that either the defender or the relevant software vendor discover the vulnerability and patch it, rendering the potential offensive opportunity useless. Actors with zero days are, thus pressured, to use „their advantage in intrusion while they have it - a spur to action that negatively affects stability."[69]

The perspectives above have been recently contested by Rebecca Slayton who argues that technology, skill and organizations are inseparable variables in cyberspace, and therefore the balance, should be accessed in terms of utility through a cost-benefit analysis.[70] Unlike the physical domains, in cyberspace „the skills are the weapon."[71] According to Slayton, this means that the cost and utility of cyber OAAs do not rely solely on the features of the technology, but also on the skills and coordination of the actors and organizations that develop, modify and deploy said technology. Most of the concepts that seem to favor the offense depend on the integration and organization of skilled actors and what Slayton calls complexity.

Rapidly changing technology means the complexity and size of ICT systems are constantly increasing to enable new functionalities, and the number of vulnerabilities grows with these advances. Protection of complex systems is „difficult to do well and impossible to do cheaply: The defender has to counter all possible attacks; the attacker only has to find on unblocked means of attack"[72], leading to the prospect of an offensive advantage.[73] These vulnerabilities however are finite and being constantly patched, and

[69] Buchanan, Ben. 2017. The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations. New York: Oxford University Press, 106.

[70] Slayton, Rebecca. 2017. "What is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment". Massachusetts: MIT Press. International Security, Vol. 41:3, 75.

[71] Allan Paller, SANS Institute. Quoted in Slayton, Rebecca, 75.

[72] Geer, Daniel; et al. 2003. "Cyber*in*security: The Cost of Monopoly—How the Dominance of Microsoft's Products Poses a Risk to Security". Independent Report published by the Computer and Communication Industry Association.

[73] Slayton, Rebecca. 2017. "What is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment". Massachusetts: MIT Press. International Security, Vol. 41:3, 87-90.

the more complex a system becomes, the harder it is for the adversary to navigate through it and establish an attack vector.[74] The defender on the other hand has complete access to its systems, and while it is impossible to find and fix every vulnerability before an adversary finds one, effective management and cybersecurity processes can prevent the attacker from fully exploiting it.[75] Slayton's own analysis led her to conclude that the offense-defense balance is highly contextual, meaning that „specific adversaries with distinctive goals and levels of capability in managing complex information technology"[76] must be taken into account. Slayton's claim is supported by Lindsay: „Cyberspace as an operational domain is highly sensitive to technological expertise and the ability to plan, coordinate, and execute complex operations, suggesting that factors other than technology should be at least as critical, and possibly even more important, in shaping the offense-defense balance in cyberspace."[77]

Determining the offense-defense balance of cyberspace goes far beyond the scope of this thesis. This chapter points out that despite the dominant perspective of offensive superiority in cyberspace, such an advantage is highly contextual and susceptible to factors outside the capabilities themselves. Taking both sides of the debate into consideration, offensive advantage in cyberspace seems to be a perception stemming from mainly technological advantages that is proving to destabilize the international environment.

[74] Buchanan, Ben. 2017. The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations. New York: Oxford University Press, 103-106.

[75] Slayton, Rebecca. 2017. "Why Cyber Operations Do Not Always Favor the Offense". Massachusetts: MIT Press. International Security, Policy Brief Issue February 2017, 3-4.

[76] Slayton, Rebecca. 2017. "What is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment". Massachusetts: MIT Press. International Security, Vol. 41:3, 106.

[77] Lindsay, Jon R. and Erik Gartzke. 2015. "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace". Security Studies, Vol. 24:2, 325.

3. NATO Cyber Posture

The importance of cyberspace as an emerging security concern for NATO became evident following the cyber-attacks the Alliance suffered during the 1999 Kosovo Operation Allied Force[78]. While the perpetrators did not manage to acquire any sensitive information nor disrupt NATO operations, the event drove NATO to include later that month in its Strategic Concept that “state and non-state adversaries may try to exploit the Alliance's growing reliance on information systems through information operations designed to disrupt such systems. They may attempt to use strategies of this kind to counter NATO's superiority in traditional weaponry.”[79]

NATO only began to specifically mention cyber warfare during its Prague Summit in 2002.[80] The creation of the NATO NCIRC as a part of the NATO Communication and Information Service Agency represented one of the most decisive outcomes of the summit. Even so, this technical center - tasked with protecting Information and Communication Technology (ICT) infrastructure - lacked any “long-term military planning capacity”[81] and was limited to the Alliance's own networks, leaving the protection of allied systems to the sole responsibility of its member states. Heads of state and government of the NATO member countries declared in the Prague Summit that they would improve their „capabilities to defend against cyber attacks”[82], however few steps were taken beyond the declaration itself. NATO's progress in the

[78] Healey, Jason and Leendert Van Bochoven. 2011. "NATO’s Cyber Capabilities: Yesterday, Today, and Tomorrow". Washington, DC: Atlantic Council, 1.

[79] Saltzman, Ilai. 2013. “Cyber Posturing and the Offense-Defense Balance", Contemporary Security Policy, Vol. 34:1, 53.

[80] Ibid.

[81] Ibid.

[82] North Atlantic Treaty Organization. Prague Summit Declaration. Brussels: North Atlantic Treaty Organization, 2002.

cyber domain remained under the radar up until the 2006 Riga Summit[83], in which NATO expressed its will to develop a Network Enabled Capability (NEC) to share intelligence and data in a reliable and secure way, and called for further development of cyber capabilities and doctrines.[84] Again, beyond the scope of its declarations NATO's cyber defense policy did not register any major changes from 2002 until 2007.

The year 2007 became an indisputable turning point in NATO's cyber posture. As Gergely Szentgáli (Defence Policy Officer, Ministry of Defence, Hungary) stated in 2013, the cyber attacks against Estonia were the first operational example of the potential reality of cyber war and highlighted the importance of cybersecurity in the eyes of many political and military leaders.[85] Gergely and Saltzman agree that while the event failed to trigger Article 5 (despite Estonia requesting NATO emergency assistance), it generated a strong institutional response: during the meeting of defense minister of the member states two months later it was agreed to unify cybersecurity efforts of the allied members.[86] In January 2008 the Cyber Defense Policy was accepted and introduced within the Alliance in an effort to coordinate this commitment, representing its first official framework on cybersecurity. Following the Bucharest Summit that same year - in which member countries agreed that „the relationship between NATO and the national authorities on cyber defense should be enhanced, the experiences of the member states regarding cyber issues should be shared"[87] - NATO established the CCDCOE and the Cyber Defense Management Authority (CDMA). The CCDCOE, set up in Estonia, was designed to act as a research and educational center,

[83] Caton, Jeffrey L. 2016. NATO Cyberspace Capability: A Strategic and Operational Evolution. Strategic Studies Institute and U.S. Army War College Press, 2.

[84] North Atlantic Treaty Organization. Riga Summit Declaration. Riga: North Atlantic Council, 2006.

[85] Szentgáli, Gergely. 2013. "The NATO Policy on Cyber Defense: The Road so Far". AARMS Vol. 12:1, 83.

[86] Ibid; Saltzman, Ilai. 2013. "Cyber Posturing and the Offense-Defense Balance", Contemporary Security Policy, Vol. 34:1, 54.

[87] Canbolat, Mustafa and Emrah Sezgin. 2016. "Is NATO Ready For a Cyber War?". Master Thesis, Naval Postgraduate School, Monterey, 49.

and its responsibilities include helping member countries develop their own cyber capabilities, providing training sessions and assisting in the elaboration of doctrines, legal framework and strategies. On the other hand, the CDMA was tasked with overseeing cyber defense efforts at both a centralized level and individual member level, as well as responding to attacks directed at the organization and/or its members.[88]

Saltzman, however, argues that even though the 2007 attacks exposed NATO's cyber deficiencies at a military, political and infrastructural level, NATO's response and the consequent establishment of the agencies mentioned above was an almost exclusively defensive move, focusing only the protection of critical systems and capability to assist Allied nations upon request in countering a cyber attack.[89] The August 2008 Russian-Georgian conflict showed again the growing importance of information operations and cyber warfare along with its escalatory nature. Although the cyber attacks against Estonia and Georgia are the most visible examples of the evolving cyber threat, they were not remote in any way. Other serious incidents against NATO members, such as the intrusion of Chinese hackers within the networks of the German Chancellery and three other Ministries in August 2007, a coordinated cyber espionage campaign by the Chinese military against British businesses in November 2007, and the series of cyber attacks suffered by Lithuania in June 2008 due to vetoing an EU energy partnership deal with the Russian Federation, helped raise the growing importance of cybersecurity during this time.[90] This rising threat in cyberspace prompted NATO to

[88] Ibid.

[89] Saltzman, Ilai. 2013. “Cyber Posturing and the Offense-Defense Balance", Contemporary Security Policy, Vol. 34:1, 54.

[90] Burton, Joe. 2015. "NATO's cyber defence: strategic challenges and institutional adaptation", Defense Studies, Vol. 15:4, 306-307.

classify cyber attacks as one of several key global threats to the international community, but little further progress was made.[91]

Such progress seemed to return during the Lisbon Summit: NATO adopted a new Strategic Concept in which it included the cybersecurity issue as one among the most important emerging security challenges.[92] According to the summit declaration

> „In order to ensure NATO's permanent and unfettered access to cyberspace and integrity of its critical systems, we will take into account the cyber dimension of modern conflicts in NATO's doctrine and improve its capabilities to detect, assess, prevent, defend and recover in case of a cyber attack against systems of critical importance to the Alliance. (...) promote the development of Allies' cyber defence capabilities, to assist individual Allies upon request, and to optimise information sharing, collaboration and interoperability."[93]

Saltzman observed that NATO maintained the same defensive reasoning at this point[94]. Most points stated in the 2008 Cyber Policy remained adamant, and NATO's cyber capabilities to „detect, assess, prevent, defend and recover" when facing cyber attacks can be seen as static defenses[95], reminiscent of a cyber Maginot Line. While the Alliance reiterated its continued focus on defensive improvements[96], the „numerous references to cyber warfare as a security threat were extremely narrow"[97], avoiding any discussions on active defense and offensive capabilities. The Summit did however enable a major call for NATO to work more closely with the EU on cyber defense issues. Both constant targets of cyber attacks, cooperation between these two

[91] Szentgáli, Gergely. 2013. "The NATO Policy on Cyber Defense: The Road so Far". AARMS Vol. 12:1, 83.

[92] Rühle, Michael. 2011. "NATO and Emerging Security Challenges: Beyond the Deterrence Paradigm". American Foreign Policy Interests, Vol. 33:6, 281.

[93] North Atlantic Treaty Organization. Lisbon Summit Declaration. Brussels: North Atlantic Treaty Organization, 2010.

[94] Saltzman, Ilai. 2013. "Cyber Posturing and the Offense-Defense Balance", Contemporary Security Policy, Vol. 34:1, 54.

[95] Lee, Robert M. 2015. "The Sliding Scale of Cybersecurity". SANS Analyst Whitepaper. Swansea: SANS Institute, 9.

[96] Healey, Jason and Leendert Van Bochoven. 2011. "NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow". Washington, DC: Atlantic Council, 2.

[97] Saltzman, Ilai; 54.

organizations would bring significant advantages to both.[98] Two years later at the Chicago Summit, NATO once more underscored its commitment to improving its cyber defense capabilities through the implementation of more appropriate procedures and structures for cooperation and interoperability between member states. The importance of collaboration with other relevant institutions such as the UN, the EU and OSCE was also highlighted.[99]

The Wales Summit, held in 2014, centered on the adoption of a new Cyber Defense Policy and action plan. A refined version of its predecessor, the NATO Enhanced Cyber Defense Policy officially linked cyber into the Alliance's core task of collective defense and supported the application of international law to cyberspace. The Policy however did not set any detailed criteria or threshold for the activation of Article 5, instead reiterating that in the event of a cyber attack, Allied nations are expected to be able to defend their own system and requests for activating Article 5 would be decided on a case-by-case basis.[100]A more significant outcome of this summit was the NATO Industry Cyber Partnership (NICP), the result of a two-day conference in which industry leaders and policy makers that brought a much needed closer cooperation between NATO and the private sector on „the evolving cyber threat"[101]. Through this initiative, NATO recognized the „importance of working with industry partners to enable the Alliance to achieve its cyber defense policy's objectives."[102] The decisions made during

[98] Canbolat, Mustafa and Emrah Sezgin. 2016. "Is NATO Ready For a Cyber War?". Master Thesis, Naval Postgraduate School, Monterey, 53.
[99] Caton, Jeffrey L. 2016. NATO Cyberspace Capability: A Strategic and Operational Evolution. Strategic Studies Institute and U.S. Army War College Press, 4-12.
[100] NATO Cooperative Cyber Defense Center of Excellence. 2014. "International Cyber Developments Review" Tallinn: Incyder news.
[101] North Atlantic Treaty Organization. Last updated: 16 Jul. 2018. "Cyber Defence".
[102] Ibid.

the Wales Summit can be seen as „the culmination of the policy debate that was started within NATO by the attacks against Estonia in 2007."[103]

While NATO had already come far from its state before the 2007 cyber attacks against Estonia, the organization took its first large step towards the possibility of any use of offensive cyber capabilities during the 2016 Warsaw Summit. A topic long avoided by NATO due to treading „on a range of sensitive political issues that militate against any change in policy in the near term"[104], such capabilities can be considered as tools used outside of the Alliance's own defensive network to neutralize specific internet nodes that are enabling or enabled attacks or in support of NATO defensive operations. Cyber expert Dr. James Lewis had already addressed this issue in the Tallinn Papers in 2015, stating that"[t]he central question for NATO's cyber doctrine is how the lack of an articulated offensive cyber capability affects its ability to deter or defend."[105]

In the document, Lewis goes on to state that failure to add such capabilities to NATO in the near future would not just erode the Alliance's deterrent potential but also deprive it from essential tools that were being increasingly integrated into larger operations. The author adds that NATO would feel increasing pressure to consider offensive capabilities as potential opponents were already beginning to use such tools themselves in new ways, such as hybrid warfare.[106] This view had been previously present within the NATO ranks before the release of the document mentioned above, as one NATO cyber officer admitted in 2014 that "NATO has established a capable

[103] Burton, Joe. 2015. "NATO's cyber defence: strategic challenges and institutional adaptation", Defense Studies, Vol. 15:4, 308.
[104] Lewis, James A. 2015. "The Role of Offensive Cyber Operations in NATO's Collective Defense". Tallinn Paper No. 8. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2.
[105] Ibid.
[106] Ibid, 3.

defense for most cyber threats, but that is just the first step and what needs to quickly follow is the development of active defense capabilities."[107]

The recognition of cyberspace as the fifth domain of operations at the Warsaw Summit in June 2016 placed this area at the same level as land, sea, air and space. While this move did not alter the organization's defensive mission nor its commitment to international law in any way, it sent a statement to the international community that NATO will defend itself as effectively as it did in any other domain while still avoiding escalation and respecting international law, opening the door to the possible introduction of active defenses and offensive cyber operations in the future.[108]In December that year NATO and the EU considerably bolstered their cooperative measures in cybersecurity, from increased participation in exercises to research support, training and information-sharing.[109]

On February 2017, the Cyber Defense Action Plan was updated and a roadmap was agreed to implement the Warsaw Summit's declaration of elevating cyberspace to a domain of operations[110], paving the way to the most decisive policy shift in NATO's cyber posture in decades.

> „On 8 November 2017, defense ministers expressed their agreement in principle on the creation of a new Cyber Operations Centre as part of the outline design for the adapted NATO Command Structure. This will strengthen NATO's cyber defenses, and help integrate cyber into NATO planning and operations at all levels. Ministers also agreed to allow the integration of Allies' national cyber contributions into Alliance operations and missions. Allies will maintain full ownership of those contributions, just as Allies own the tanks, ships and aircraft in NATO missions."[111]

[107] Caton, Jeffrey L. 2016. NATO Cyberspace Capability: A Strategic and Operational Evolution. Strategic Studies Institute and U.S. Army War College Press, 27.

[108] North Atlantic Treaty Organization. Last updated: 16 Jul. 2018. "Cyber Defence".

[109] Ibid.

[110] Ibid.

[111] Ibid.

During the press conference that followed the defense ministers meeting, NATO Secretary General announced „the creation of a new Cyber Operations Centre as part of the outline design for the adapted NATO Command Structure. This will strengthen our cyber defenses, and help integrate cyber into NATO planning and operations at all levels. We also agreed that we will be able to integrate Allies' national cyber capabilities into NATO missions and operations."[112]

Later that same month, US Navy Commander Michael Widmann stated at the NATO CCDCE that "There's a change in the [NATO] mindset to accept that computers, just like aircraft and ships, have an offensive capability"[113]. This shift has since become more noticeable: an agreement was reached in February this year between defense ministers of the NATO member countries as to the location of the new Cyber Operations Center. The chosen location was theNATO Supreme Headquarters Allied Powers Europe(SHAPE)in Belgium.[114]

NATO's Cyber Defense Strategy is turning towards the use of offensive capabilities as part of their collective defense apparatus, and a number of NATO's member states (United States, United Kingdom, Germany, Spain, Norway, Netherlands, Denmark) are also in the process of developing a series of guiding cyber warfare principles to enable and justify the deployment of offensive cyber capabilities more broadly, and hope to have reached an agreement by 2019.[115] Despite this progress, the Alliance's strategy currently still remains heavily focused on defense by deterrence[116].

[112] North Atlantic Treaty Organization. November 2017. "Press conference by NATO Secretary General Jens Stoltenberg following the meeting of the North Atlantic Council at the level of Defence Ministers".

[113] Emmott,Robin. 2017. "NATO mulls 'offensive defence' with cyber warfare rules".[NATO CCDCE Head of Strategy Michael Widmann, interview with REUTERS], REUTERS.

[114] North Atlantic Treaty Organization. Last updated: 16 Jul. 2018. "Cyber Defence".

[115] NATO CCDCE Head of Strategy Michael Widmann, In Emmott,Robin. 2017. "NATO mulls 'offensive defence' with cyber warfare rules".[NATO CCDCE Head of Strategy Michael Widmann, interview with REUTERS], REUTERS..

[116] Burton, Joe. 2015. "NATO's cyber defence: strategic challenges and institutional adaptation", Defense Studies, Vol. 15:4, 304-308.

Based on the approach of total deterrence that was so successful in the nuclear realm, it remains entrenched within policy makers' minds when facing threats in cyberspace.

3.1 NATO's Shortcomings

Focusing on the threat of punishment, the UK's National Security Strategy (NSS) document of 2015 already declared that the state would treat a cyber attack against it as seriously as an equivalent conventional attack, and would defend itself accordingly.[117] The United States made its own deterrence statement as part of its International Strategy for Cyberspace:

> „When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners. We reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests."[118]

The U.S. statement explicitly includes the protection of allies, which puts NATO under the U.S. cyber deterrence umbrella. This notion is also present in NATO's own reports, in which it is stated that a major action in cyberspace that meet the threshold equivalent of an armed attack could warrant a collective response by its member states against the perpetrator.[119] The logic behind the promise of reprisal in the physical domain to prevent a threat in the cyber domain is well understood: it influences „adversary's cost/benefit calculus so that it concludes that the costs of challenging the

[117]Her Majesty's Government. 2015. National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom. London: HM Government.

[118] Caton, Jeffrey L. 2016. NATO Cyberspace Capability: A Strategic and Operational Evolution. Strategic Studies Institute and U.S. Army War College Press, 28-29.

[119] Lucas Kello, Lucas. 2017. The Virtual Weapon and International Order. New Haven: Yale University Press, 199.

status quo outweigh the benefits."[120] NATO's stance is defensive however, and its doctrine focused accordingly in deterrence by denial. In cyberspace, deterrence by denial works by consuming the attacker's resources and time, which are limited, and exponentially increasing the costs up to the point of disruption of the balance in the adversary's cost-benefit analysis.[121] This has the added benefit of increasing the risk for the attacker of being detected. Both punishment and denial are stated as part of the NATO Cyber Defence Policy according to the organization's 2011 Issue Brief:

> „Defenses before an attack, and responses after, should be effective enough so that potential adversaries know they may not be able to achieve their intended effects. The strong (...) measures (...) can, if implemented, be a strong deterrent, denying benefits to potential adversaries (...) The Alliance may also achieve deterrence by punishment".[122]

This focus has been considered appropriate due to the Alliance's reluctance towards using offensive cyber capabilities.

The use of offensive cyber capabilities within the context *Ius in bello* is addressed in the Tallin Manual 2.0, which states that cyber OAAs that result in death or injury of individuals or destruction or damage of objects could invoke Article 5.[123] Even so, the group of experts that developed the manual couldn't agree whether the Stuxnet virus - which caused physical damage to Iranian centrifuges - constituted an armed attack.[124]

Current NATO deterrence policy does not seek to prevent only sophisticated cyber attacks, but also sub-threshold events. NATO Assistance Secretary General for

[120] Harknett, Richard J. and Michael P. Fischerkeller. 2017. "Deterrence is Not a Credible Strategy for Cyberspace", Orbis, Vol. 61:3, 385.

[121] Nye Jr., Joseph S. 2017. "Deterrence and Dissuasion in Cyberspace", Massachusetts: MIT Press, International Security, Vol. 41:3, 56-57.

[122] Healey, Jason and Leendert Van Bochoven. 2011. "NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow". Washington, DC: Atlantic Council.

[123] Schmitt, Michael N.(g.e.). 2017. Tallinn Manual 2.0 On The International Law Applicable To Cyber Operations. Tallinn: Cambridge University Press, 339.

[124] Jasper, Scott. 2017. Strategic Deterrence: The Active Cyber Defense Option. New York: Rowman & Littlefield, 14.

Emerging Security Challenges Ducaru stated during an interview that “[it] applies also to sub-threshold action - not just scenarios that unambiguously meet the criteria of Article 5”[125]. Dealing with attacks that do not meet the Alliance's criteria is not a straight forward task however, as different actors have different thresholds tolerance. [126]

Lucas Kello calls the application of the core principles of *ius in bello* to cyber conflict by leading public officials into question. The promise of a cross domain retaliation equivalent to the attack suffered can reduce the probability of falling victim to a major high-end cyber operation. The same pledge increases the chances of a cyber attack up to that threshold line, as attackers will not fear a severe reprisal as long as their actions retain a lower intensity.[127] Regarding the denial approach, Joseph Nye, warned that although „better defenses and cyber hygiene can enhance deterrence by allowing the government to focus on advanced persistent threats[128] (...) the need for other methods of deterrence and resilience remains, however”.[129] In her NATO Defense College research paper, Christine Hegenbart called for the development of appropriate and decisive language to better devise steps in a cyber conflict escalation ladder with a spectrum from hacktivism/cyber vandalism all the way up to cyber war.

It is clear that NATO has continuously avoided approaching the themes of cyber warfare and offensive capabilities due in great part to the conflict between the debated legal principles that surround both concepts and the Alliance’s own defensive nature and commitment to the rule of law. The increasing number of attacks and incidents in

[125] Kello, Lucas. 2017. The Virtual Weapon and International Order. New Haven: Yale University Press, 202-206.

[126] Caton, Jeffrey L. 2016. NATO Cyberspace Capability: A Strategic and Operational Evolution. Strategic Studies Institute and U.S. Army War College Press, 29.

[127] Kello, Lucas. 2017. The Virtual Weapon and International Order. New Haven: Yale University Press, 202-206.

[128] APT (Advanced Persistent Threat) is a term for a new type of threat in cyberspace that stealthily uses multiple attack techniques and vectors at once to retain control over target systems over a long period of time. In Tankard, Colin. 2011. "Advanced Persistent Threats and how to monitor and deter them", Network Security, Vol. 2011:8, 16-19.

[129] Nye Jr., Joseph S. 2017. "Deterrence and Dissuasion in Cyberspace", Massachusetts: MIT Press, International Security, Vol. 41:3, 57.

recent years have made NATO reconsider its position and view offensive cyber capabilities under a different light. Despite such progress, NATO still lacks a proper strategy for the use of these capabilities, and its approach to cybersecurity remains insufficient.

4. Strategic Analysis: The Lykke Model

In order to formulate a strategy and discuss strategic value within the context of this thesis, the term *strategy* and its field of study must be understood. The meaning of this term has been the subject of an exhaustive academic debate, from the military sphere to business and medicine. With NATO being an intergovernmental military alliance, the focus falls onto the military sphere of strategy., but also includes multiple nonmilitary aspects.

Renowned contributors to Strategic Studies have had differing views on what the term entails. Clausewitz stated that "Strategy is the use of the engagement for the purpose of the war. The strategist must therefore define an aim for the entire operational side of the war that will be in accordance with its purpose."[130] Although Clausewitz's work has strongly influenced modern military strategy, his definition is insufficient as „it deals only with the military element and is at the operational level rather than the strategic"[131]. British military historian Basil H. Liddel Hart attempted to provide a more modern concept of strategy to face the growing expansion of nonmilitary aspects and defined it as „the art of distributing and applying military means to fulfill the ends of policy."[132]Henry Eccles described strategy as „the comprehensive direction of power to control situations and areas in order to attain objectives".[133]

The concept, however, remains vague and must be narrowed to the context of this paper. For this reason, the thesis makes use of Starr's definition of cyberstrategy. In

[130] Howard, Michael (g.e.) and Peter Paret (g.e.). 1976. Carl Von Clausewitz. On War. Princeton: Princeton University Press, 177.

[131] Júnior, J. Boone Bartholomees. 2008. "A Survey of The Theory of Strategy", in: Júnior, J. Boone Bartholomees (g.e.). U.S. Army War College Guide to National Security Issues. Volume I: Theory of War and Strategy, 3rd Edition. Washington, DC: Department of National Security and Strategy, 13.

[132] Hart, Basil H. Liddel. 1967. Strategy. A., Fredrick (g.e.). Second Revised Edition. New York: Praeger Publishers, 335.

[133] Eccles, Henry E. 1965. Military Concepts and Philosophy. New Brunswick: Rutgers UP, 48.

an attempt to develop a theory of cyberpower, Starr argued that a strategy in cyberspace consists in „the development and employment of capabilities to operate in cyberspace, integrated and coordinated with the other operational domains, to achieve (...) objectives across the elements of national security strategy."[134]

Regardless of the domain, a strategy aims to serve national/organizational interests and produce strategic effects that contribute to an end state, implying action that possesses strategic value. In a research report to the U.S. Air Command And Staff College, Major Schnobrich attempted to connect strategy and tactics through a strategic value model. For this purpose he described strategic value as „the estimated utility a given action, policy, or resource will have when applied within specific context to meet strategic objectives, either directly or indirectly."[135] This definition is used in this thesis to enable the interpretations and discussion of results from the analysis.

To correctly determine if the selected theoretical concepts present a strategically viable course of action on the use of offensive cyber capabilities for NATO, it is necessary to build a strategy around the concepts that can be properly evaluated. In order to provide the necessary framework to achieve this, the thesis recurred to the Lykke Model due to its adaptability, widespread adoption and influence within North American military strategy as the basis for its military strategy instruction.

4.1 Lykke Model

Alluding to Henry Eccles' definition mentioned in the previous chapter, strategy expresses how a state or group of states will use the power it has available to exert

[134] Starr, S. H. 2009." Towards an Evolving Theory of Cyberpower", in Czosseck, C. and Kenneth Geers. The Virtual Battlefield: Perspectives on Cyber-Warfare. Amsterdam: IOS Press, 23.

[135] Schnobrich, Peter J. 2014. "Breaking Out Tactics: The Strategic Value Model and Thinking Critically at The Operational Level of War", Research Report, US Air Command and Staff College. Air University, Alabama, 12.

control over certain circumstances and areas to achieve objectives that support its interests.

Art Lykke created his theory of strategy based on the condition that each part of a strategy adds to the other and becomes consistent, meaning that they should reflect an appropriate balance between them. Lykke illustrated this through a three-legged stool model: the *ends*, *ways* and *means* being the legs that support the main body (the strategy). Lykke complemented the components with a fourth part to take into account the relationship between them: *risk*. Risk is represented by the angle at which the stool tilts. If any of the legs are too short the whole stool (strategy) will fall over, meaning that the risk is too great. In other words, „a valid strategy must have an appropriate balance of objectives, concepts, and resources or its success is at greater risk"[136] In this metaphor the *means* are the *resources*, the *ends* are the *objectives*, and the *ways* are the *concepts*. The *ends* answer the question to what is to be achieved. They are usually expressed with verbs and if accomplished will contribute towards the completion of national/organizational interests. The *ways* explain how the objectives can be reached by employing the available resources. They must be clear enough to be able to „provide planning guidance to those who must implement and resource it."[137] The *means* encompass the specific assets to be used in „applying the concepts to accomplish the objectives (...)."[138] These can range from tangible means such as facilities and equipment to intangible like intellect or morale. The final variable - *risk* - „explains the gap between what is to be achieved and the concepts and resources available to achieve

[136] Yarger, Harry R. 2008. "Toward a Theory of Strategy: Art Lykke and the U.S. Army War College Strategy Model", in Júnior, J. Boone Bartholomees (g.e.). U.S. Army War College Guide to National Security Issues. Volume I: Theory of War and Strategy, 3rd Edition. Washington, DC: Department of National Security and Strategy, 46.

[137] Ibid, 47.

[138] Ibid.

the objective."[139] Any strategy developed for the competitive international environment has a certain degree of risk to it. The breakdown of a strategy into its component parts by Lykke also enables its evaluation. The resulting balance can be accessed through three categories: *suitability*, *feasibility*, and *acceptability*. *Suitability* regards to the objectives of the strategy (Is the concept aligned with the objectives, and will achieving them with the determined concept produce the desired effects?). *Feasibility* relates to the concepts (Can they be implemented with the available resources and current level of organizational structure?). Lastly, *acceptability* asks if the costs and methods that each approach carries can be justified by their respective desired effect, and acceptable to the internal and external political bodies.

4.2. Components

Developing a valid strategy requires that its components support each other to counter the risks, and fit within the context at which they are being applied[140], and so it is essential to delineate these components in detail to understand what they encompass, their limitations, and their relationship with one another.

4.2.1. Component 1: Objectives

Objectives explain what is to be accomplished and provide justification for the courses of action taken in a strategy, as it provides purpose. Such purpose is displayed in policy, which represents the desired end state in the pursuit of national interests. Quoting Yarger, policy aspires to be a „clear articulation of guidance for the employment of the instruments of power towards the attainment of one or more end states."[141] Objectives are restricted by such policies and selected to create strategic

[139] Ibid.
[140] Ibid, 47-48.
[141] Ibid, 44.

effect. According to Yarger, accomplished strategic objectives should generate or contribute towards the creation of strategic effects „that lead to the achievement of the desired end state at the level of the strategy being analyzed and, ultimately, serve national interests."[142] Yarger sets the second Iraq War as an example: the strategic objectives set out by the Bush administration were to defeat Iraqi military forces, remove Saddam Hussein from power and establish a new democratic regime in the country. The intended strategic effect from attaining these objectives was a regime change, which in turn would lead to the main goal - deny state sponsorship and potential weapons of mass destruction to international terrorists. This theoretical example is represented here to show the logic behind this component. In practice, the positioning of the defeat of Iraqi military forces as the first primary objective to be pursued overshadowed the establishment of a new democratic regime, which according to Yarger should have been the key objective and true point of focus.[143]

4.2.2. Component 2: Resources

Resources represent the means which can be used to achieve the objectives and are necessary to support the concept. This component can be divided between tangible and intangible resources. Tangible resources include physical means such as facilities, people, forces and money, while intangible ones encompass abstract things like intellect, national will and morale. Both complete each other, but present some shortcomings when viewed in isolation: the former is rarely sufficient to optimally support the concept due to competing demands, inability to resource or lack of agreement among leadership officials for funding allocation. The latter are problematic because they are often not measurable or reliable. Yarger gives the example of national

[142] Yarger, Harry R. Strategic 2006. Theory For The 21st Century: The Little Book On Big Strategy. Strategic Studies Institute, US Army War College, 69.
[143] Ibid, 54-55.

will to prove this point: although it can be an essential resource, it is a concept that cannot be taken for granted as it requires sustainment and an accepted cause.[144]Resources can be quantified even if only in general terms, as long as they are stated in clear enough terms to understand what is to be made available to support the concept(s).

4.2.3. Component 3: Concepts

Often sidelined by the U.S. defense community[145], the concepts - or ways - represent the core function of strategy, which is to resolve what to do with the available resources to achieve stipulated objectives, and considering alternatives. As the model is being applied to an existent organization with stipulated resources and objectives, concepts take the center stage in the analysis. Numerous scholars have introduced different approaches towards the use of offensive capabilities in cybersecurity, however only a few of them are compatible with NATO's principles and objectives, and therefore relevant to this thesis. Three diverging concepts have been selected from different experts' works in the field of cybersecurity: the concept of cyber persistence by Dr. Richard J. Harknett (in collaboration with Michael Fisherkeller), deterrence in cyberspace by Dr. Jon R. Lindsay (in collaboration with Erik Gartzke), and punctuated deterrence by Dr. Lucas Kello. Each of these concepts were chosen for their different paths in which a nation-state or international organization can use offensive capabilities for its defense at a strategic level, and most importantly for this thesis, without breaking international law.

[144] Ibid, 60.

[145] In a critique addressed at the US defense community, Dr. Jeffrey W. Meiserstates that Lykke's model has been misinterpreted and diminished strategy to a problem of ends-means congruence. *In* Meiser, Jeffrey W. 2017. "Are Our Strategic Models Flawed? Ends + Ways + Means = (Bad) Strategy". US Army War College: Parameters, Vol. 46:4, 81-91.

Cyber Persistence

Richard Harknett and Michael Fischerkeller set the background for their concept on the uniqueness of cyberspace and the flawed strategic approach of deterrence taken in this field by western nations, more specifically the U.S.. This uniqueness is expressed by the unprecedented scale at which both state and non-state actors can modify the operational domain of cyberspace, the low cost of entry to operate within the domain which enables various actors to affect national power, and the current lack of an internationally agreed upon concept for cyberspace sovereignty.[146]

The authors go on to state that although such characteristics should be taken into consideration when developing a strategy for cyberspace, this is not the case as witnessed by the strategic approach that has dominated U.S. policy, and to an extent NATO policy as well. As discussed earlier in this thesis, the objective of deterrence „is to influence an adversary's cost/benefit calculus so that it concludes that the costs of challenging the status quo outweigh the benefits."[147] At an operational level, this translates into avoiding costly operational contact through threat of punishment; however the concepts that constitute the uniqueness of cyberspace in the eyes of the authors have so far prevented a successful declaration of thresholds and thus the existence of a strong posture in cyberspace for the U.S.. In a more detailed manner, the absence of a recognized concept of cyberspace sovereignty means no boundaries are recognized to be identified as thresholds not to cross. International law experts have stated in the Tallinn Manual 2.0 that the concept of state sovereignty applies to cyberspace, and that it can be violated when the results do not produce physical damage or injury, such as destruction of data, cyber-enabled political influence, economic

[146] Harknett, Richard J. and Michael P. Fischerkeller. 2017. "Deterrence is Not a Credible Strategy for Cyberspace", Orbis, Vol. 61:3, 382.
[147] Ibid, 385.

espionage, etc. However, there is still „no clear consensus in the international community on whether acts that cause no physical damage qualify as a violation."[148]

According to Harknett this raises doubts as to the value of the currently adopted strategy of deterrence in cyberspace, which requires to a certain extent the specification of such boundaries. NATO has a threshold in place that if crossed would justify a cross-domain response, however this invisible line requires a cyber OAA that would deal damage equivalent to use of force to cross it. In reality - as discussed in previous chapters - much of the cyber OAAs that have been causing significant damage to Allied nations occur below this threshold. The main weakness of a strategy of deterrence that contrasts with the authors' own concept is the degree of operational contact: a strategy of deterrence seeks to avoid such contact, which to the authors is a futile effort as cyberspace participants are interconnected and therefore all operations in cyberspace involves contact. „Deterrence applied to cyberspace seeks the absence of unwanted activity in an environment of constant activity and, thus is a comprehensive mismatch."[149]In Harknett's eyes, cyberspace is not exclusively a military domain, but an interconnected one in which various actors operate with overlapping interests and levels in a condition of constant contact, making cyberspace an offense-persistent environment: you can defend but only in the moment, and the cumulative effect of this defense will have little impact on the attacker's capacity to act. The academic argues that the defender should persist operationally.[150]

In what Harknett and Fischerkeller call cyber persistence, they cast aside the logic of operational restraint and threat of force behind deterrence and defend the exact

[148] Jasper, Scott. 2017. Strategic Deterrence: The Active Cyber Defense Option. New York: Rowman & Littlefield, 141.
[149] Ibid, 386.
[150] Harknett, Richard J. 2017. "Cyber Persistence: Re-thinking Security and Seizing the Strategic Cyber Initiative", in Townsend, Elizabeth; et al. Emerging Trends and Methods in International Security: Proceedings of a Workshop. Washington, DC: The National Academies Press, 24-28.

opposite: “a strategy based upon the use of cyber OAAs (...) to generate through persistent operational contact continuous tactical, operational and strategic advantage in cyberspace (...).”[151] Ultimately, this would enable a nation-state or international entity to „deliver effects in, through, and from cyberspace at a time and place of its choosing.”[152]In order to avoid potential escalation when dealing with state actors, duration, range, and magnitude of the defender's cyber OAAs and their consequent technical damage can be manipulated by considering the attacker's abilities to recover lost functionality. The authors entertain the possibility of „cyber tactical action-target pairings”[153] designated to distribute damage at multiple levels from slight (no reconstitution required by attacker) to moderate (functionality transfer to redundant systems) and severe/significant (termination of systems and complete loss of functionality). Such systems could also be designed to deliver reversible damage so that escalation thresholds can be crossed and withdraw at the defendant’s will.[154] Cyber OAAs within the context of strategic persistence can also be managed to generate strategic effects. As cyberspace is defined by both authors as „consisting of interconnected physical systems”, a cyber OAA's tactical effect could be intentionally prolonged, as well as be directed at multiple similar targets, thus generating a cumulative strategic effect over time and space.

The authors cite the enormous volume of cyberspace interactions to justify an important requirement to their concept: automated courses of action. The current advancements and high amount of investment on machine learning and AI are regarded as opportunities to be applied in managing intrusion detection systems. Automated solutions could also be developed to disrupt the source of a hostile cyber action using

[151] Harknett, Richard J. and Michael P. Fischerkeller. 2017. "Deterrence is Not a Credible Strategy for Cyberspace", Orbis, Vol. 61:3, 389.
[152] Ibid.
[153] Ibid, 390.
[154] Ibid.

cyber OAAs to inflict temporary or reversible damage without reaching the threshold of armed attack. The successful introduction of such level of automation as an aspect of persistence will, according to Harknett, gain a major security advantage provided that great care would be taken into the decision-making models of these systems.

Punctuated deterrence

The NATO Enhanced Cyber Defense Policy states that any decision as to whether a cyber attack would meet the criteria to invoke Article 5 „is subject to political decisions by the North Atlantic Council on a case-by-case basis"[155], meaning that even actions carried out by the same actor will be measured independently. The manner in which NATO assesses each hostile cyber OAA also remains unclear due no predetermined and agreed upon standards, as well as the differing internal criteria held by individual member countries. This „ambiguity"[156]led to an already mentioned incident: the 2007 attacks on Estonia caused a major paralysis of the countries' economic and financial activities, inflicting infrastructural damage at a level that drove the country to request the activation of Article 5. The lack of a retaliatory response by NATO at the time showed the world that officials struggled to describe and respond to „a phenomenon that is neither recognizably war nor recognizably peace."[157]

More recent events such as the Sony hack, the numerous large scale ransomware attacks like Petya, NotPetya and Wannacry, as well as the alleged Russian interference in the 2016 U.S. elections exposed the failure to address this growing mid-spectrum activity and the necessity for a „mindshift in approach"[158] in the words of NATO Assistant Secretary General for Emerging Security Challenges Ducaru. The possibility

[155] Jasper, Scott. 2017. Strategic Deterrence: The Active Cyber Defense Option. New York: Rowman & Littlefield, 14.
[156] Ibid.
[157] Kello, Lucas. 2017. The Virtual Weapon and International Order. New Haven: Yale University Press, 207.
[158] Ibid., 206.

of adjusting the thresholds themselves to the specific conditions of each attack is quickly dismissed by Kello, as according to him the gradual lowering of penalties would encourage potential attackers to accept such costs, and the cyber actions are too frequent and of diverse effect to capably create appropriate penalties on a case-to-case basis.[159]

Rather than outright reject the principle of deterrence, Kello proposes an approach to tackle the middle spectrum issue and complement the deterrence strategy already in place. In his own words, this „approach would aim to deter not individual actions but a series of actions; not one-off effects but cumulative effects"[160], factoring in the intensity of harm caused, the timescale in which it was perpetrated and the extension of damage caused to friendly interests. Ben Buchanan also agrees with this line of thought in his book "The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations":

> „[In international affairs] (...) the state suffering the intrusions [of another state or state sponsored actor] will be better able to consider their impact and what they mean for the relationship with the intruding state by investigating the incidents individually but then aggregating them together for the purposes of determining a cumulative response."[161]

From a strategic point of view, this principle holds several advantages but also suffers from relevant flaws, the challenge of signaling being the most prominent. Signaling can be defined as „the effort to communicate the message to the intended audience"[162], and its components in international affairs mainly consist of policy development and official public declarations. Several examples of signaling can be

[159] Ibid., 202-206.

[160] Ibid, 209.

[161] Buchanan, Ben. 2017. The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations. New York: Oxford University Press, 182.

[162] Trujillo, Clorinda. 2014. "The Limits of Cyberspace Deterrence". Joint Force Quarterly, Issue 75. Washington, D.C.: National Defense University Press.

traced to NATO's declaration at the Warsaw Summit (recognition of cyberspace as the fifth domain of operations) and NATO Secretary-General Jens Stoltenberg's remarks in interviews and press releases alike.[163]

Kello acknowledges that an opponent „may not perceive that his actions constitute a coherent series of moves, even if their damaging consequences accumulate coherently in the eyes of the victim."[164]The possibility of a major misunderstanding that could lead to escalation forces the defender to „supply a framework of cumulative penalties"[165] to the attacker, along with signaling procedures and diplomatic efforts to show attackers that their individual actions will not cause isolated responses, but instead will be viewed as a complex aggregation of hostile activity in cyberspace and punished accordingly.[166]

Kello's concept holds several strategic advantages. First of all it would alter the enemy's perception of the retaliatory costs inflicted by the defender: an adversary state finds it easier to manage and is more willing to accept the punitive costs of its hostile actions if such costs are administered over a long period of time on an individual basis. However, such an assessment would less likely be accepted if the punitive measures were applied in a single move that „concentrates and compounds the punishment."[167] Secondly, the current tendency to treat hostile cyber acts on an individual level puts pressure on the victim and compels it to react soon after the act becomes known. Kello states that such a pressure gives the attacking entity „the ability to influence the time and context of the penalties the victim imposes upon him - and whether he imposes

[163] Shalal, Andrea. Grebler, Dan (ed.) and Mark Heinrich (ed.). 2016. "Massive cyber attack could trigger NATO response: Stoltenberg", REUTERS [Berlin], 15 June 2016.

[164] Kello, Lucas. 2017. The Virtual Weapon and International Order. New Haven: Yale University Press, 209.

[165] Ibid.

[166] Ibid.

[167] Ibid, 210-211.

them at all."[168] Punctuated deterrence solves this issue by enabling the defending entity to choose the appropriate time to dish out punishing measures - taking into account any past actions by the attacker and the level of severity accumulated by them.[169]

Lastly, Kello argues that his concept could benefit international organizations by providing the opportunity for nations to combine efforts and penalize common enemies for „similar harmful actions directed against them separately."[170] Punctuated deterrence on a collective level would prevent an adversary from shifting its actions from member state to member state in order to spread any retaliation costs across allies who would be unable to respond individually.[171]

Cyber Deception

As written in chapter two, conventional wisdom puts offense as the dominant force in the cyber domain. The attribution problem, the wide range of actors (both rational and irrational) with access to cyber tools, as well as the technical and financial challenges of constantly being able to block an intrusion (while the attacker only has to succeed once) leads to offense dominance being represented as „an inevitable consequence of information technology."[172] In „Weaving Tangle Webs: Offense, Defense, and Deception in Cyberspace", Jon R. Lindsay and Erik Gartzke call this academic consensus into question due to the absence of high-intensity cyber aggression. They combine this disagreement with the introduction of their own concept - that of deception in cyberspace - through an historic case: the Stuxnet worm released in the late 2000s which constitutes the only known example of physical infrastructure damage via

[168] Ibid,. 211.

[169] Ibid.

[170] Ibid.

[171] Ibid.

[172] Lindsay, Jon R. and Erik Gartzke. 2015. "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace". Security Studies, Vol. 24:2, 323.

a cyber OAA. In Lindsay's and Gartzke's eyes however, the operation actually revealed the limitations of offensive capabilities and cyberwar rather than its potency, as the worm caused only limited and temporary disruption of Iran's nuclear program. Rather than focusing on the potentials of the technology alone, the authors bring up an often overlooked component in cyber OAAs: deception. For Stuxnet to be successful, it combined several deceptive moves to reach its objectives, such as 'man in the middle' attacks and anti-virus detection and evasion. According to James Joseph Yuillwho wrote one of the most accepted definitions for the field in his dissertation, deception within the context of cybersecurity can be seen as the „planned actions taken to mislead attackers and to thereby cause them to take (or not) specific actions that aid computer-security defenses."[173]

The potential for deception in cyberspace is much higher than in other realms due to information technology being vastly integrated in most of the world. Most literature on deception also focuses on actions exercised towards offense. Calling it a „deception revolution"[174], Lindsay states that both basic tactics in deception (dissimulation and simulation)[175] now target not just the „cognitive constructs of users but also the rules that designers have engineered into software code itself"[176], meaning that deception extends beyond psychological effect in cyberspace, greatly expanding opportunities for deception. Although the web's capacity for deception clears the way for its malicious uses, the concept at hand is a „double-edged sword"[177], meaning the attacker can also be fooled by the defender. Just as it is difficult to distinguish malignant from benign activity online by the defender, it is troublesome for the attacker to detect

[173] Yuill, James Joseph. 2007. "Defensive Computer-Security Deception Operations: Processes, Principles and Techniques", PhD dissertation, Raleigh: North Carolina State University, xiii.
[174] Lindsay, Jon R. and Erik Gartzke. 2015. "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace". Security Studies, Vol. 24:2, 332.
[175] Dissimulation refers to hiding information while simulation refers to showing fake information.
[176] Lindsay, Jon R. and Erik Gartzke, 332.
[177]Ibid, 316.

virtual minefields during an operation. Cyber defense through deception would encourage or even facilitate access to the defender's systems while assimilating offensive capabilities within its networks. Unauthorized access to the victim's network would trigger viruses or silent alarms on the attacker while the latter sifts through data, potentially leading to the disabling of the attacker's own system. Offensive assimilation would also cause attackers to indivertibly download malware into their hardware while extracting realistic enough files. Rather than use offensive capabilities as a response to a hostile cyber OAA, intruders would be punished by themselves by carrying harmful data back to their home network or getting lost/confused amidst terabytes of intentionally placed disinformation. Anonymity can also be compromised through broadcasting beacons that track the attack to its origin the longer it stays in the network.

As Lindsay and Gartke argue, the information age has made defense and deterrence alone ineffective strategies. Instead, cyber OAAs can be disrupted not just by blocking intrusions through passive defenses such as firewalls or threats of punishment, but by „converting the penetration into something that confuses or harms the attacker"[178] as well. The concept may be distinct from the strategies of defense and deterrence that are currently used, but its effectiveness is linked to the combined use with the other two.[179]

The use of deception techniques in cyberspace - mostly in the shape of honey-based tools[180] - while valuable, suffers from major limitations if used in isolation. Such techniques require prolonged interaction by the attacker in the defender's systems to be

[178] Ibid, 336.

[179] Ibid, 338.

[180] Used to refer to an extensive range of techniques and tools that incorporate the act of deception. The concept behind their use is to entice attackers to interact with them. These include but are not limited to honeypots (fake systems), honeyfiles (fake files), honeywords (fake passwords). *In* Almeshekah, Mohammed H. and Eugene H. Spafford. 2016. "Cybersecurity Deception", in: Jajodia, Sushil (ed.), et al. Cyber Deception: Building the Scietific Foundation. Geneva: Springer International Publishing, 29.

able to learn the perpetrator's objectives and attribute them. Another challenge is the defender's ability to ensure that any legitimate users do not become collateral damage once an offensive capability is triggered.[181] A final shortcoming that can be witnessed relates to the 'one-time use' characteristic inherent to most offensive tools. Any capabilities assimilated that enable the disruption of the source of the hostile cyber OAA can be studied by the adversary, who then can circumvent them in the future, not to mention reverse engineer them and use them against the defender. As the commander of U.S. Air Force Space Command General William Shelton pointed out, „You use them once and they're pretty much gone, because once you do it people are very quick, they'll figure it out, and they'll learn how to block it for next time."[182]

4.3.3. Component 4: Risk Assessment

The use of cyber offensive capabilities, regardless of the context in which they are utilized, bears risks for states and organizations alike. In Yarger's words, risk can be seen as „an assessment of the balance among what is known, assumed, and unknown, as well as the correspondence between what is to be achieved, the concepts envisioned, and the resources available. (...) Risk weighs the potential advantages and disadvantages of adopting the strategy."[183] In other words, assessing risk means examining the strategy as a whole within the context of the respective environment, determine the implications created by the implementation of the strategy and whether it results in a more or less favorable environment for the state/entity. While the strategist seeks to minimize risk during the formulation of the strategy, those risks are still fully disclosed to decision

[181] Lindsay, Jon R. and Erik Gartzke. 2015. "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace". Security Studies, Vol. 24:2, 316-348.

[182] General William Shelton In Briggs, Z. Fryer. 2012. "U.S. military goes on cyber offensive", [U.S. General William Shelton, interview with Defense News]. 24 March 2012, Defense News.

[183] Yarger, Harry R. Strategic 2006. Theory For The 21st Century: The Little Book On Big Strategy. Strategic Studies Institute, US Army War College, 63.

makers so as to determine if they are acceptable or not.[184] Hence risk represents the gap between the objectives, the resources and the concept, and its assessment is a deciding factor when determining the validity of a strategy.

In its 2012 memorandum, the Israeli Institute for National Security Studies discussed some of the risks that surround the use of these tools. The first two risks mentioned are the possibility of counter-attack and weak cyber defenses[185], however, as NATO is a collective defense organization and therefore restricts its efforts in cyberspace towards its own defense, the former can be incorporated into another risk that will be approached below, while the second does not apply to the Alliance. The two other major risks mentioned - exposure of capabilities and conflict of interests - are intimately related by causality, and so can be combined as one relevant risk for NATO in this thesis. Most offensive cyber tools rely on system vulnerabilities to succeed. Its use would likely expose sensitive capabilities not just exclusively to the target but to NATO's adversaries in general, which in turn would lead to the vulnerabilities being patched and reverse-engineering by adversaries. This means that an offensive cyber capability is for the most part disposable from the moment it is revealed, at the expense of the state that developed it in terms of resource allocation and information gathering[186]. NATO was very clear that it is not planning the development of its own capabilities, but will however adopt and use upon request its members capabilities[187], which can lead to conflicts of interest within the Alliance. Some member states are hesitant to reveal and commit their capabilities when others in the organization will

[184] Ibid, 63-64.

[185] Leading nations in offensive capabilities are themselves highly vulnerable due to minor development on defensive capabilities. See: Even, Shmuel and David Siman-Tov; Rosen, Judith (ed.). 2012. Cyber Warfare: Concepts and Strategic Trends. Memorandum 117. Tel Aviv: Institute for National Security Studies.42.

[186] Ibid, 40-43.

[187] North Atlantic Treaty Organization. November 2017. "Press conference by NATO Secretary General Jens Stoltenberg following the meeting of the North Atlantic Council at the level of Defence Ministers".

benefit without making the same heavy investments[188], while intelligence agencies from NATO members or its partners consider their acquired information too important or sensitive to share.[189]Allied nations with lower investment in cyber capabilities who also have economic ties in energy with non-NATO countries can compromise attribution efforts by the Alliance due to fears of retaliation. Conflict of interests is notable when considering strategies that can also be wrongly perceived as hostile by other nations and international organizations, and is therefore considered a valid risk in this thesis.

Moving to the theoretical concepts that this thesis analyses, Kello, Harknett and Lindsay seem to agree on one risk than can greatly affect the use of offensive capabilities for defensive purposes in cyberspace. If not correctly addressed by diplomatic and technical efforts and/or evaluated prior to a punitive response, escalation represents a very realistic scenario, one that can culminate in armed conflict. Kello addresses this risk as a lack of perception by the adversary meant to be tackled by diplomacy and signaling[190], Harknett sees it as a failure to consider the adversaries' own abilities[191], and Lindsay states that the secret nature of cyber OAAs complicates de-escalation efforts.[192] Escalation is thus a logical choice to be listed as a risk. The authors also mention the heavily debated issue of attribution as one of the challenges that their own approaches could mitigate or circumvent. The subject of attribution is one of the largest issues a cyber OAA victim must overcome, as explained in chapter two of this thesis. David Clark and Susan Landau underline it as a critical problem that is hard to

[188] Bragetto, Pascal; Kaska, Kadri and Matthijs Veenendaal. 2016. "Is NATO Ready to Cross the Rubicon on Cyber Defence?" Tallinn: NATO Cooperative Cyber Defence Center of Excellence, Cyber Policy Brief, 3-6.

[189] Lewis, James A. 2015. "The Role of Offensive Cyber Operations in NATO’s Collective Defense". Tallinn Paper No. 8. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 7-8.

[190] Kello, Lucas. 2017. The Virtual Weapon and International Order. New Haven: Yale University Press, 209.

[191] Harknett, Richard J. and Michael P. Fischerkeller. 2017. "Deterrence is Not a Credible Strategy for Cyberspace", Orbis, Vol. 61:3, 389-390.

[192] Lindsay, Jon R. and Erik Gartzke. 2015. "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace". Security Studies, Vol. 24:2, 347.

address in attempting to deter cyber attacks and argue that „retaliation requires knowing with full certainty who the attackers are."[193], an effort made exponentially harder by NATO Allies and partner's reluctance to share cyber capability information between themselves.[194] It is important to ascertain how and if each approach can deal with this complication, as failing to do so can compromise an entire cyber strategy.

Therefore, and in order to simplify the analysis and maintain the scope of this thesis, three main risks were selected to represent this component: *Attribution*, *Escalation*, and *Conflict of Interests*.

[193] Clark, David R and Susan Landau. 2010. "Untangling Attribution", in: National Research Council (ed.). Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy. Washington, DC: National Academies Press, 25.

[194]Bragetto, Pascal; Kaska, Kadri and Matthijs Veenendaal. 2016. "Is NATO Ready to Cross the Rubicon on Cyber Defence?" Tallinn: NATO Cooperative Cyber Defence Center of Excellence, Cyber Policy Brief, 3-6.

5. Methodology

The acceptance that computers share an offensive power just as any other military equipment opened a new path for research in the field of security studies. Since the statements made by the NATO Secretary General are relatively recent and there is not enough literature nor practical examples that could lead to a more straightforward approach in the field of NATO's use of offensive capabilities in responding to cyber threats, the following questions were asked to understand and foresee NATO's actions in this context:

- How exactly would NATO be able to use offensive capabilities as part of its defensive posture?
- With what objective(s) would NATO use these capabilities?
- What consequences could this have for NATO's relationship with its Allies, partners and external nations?

These initial questions are factored in the thesis to help answering the main research question:

Can known concepts on the use of offensive cyber capabilities in the context of cybersecurity become valid, operational strategies for NATO and retain their theoretical strategic value?

The basis for this paper's analysis rests on the three distinct theoretical concepts on the use of offensive cyber capabilities: *Cumulative Deterrence Theory* from "The Virtual Weapon and International Order" by Lucas Kello, *Cyber Persistence Theory* from "Deterrence is Not a Credible Strategy for Cyberspace" by Richard J. Harknettand

Michael P. Fischerkeller, and *Cyber Deception Theory* from "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace" by Jon R. Lindsay and Erik Gartzke. The analytical process consists in the integration of each theoretical concept within NATO's existing capabilities, followed by their operationalization and evaluation through Lykke's strategic model.

Arthur Lykke's proposition, first published in 1989is a „model for analyzing and evaluating the strategy of historical and current strategic level leadership."[195] Tested numerous times in both historical case studies and practical applications, the Lykke Model was chosen for its adaptability and significant contribution to modern strategic thought. It is used to this day as a relevant model in modern American military strategy, as well as baseline for strategy evaluation in military educational manuals such as the "U.S. Army War College Guide to National Security Issues". The model's adaptability is made evident by the two types of strategic practice that, according to Lykke, the model analyses: operational strategy and force developmental strategy. The first is based on existing military capabilities. The second is based on future threats and objectives, and not limited by existing capabilities[196]. Considering that this thesis focuses on existing NATO resources and capabilities, the type of military strategy engaged is operational strategy.

The model encourages the strategist to use the term *strategy* correctly „while applying the strategy model and its four parts – ends, ways, means and risk"[197].The integration of the theoretical concepts within NATO capabilities makes it possible to formulate potential strategies that can be evaluated on three categories: *Suitability*,

[195] Yarger, Harry R. 2008. "Toward a Theory of Strategy: Art Lykke and the U.S. Army War College Strategy Model", in Júnior, J. Boone Bartholomees (g.e.). U.S. Army War College Guide to National Security Issues. Volume I: Theory of War and Strategy, 3rd Edition. Washington, DC: Department of National Security and Strategy, 48.

[196] Ibid.

[197] Ibid.

Feasibility and *Acceptability*[198]. The purpose of this process is to ascertain whether any of the three mentioned conceptions on the use of offensive cyber capabilities can produce valid strategic results for NATO and ultimately answer this thesis' research question.

Further research support consisted of mainly academic literature. News articles and official public documents were also used to provide background information on NATO's policies and their development. In light of a lack of relatable historical examples and empirical studies on the strategic use of offensive cyber capabilities in the context of cybersecurity, in large part due to the secrecy of these operations, this thesis uses sources primarily from the military and security studies fields to fill this gap, including but not limited to dissertations of military graduates from the Naval Postgraduate School, military educational manuals such as the "US Army War College Guide to National Security Issues", and scientific journals from various institutes.

It is important to note that this thesis is not without limitations. By approaching concepts that focus on the protection of critical infrastructure, this thesis did not take the support of military operations into deeper consideration. The strategies formulated in this paper are intended to respond to threats within cyberspace that could compromise the Alliance's networks, and by extension sabotage its military and political efforts. NATO's priority role in cyberspace during a conflict or military operation would be the protection of its military networks and assistance to Allied networks, and as such, the potential real-time use of offensive cyber capabilities by NATO to directly aid a military operation (e.g. disabling enemy weapon-systems prior to a conventional engagement) was not explored. One of the most problematic aspects in this research is

[198] Ibid.

its starting point. Due to the sensitive nature of cyber capabilities, the inclusion of offensive tools in the integration process of Allied capabilities into NATO has not been publicly confirmed, but also not denied. This makes room for the assumption that offensive capabilities were included.

6. Analysis

Making use of the model, the first step in this analysis is to assemble the necessary components to formulate a strategy: objectives, resources and concepts. As the objectives and resources remain constant between the analyzed strategies due to being associated to the same organization (NATO), they are approached before the analysis of each strategy to avoid repetition. The analysis will then be divided into three subchapters, each pertaining to one of the three strategies derived from the concepts presented in the previous chapters: punctuated deterrence, cyber persistence and cyber deception. Each of these subchapters will include the respective risk assessment, followed by the evaluation of the strategy in the categories of suitability, acceptability and feasibility.

6.1. Objectives

The NATO Policy on Cyber Defense is overseen by the political, military and technical authorities of the Alliance, as well as by individual member states. Presently, NATO's main focus in the area of cyber defense is the protection of its own networks (including operations and missions) and resilience[199] improvement across the Allied nations. It is also established that cyber defense is part of NATO's core task of collective defense. The Alliance's fundamental purpose is, according to the 2010 Strategic Concept, „to safeguard the freedom and security of all its members by political

[199] Considered a core element of collective defense in NATO, it refers to the measures of prevention, response and recovery from cyber attacks when put in the context of cyberspace, as well as their improvement. See: North Atlantic Treaty Organization. 2016. "Resilience: a core element of collective defence". NATO Review magazine, North Atlantic Treaty Organization.
Singer argues that the term is "about understanding how the different pieces fit together and then how they can be kept together or brought back together when under attack." *In* Friedman, Allan and Peter W. Singer. 2014. Cybersecurity and Cyberwar: What Everyone Needs to Know. New York : Oxford University Press, 173.

and military means” and remain „an essential source of stability”[200] globally. Having said that, NATO's current goals do not consider the use of offensive capabilities in cyberspace, but retain generalist terms that allow such an inclusion. The protection of its networks can include offensive means and therefore be considered the main desired effect, which leads to the formulation of strategic objectives. A NATO strategy for the use of offensive cyber capabilities should then include the following objectives:

- Have a response framework that complies with international law. This objective represents one of the most important conditions for the Alliance, as per Secretary General Jens Stoltenberg own words, „regardless of whether we speak about a plane or a tank or a cyber capability, the use of these capabilities is going to be in accordance with international law and it's going to be part of the defensive posture of NATO.”[201];

- Analyse, prevent and respond to cyber OAAs that do not reach kinetic threshold by means of, but not limited to, offensive cyber capabilities. Explained in detail in chapter three, NATO has already declared that any cyber OAA against a member state that reaches the kinetic threshold can justify the activation of Article 5, but the Alliance has struggled to tackle sub-threshold threats. It is a gap that the strategic use of cyber capabilities must cover.

- Encourage allied contributions to capabilities. As NATO does not plan on developing its own cyber capabilities[202], it is paramount that it secures a reliable and continuous supply from Allied nations.

6.2. Resources

NATO possesses a vast assortment of institutional and military resources to pursue its objectives in cyberspace. The NATO Computer Incident Response Capability

[200] North Atlantic Treaty Organization. 2016. "NATO Cyber Defense".

[201] North Atlantic Treaty Organization. November 2017. "Press conference by NATO Secretary General Jens Stoltenberg following the meeting of the North Atlantic Council at the level of Defence Ministers".

[202] Ibid.

(NCIRC) is the body responsible with protecting the Alliance's own networks through centralized 24/7 cyber defense support. Beyond the regular staff the NCIRC's main asset are its Rapid Reaction Teams, which can be deployed not only to support emergencies within NATO but also to Allied networks. NATO can also count on its members' government agencies for cyber related intelligence sharing and assistance towards the improvement of its own cyber defense capabilities[203], efforts that are coordinated by its own agency, the NATO Communications and Information Agency (NCIA).

Regarding capacity building, the NATO CCDCOE, in spite of not being part of the NATO command structure, focuses on research and development offers renowned experience, expertise, professional training, and hosts regular exercises for NATO cyber forces[204]. The Alliance's partnerships with international organizations and the private sector represents a powerful resource. While cooperation with bodies such as the UN and OSCE helps NATO exchange information and legal practices, cooperation with the cyber industry through the NATO Industry Cyber Partnership (NICP) gives the Alliance access to exclusive technological innovations and expertise. NATO's burden-sharing partnership with the EU on cybersecurity issues is also a crucial asset due to the EU's strength in dealing with internal threats in the Alliance, such as cybercrime, which allows NATO to focus on external threats.[205]

NATO has now a much larger array of cyber capabilities available. Its member states (The US, UK, France and Germany being the most cyber developed members)[206]

[203] The Memorandum of Understanding on Cyber Defense between NATO and its members was gradually signed by all 29 Allied Nations, the last being the United Kingdom in February 2017. *In* North Atlantic Treaty Organization. 2017. "United Kingdom and NATO deepen cyber defence cooperation". NATO Industry Cyber Partnership.

[204] North Atlantic Treaty Organization. 2016. "NATO Cyber Defense".

[205] European Commission. 2017. "Joint Communication to the European Parliament and the Council. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU". Brussels: High Representative of the Union for Foreign Affairs and Security Policy, 2-21.

[206] Lewis, James A. 2015. "The Role of Offensive Cyber Operations in NATO’s Collective Defense". Tallinn Paper No. 8. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 7.

recently agreed on providing their own capabilities to NATO's missions and operations upon request. Tangible resources such as these are important to mention, however they remain highly sensitive material and cannot be specifically approached.

When considering intangible resources, the most relevant for this thesis is will power, in this case will power among member states to cooperate in cybersecurity issues and comply with NATO requests pertaining to the use of offensive cyber capabilities. The ongoing construction of NATO's Cyber Operations Center at SHAPE is proof of this will, and its importance is only matched by the risk of conflicting interests that it carries.

6.3. Strategy of Punctuated Deterrence

Lucas Kello's approach of punctuated deterrence effectively complements NATO's current Cyber Defense Strategy by adding to its deterrent effect rather than replacing it. Should the Alliance's deterrence by denial fail to deter a hostile cyber OAA against its networks that does not reach the maximum kinetic threshold for deterrence by punishment to work, punctuated deterrence provides a middle ground solution. Rather than assessing hostile cyber OAAs individually and determining a proper course of action for each, NATO and its allies investigate each incident but aggregate them together as a series of actions by the attributed actor and respond accordingly at a time of their choosing. This concept can also be applied on a collective level: harmful actions in cyberspace against individual member states are also taken into account when considering punishing measures.[207] Based on the argumentation and sources that preclude this concept in "The Virtual Weapon and International Order", it is clear that Kello envisioned NATO as a potential beneficiary of an otherwise state-centric remedy,

[207] The strategies in this analysis are directed towards the use of offensive cyber capabilities in cybersecurity. While punishing measures in Lucas Kello's concept may include efforts outside cyberspace such as economic sanctions, this thesis focuses solely on responses within cyberspace.

although the author refrained from directly naming the organization when presenting the concept.[208]

It is also worth noting that the punishing regime of this strategy is aimed at state actors. When faced with nonstate actors outside Allied jurisdiction, NATO should only apply punctuated deterrence if the state from which the cyber OAA originated refuses to take action and prosecute those responsible, as per Rule 11, "Extraterratorial enforcement jurisdiction", in general international law.[209]

6.3.1. Risk Assessment

The first enumerated risk, *attribution*, is one of the biggest challenges that the victim faces as it involves finding the source of the cyber OAA and assigning blame.[210]An investigation into an incident of this kind requires not only technical means to retrace the attack but also actionable intelligence that can produce compelling proof of the act and its perpetrator(s).[211] Such a process requires considerable time and resources, and the lack of either can seriously affect the victims' ability to respond. The accretion principle of punctuated deterrence can provide the luxury of additional time for NATO and its member states to attribute the origin and perpetrator of the cyber OAA(s), as they would not feel compelled to immediately retaliate.

A major issue within the concept of punctuated deterrence - recognized by Kello - concerns the possibility of escalation. Holding another entity responsible and dishing out punitive measures risks increasing hostilities.[212] Attribution must be properly

[208] Kello, Lucas. 2017. The Virtual Weapon and International Order. New Haven: Yale University Press, 195-212.

[209] Schmitt, Michael N.(g.e.). 2017. Tallinn Manual 2.0 On The International Law Applicable To Cyber Operations. Tallinn: Cambridge University Press, 18.

[210] Clark, David R and Susan Landau. 2010. "Untangling Attribution", in: National Research Council (ed.). Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy. Washington, DC: National Academies Press, 25-40.

[211] Ibid.

[212] Kello, Lucas. 2017. The Virtual Weapon and International Order. New Haven: Yale University Press, 209.

addressed to provide publicly accepted evidence. Misperceptions may also take place due to the need of the attacker being aware that its actions in cyberspace will be aggregated, considered as a whole regardless of the time span between them and the NATO member state(s) targeted, and punished accordingly. Unknowing adversaries can very well consider any punitive measures as disproportional and unjustified aggression, one that can cause a cross-domain counterattack and legitimize the kind of behavior that NATO wishes to avoid in cyberspace. A regime of punishment via cyber means, legitimate as it may be, opens the precedent for potential adversary states to conduct cyber OAAs under the guise of national security and erroneous interpretations of international norms, particularly from states known for using cyber OAAs are a foreign policy tool (e.g. China and Russia).

The strategy of punctuated deterrence entails the use of offensive capabilities to advance the agreed punishment, but in a sporadic regime over long periods of time. Depending on the severity of the cyber OAAs perpetrated against NATO or its members, the Alliance may request capabilities from its more powerful members in cyberspace such as the United States, United Kingdom, France or Germany. As explained in the previous chapters, these capabilities require considerable effort to develop and become obsolete once exposed, meaning states might be unwilling to share such hardly obtained technology, e.g. cyber developed states that did not fall victim to the adversaries' actions. Although occasional - rather than regular - use of such capabilities somewhat eases this issue, as well as the fact that NATO can count on multiple members to supply such tools, the signaling issue can create disagreements among Allied countries. Signaling may require revealing the punitive measures that could be used in NATO's response in advance, which in turn can expose particular cyber capabilities and render them obsolete.

This concern over exposure extends to attributive capabilities, in which this strategy heavily relies. Whereas the methods designed towards attribution are not offensive in nature, NATO still depends on its members for intelligence collection and sharing, and may request cyber capabilities towards this end or to compliment its own attribution tools. Attribution can normally require public exposure on how evidence was obtained, a condition that individual member states can consider a national security risk and consequently withhold potential contributions to the Alliance.

In addition, NATO's defensive nature and commitment to international law complicate its role in this strategy. While NATO can respond to attacks against its own networks, the Alliance cannot directly apply punishing measures in response to attacks directed only against its member states. NATO can potentially request the capabilities should only weaker states have been affected and coordinate punitive efforts, however the member states involved are unable to hide behind the organization and must be the ones to cohesively 'pull the trigger'. Weaker member states might then be wary of going through with the strategy due to their own national concerns, such as shared borders or economic/energy ties with the accused state.

6.3.2. Evaluation

Suitability

For punctuated deterrence to be a suitable strategy, its concept needs to be aligned with NATO's objectives to able to produce the desired effects that will contribute to the Alliance's fundamental purpose, which is to „safeguard the freedom and security of all its members by political and military means and remain an essential source of stability"[213]

[213] North Atlantic Treaty Organization. 2016. "NATO Cyber Defense".

The concept of punctuated deterrence offers a framework that, if applied correctly, is compatible with international norms. The concept goes beyond the scope of NATO's intended effects in cyberspace: the protection of its own networks. Punctuated deterrence seeks to extend this protection to NATO member states, effectively forming a 'cyber umbrella'. The limited use of offensive cyber capabilities by NATO within the framework of punctuated deterrence can be justified under the law of countermeasures[214], specifically when dealing with cyber threats short of an armed attack threshold where the right to self-defense[215] cannot be used. This is only true for cyber OAAs against the Alliance's own networks: NATO itself cannot respond to sub threshold cyber OAAs perpetrated against individual member states, it can only coordinate and lead the affected member state's efforts. Should the same adversary have taken action against both Allied nations and NATO's networks in separate instances, then NATO has the possibility to aggregate them and issue a collective punishment regime accordingly. The fact that this strategy enables NATO to aggregate cyber OAAs from the same intruder against different member states also facilitates the use of the plea of necessity[216] to justify a harsher response, a last resort option in the case of

[214] "Countermeasures are an instrument to induce a State that is responsible for an internationally wrongful act to comply with its international obligations as reflected in the Articles on State Responsibility adopted by the International Law Commission (ILC) in 2001 (Articles 22 and 49-54). Application of this instrument presupposes that the conduct to be countered is attributable to a State." *In* Schaller, Christian. 2017. "Beyond Self-Defense and Countermeasures: A Critical Assessment of the Tallinn Manual's Conception of Necessity". Texas Law Review, Vol. 95:1619, 1620.

[215] "A State facing a cyber operation that constitutes an armed attack can exercise its inherent right to self-defense as laid down in Article 51 of the U.N. Charter, irrespective of whether the attack has been carried out by another State or a non-State actor. In most cases, however, the threshold of an armed attack will not be crossed." *In* Schaller, Christian. 2017. "Beyond Self-Defense and Countermeasures: A Critical Assessment of the Tallinn Manual's Conception of Necessity". Texas Law Review, Vol. 95:1619, 1619-1620.

[216] According to Rule 26 of the Tallinn Manual 2.0, in circumstances where neither self-defense or law of countermeasures apply and a states' essential interests are at risk, the plea of necessity can be invoked to justify the use of cyber means to issue a response. *In* Schmitt, Michael N.(g.e.). 2017. Tallinn Manual 2.0 On The International Law Applicable To Cyber Operations. Tallinn: Cambridge University Press, 135-142.

overwhelming number or intensity of hostile cyber OAAs due to the ease of abuse of this plea.

Punctuated deterrence does not directly prevent intrusions, and therefore lacks a real-time response that could prove crucial to NATO military forces. This can be mitigated by the already existing defense mechanisms, and the use of the strategy can deter potential adversaries from acting against NATO in the future. The strategy's heavy focus on attribution also means that hostile cyber OAAs are properly analyzed through multiple means. This leads to the biggest point of this strategy: a collective punitive response based on careful aggregation and analysis of hostile cyber OAAs, from an adversary against any member state. The inclusion of cyber OAAs suffered by individual member states, together with the limited use of requested capabilities and lack of time pressure to issue a response, can be seen as encouragements for Allied contributions to NATO's cyber arsenal.

Feasibility

The resources and structure required to apply the concept of punctuated deterrence are already largely present in NATO, or currently in development (e.g. NATO's Cyber Operations Center). The fact that the concept complements existing defense strategies indicates that NATO does not require any sizable policy or structural reforms.

However, two resource issues seem to arise from a NATO strategy of punctuated deterrence. Making cyber OAAs against individual state members accountable in the cumulative process means not only NATO but also individual member state resources are relevant, as the strategy will only work if the affected states have the means to detect the intrusions themselves and report them. The Alliance has made the improvement of

Allied cyber resilience one of its main priorities in cyberspace, but to date several Allied nations still possess inadequate or insufficient detection mechanisms.

Another problem arises from the possibility of conflicting interests. Will power to cooperate in cybersecurity issues and comply with NATO requests pertaining to the use of offensive cyber capabilities is crucial in punctuated deterrence, as the entire process - from detection to attribution and application of punishment - depends on the cooperation and coordination between NATO and its member states. Current international environment has somewhat diminished this resource due to arising internal divisions among its members: ongoing Brexit negotiations and conflicting foreign policies between the US and European Allies signifies that two out of the few NATO countries that possess offensive capabilities could be less willing to provide them when requested.

Acceptability

For the strategy of punctuated deterrence to be acceptable, one must consider whether the strategic effect(s) sought – the protection of NATO networks and defense improvement across Allied nations – can justify the methods used to achieve them, and the costs in resources and potential insecurity in the eyes of both domestic and international communities, as derived from the risk assessment.

Although the use of attribution capabilities is intensive, the strategy does not suffer from time pressure, and any use of offensive capabilities is sporadic. This means NATO requests can be spread across capable member states, reducing the resource burden. The Alliance also possesses most of the necessary infrastructure to apply this strategy, with only diplomatic and policy reforms required, making punctuated deterrence a very attractive cost-effective option.

Internally, acceptability is linked to attribution efforts, public opinion and interstate relations inside the Alliance. NATO member states are more likely to rally in support of a collective response effort if the evidence gathered is accurate and convincing. Due to the sensitive nature of cyber capabilities, information regarding the evidence and how it was obtained might be withheld from the public or in extreme cases even from member states with strong relationships to the nation accused, potentially leading to protests in member states with large minorities from the attributed state and/or disagreements between Allied nations. The inherent collective characteristics of punctuated deterrence are what could cement its internal acceptance, or condemn it to failure: the collective extension of a NATO response regime in cyberspace effectively places its member states under a 'cyber umbrella' of sorts, making it an appealing solution for most member states; on the other hand, the strategy can quickly fall if the high levels of cooperation and unity required for it are not met, due to conflicting national security concerns or political divisions between member states.

Externally, assessing acceptability for this strategy becomes more complicated. Punctuated deterrence has the benefit of fitting international law without stretching the interpretation of its concepts, but the strategy's reliance on attribution tools prevents total transparency, which can allow affected states to contest the attribution, citing an apparent lack of evidence in an attempt to gather international support and deem it illegitimate. Yet the strategy itself significantly mitigates this risk. As more incidents are aggregated, the risk of attributive capability exposure diminishes, since NATO can justify its response by "pointing to a pattern of activity." Moreover, NATO can „choose to omit a specific incident from its public justification entirely - treating it as unattributed or providing comparatively less information to the public - but nonetheless increase the severity of its response to account for it. "[217]

6.4. Strategy of Cyber Persistence

Harknett's concept of cyber persistence takes advantage of the „uniqueness of cyberspace"[218]and casts aside the strategies of deterrence by punishment and denial. Although promoting the use of persistent cyber OAAs to face the ever increasing and adapting threats, the intent is not to replace defense with offense. Harknett and Fischkeller defend the development of automated solutions that not only disrupt or degrade the source of the hostile cyber OAA by delivering temporary or reversible damage, but also incorporate existing defensive mechanisms such as intrusion detection, forensic and resilience capabilities. NATO thus no longer focuses on the threat of punishment or denial and instead prioritizes constant operational contact while maintaining its existent defensive structure. The Alliance accepts „that the absence of sovereignty as well as constant contact are structural and operational characteristics of the cyberspace domain"[219], and employs continuous cyber OAAs - ranging from extensive intelligence collection and network monitoring to limited strikes on an adversaries' systems - to uncover and disrupt threats in cyberspace without sacrificing the Alliance's defense practices. This frustrates efforts at exploitation all the while giving precious time for the automated offensive systems to act. It is relevant to add that NATO as a collective defense organization can only fulfill all these actions in protection of its own networks, and cannot act in the name of one of its member states. Should NATO uncover any potential threats against one of its Allied nations its role is

[217] Buchanan, Ben. 2017. The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations. New York: Oxford University Press, 181-182.

[218] Harknett, Richard J. and Michael P. Fischerkeller. 2017. "Deterrence is Not a Credible Strategy for Cyberspace", Orbis, Vol. 61:3, 381.

[219] Ibid, 391.

mainly restricted to intelligence sharing, with the possibility to help coordinate a response by the affected member state.A strategy of active engagement, combined with the Alliance's partnership with the private sector, can also enable counter-subversion efforts by calling out subversive actors publicly and mitigating manipulated information flow in real-time, thus preventing its dissemination on the large scale that has been increasingly witnessed in recent years.

6.4.1. Risk Assessment

Proper forensic work is necessary to accurately assign blame for any hostile cyber OAA suffered/detected and the period of time the process takes can be extensive. The strategy of cyber persistence shifts the emphasis of attribution from merely long-term investigation to short-term results as well, allowing for the source of the cyber OAA to be disrupted or even degraded. This clearly provides an edge to NATO regarding immediate threats, however it can lead to unacceptable levels of collateral damage: the attacker can mask his/her actual location and broadcast a fake signal, or act through other infected computers. Constant cyber operations by NATO to secure its networks in line with the concept of cyber persistence can then indivertibly damage systems from uninvolved states or even member states and result in international repercussions.

When considering escalation, the potential collateral damage on non-member states[220] due to continuous cyber OAAs by NATO is a particularly serious risk in this concept, as it can lead to an escalatory response by the affected entity. Affected systems that are private and not directly linked to that state's government can still reach national attention and lead to retaliation once the cyber OAA is traced back to NATO. Even if

[220] Should any cyber threat be detected in/originate from a NATO country and require immediate response, the case can be handled within the Alliance and repercussions mitigated.

NATO publicly announces its responses, constant cyber OAAs can also potentially antagonize the Alliance in the eyes of the international community: non-member states can easily perceive this approach as unjustified aggression and react outside cyberspace through diplomatic and conventional military means.

The strategy of cyber persistence relies on the continuous use of offensive capabilities to monitor networks outside the Alliance, collect actionable intelligence, and respond to or in some cases prevent hostile cyber OAAs. As NATO does not develop its own capabilities, its member states carry the heavy burden of constantly supplying the organization with newly developed tools and updates to existing ones. The fact that only a limited number of nations within NATO have been able to afford and develop the cyber capability level required for this strategy extensively complicates the situation. As discussed in previous chapters, most offensive cyber OAAs require resources and time to develop, not to mention the existence of vulnerabilities within the adversary's systems which once exploited become obsolete. NATO's constant requests for capabilities and the cyber development inequality among the Allied nations can clearly cause internal divisions which hurt both relations among member states and NATO's own cyber policy efforts. Additionally, many NATO countries have not reached the same level of protective measures as the organization and its most cyber developed members, making the latter more vulnerable to retaliation. This can lead to disagreements within NATO regarding operational freedom and intensity of its cyber OAAs. Outside cyberspace, fear of escalation can also cause severe rifts among member states and NATO partners, particularly from its easternmost members who share borders with Russia and Iran, both heavily militarized non-Allied states whose relationships with several NATO states have become increasingly strained.

6.4.2. Evaluation

Suitability

Although the strategy seems to be completely misaligned with NATO's assigned objectives at first sight, it is unclear if cyber persistence has a certain degree of suitability to NATO's agenda without a deeper analysis.

The strategy's compatibility with international law, when applied to state actors, rests on the issue of sovereignty. „Perhaps the most operationally relevant, and hence politically delicate, legal issue with respect to the cyber environment is the identification of criteria for determining when cyber operations directed against a state violate its sovereignty."[221] The Tallinn Manual 2.0 examines the issue and sets in Rules 1 through 5[222] what constitutes a violation of sovereignty in cyberspace and the principle of sovereignty as one „that prohibits certain types of cyber operations"[223], yet several states are reluctant to confirm this due to seeing the advantages of pursuing national security objectives that derives from the absence of this principle as outweighing the potential costs of hostile cyber OAAs equally caused by this lack of consensus[224], including Allied Countries themselves such as the U.S. Therefore, „the premise that sovereignty bars certain cyber activities even when they fall below the threshold of nonintervention"[225] remains officially unfounded in the eyes of the international community, meaning a strategy of cyber persistence by NATO does not go against currently accepted international norms. Having said that, this strategy opens a terrible precedent: if an organization with global scope such as NATO takes advantage

[221] Schmitt, Michael N. and Vihul Liis. 2017. "Sovereignty in Cyberspace: Lex Lata Vel Non?" American Journal of International Law Unbound, Vol. 111:213, 213.

[222] Schmitt, Michael N.(g.e.). 2017. Tallinn Manual 2.0 On The International Law Applicable To Cyber Operations. Tallinn: Cambridge University Press, 11-29.

[223] Schmitt, Michael N. and Vihul Liis. 2017. "Sovereignty in Cyberspace: Lex Lata Vel Non?" American Journal of International Law Unbound, Vol. 111:213, 214.

[224] Ibid.

[225] Ibid.

of the lack of consensus over certain concepts in international law, it will be setting a standard for the rest of the world, one that undermines any regulatory efforts taken by the UN so far, and is not aligned with NATO principles.

By adopting this strategy, NATO is capable of efficiently detecting and preventing intrusions. The use of advanced automated systems means threats can be quickly stopped, analyzed, and a real-time response can be issued against the origin of the attack. However, the absence of the human factor in the system's decision-making cripples the accuracy of the response, as collateral damage on a larger scale can take place. Allied contributions are hard to be made possible in this strategy. The extremely high resource demand, together with the controversy that surrounds the premise of the concept itself, far outweigh the current benefits of cyber persistence.

Feasibility

Cyber persistence is the most demanding strategy within this thesis in terms of resources. NATO's cyber infrastructure is powerful, constantly being developed, and it is logical to assume that due to the organization's size its cyber defenses have a certain degree of automation. This is insufficient to achieve the concept at hand due in large part to the automation factor: current advancements on AI technology and machine learning allow cyber automated systems to take over threat detection and network surveillance, but once an intrusion is detected human response teams are still required.[226] Furthermore, as an international military organization, NATO would need the decision-making models of such systems to be able to take into consideration attribution accuracy, international law and different types of actors before releasing any

[226] Oltsik, Jon and Jack Poller. 2017. "Automation and Analytics versus the Chaos of Cybersecurity Operations". ESG Research Insight Paper commissioned by McAfee, Enterprise Strategy Group, 3-13.

countermeasures. Human intervention is still required for all these steps, as AI technology has yet to reach this level of sophistication.

Constant operational contact implies continuous replacement of used capabilities and the development of new ones, which puts a tremendous strain on Allied resources and is not long-term sustainable. NATO lacks another important resource to implement the concept of cyber persistence into an operational strategy - will power - and for a simple reason. The development of an automated system and appropriate strategy for the use of offensive cyber capabilities - one that can easily be labeled as a tool of continuous NATO harassment by states among the international community - is a prospect that many Allied nations would be unwilling to accept.

Acceptability

In terms of resources, the technology required is costly, complex, and still in development. NATO's defensive systems also require a significant overhaul due to the extreme policy chances derived from the adoption of a policy of constant operational contact, in contrast with the Alliance's former policy of operational restraint through deterrence.

Adding to the resource problem, the policy of constant operational contact is also unsustainable, as NATO member states have no obligation to indulge the Alliance's requests for cyber capabilities and can cite national security concerns and sovereignty rights to reject the constant flow of requests from NATO. As a military organization based upon the principle of collective defense, the use of a strategy based upon the concept of constant operational contact and automation, along with the precedent it opens, risks delegitimizing the Alliance in the global stage. At this point, escalation becomes a primary concern for Allied nations, especially NATO's easternmost members.

In the eyes of the international community, this strategy can easily be seen as disproportional and unwarranted aggression by NATO, which feeds the anti-western rhetoric from states who can view NATO military presence and expansion as a threat to their national security, such as Russia and China.

6.5. Strategy of Cyber Deception

Vehemently disagreeing with the offensive dominance view in cyberspace, Lindsay's and Gartzke's cyber deception turns away from the technological focus usually seen in cyber strategy, and alternatively base their approach in the difficulty of distinguishing data derived from worldwide dependence on the internet. Using the strategy of cyber deception, NATO assimilates offensive capabilities within its own defensive networks. NATO's cyber strategy of deterrence by denial remains in effect but with a virtual minefield made up by offensive tools[227] as an additional layer of protection, along with false weaknesses that encourage an attacker to follow a predetermined path. Threat of punishment ceases to be necessary for cyber OAAs that do not meet the use of force threshold criteria, as the potential damage that an adversary faces in real-time when facing a strategy of cyber deception acts as a deterrent in itself for future hostile activity.

Although some level of deceptive measures and virtual minefields presumably already exist and are used by NATO (i.e.: honeypots, false data), they are most likely restricted to detecting and isolating a threat. Through the strategy of cyber deception, NATO goes a step further and integrates offensive capabilities within its networks and

[227] Such tools would be mostly comprised of dormant malware that would be activated if the file(s) or network to which the tool is connected to is accessed without authorization or tampered with.

files, potentially making adversaries harm themselves when extracting or tampering data.

6.5.1. Risk Assessment

As Lindsay himself recognizes, „identifying attackers is a time-consuming process relying on circumstantial evidence."[228]The strategy itself entails the use of silent intrusion-detection and tracking/broadcasting systems throughout the defendant's network which, while not full-proof, can provide valuable attribution clues. The strategy's real value however is in the ability to bypass attribution and punish intruders without an actual retaliatory response. The integration of certain offensive cyber capabilities into NATO's defensive minefields means that intruders may punish themselves by extracting false information and/or data containing malware designed to disable/damage the systems that interact with said data.[229] Despite the obvious benefits, bypassing attribution carries the possibility of arbitrary punishment, including to misinformed allies. Legitimate users can become collateral damage, and even though this type of situation can be mitigated „luring attackers into situations that authorized users would avoid"[230], it can never be completely eliminated in such a dynamic and intelligence intensive domain like cyberspace.

As NATO does not directly produce a retaliatory response, its defensive principles remain intact and international law respected, leaving the intruding state or state-sponsored entity unable to gather international support and publicly denounce the Alliance or any of its member states. Faced with such a situation, and deterred from conducting further attempts on NATO's networks, the affected state will likely recur to less visible responses that can precipitate escalation: (1) increase its offensive efforts in

[228] Lindsay, Jon R. and Erik Gartzke. 2015. "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace". Security Studies, Vol. 24:2, 321.
[229] Ibid, 339.
[230] Ibid.

cyberspace and target member states, as well as NATO partner states, for the purpose of sabotage and subversion or (2) make use of its bilateral relations with member states that share important economic or political ties to indirectly pressure NATO. Strategic signaling is also a problematic dilemma in cyber deception that can provoke escalation. Stated by Lindsay as a complication derived from the secret nature of cyber OAAs, revealing the existence of these capabilities to legitimize its deterrence makes potential adversaries aware of them and risks rendering them obsolete, while maintaining its secrecy increases operational success but also the chance of hostilities against NATO as mentioned in the previous paragraph.

Just as in the other two strategies, the regular use of offensive cyber capabilities at the expense of its member states puts NATO in a vulnerable position. Albeit not a direct consequence of the strategy itself but of NATO policy, repeated requests can cripple the will of Allied nations to honor its contribution pledges and lead to divisions among its member states. In the particular case of cyber deception, one-time use requests give way to long-term ones, as the capabilities need to be fully integrated with defensive systems, constantly upgraded or replaced and permanently present within NATO's networks. This is further aggravated due to the inherent characteristics of cyber capabilities: once used and revealed they become obsolete and need to be upgraded or replaced.

Furthermore, to use offensive capabilities in cyber deception the intruder needs to be lured into the infected files and extract them. The increasingly sophisticated ability to detect these fake systems opens a window of opportunity for the attacker to circumvent or even exploit the tools to compromise other parts of the network, thus making the use of deception tools an intolerable risk for many organizations and states.[231]

6.5.2. Evaluation

Suitability

Rather than exploiting the ambiguity of international law or attempt to create a compliant procedure for the use of offensive cyber capabilities, NATO takes a distinct path with the strategy of cyber deception. Through a level of integration of offensive capabilities that requires user interaction to act, any damage dealt to the intruder would theoretically not bear the Alliance's direct responsibility. In reality, whether or not the use of weaponized files in defensive systems can be attributed is a matter of heated discussion. The group of international experts responsible for the Tallinn Manuals debated this issue and remained divided:

> „The minority was of the view that the operation is attributable to the State creating the honeypot pursuant to the law of State responsibility (Rule 15) (...) [and] violates the sovereignty (Rule 4) of the target State because the destructive nature of the operation qualifies it as such (...) [thus] the State that placed the weaponised files into the honeypot has committed an internationally wrongful act (Rule 14). The majority took the position that the organs of the State that penetrated the honeypot factually transmitted the infected files into their own cyber infrastructure, therefore, the State that laid the trap did not conduct the actual activity causing the harm and thus the operation is not attributable to it pursuant to Rule 15."[232]

This issue puts NATO's conduct in a grey area similar to that of cyber persistence, in which the endorsement of either interpretation risks angering Allied nations and potential adversaries alike.

[231] Ibid, 29-30.

[232] Schmitt, Michael N. (g.e.). 2017. Tallinn Manual 2.0 On The International Law Applicable To Cyber Operations. Tallinn: Cambridge University Press, 174.

The methods used in this strategy enable an extensive analysis of the intruder's behavior and means used in its attempt to breach NATO networks, paving the way for defensive improvements. While cyber deception maintains NATO's current defensive structure, the strategy itself does not prevent or respond to cyber threats in the traditional sense of the term: Should an adversary successfully evade NATO's ID mechanisms, cyber deception encourages the intruder(s) to interact with the system rather than prevent said interaction, and harm itself without a direct response being issued. The deterrence effect that can emerge from the use of the strategy can be seen as a form of prevention. Some of the characteristics regarding cyber deception strategy make the encouragement towards Allied contributions difficult. Explained in detail in the *Acceptability* section below, these traits can easily raise security concerns and political discords among member states, which prevent a solid commitment and support for the strategy.

Feasibility

The resources necessary to achieve cyber deception are somewhat between the requirements for punctuated deterrence and cyber persistence. Cyber deception makes use of NATO's existing infrastructure and defensive resources, but requires a much deeper implementation of offensive capabilities than punctuated deterrence, and constant monitoring, as the frequency of use of such capabilities depends on the number of intrusions and their severity. Through its recent request policy NATO can afford to implement and use its members' capabilities, but a lack of control over the use frequency of Allied offensive cyber capabilities and their high development costs can raise concerns regarding long-term costs.

The strategy also demands a certain level of automation in its defense systems, although not as extreme as in cyber persistence. Cyber deception's offensive mechanisms do not require complex decision-making models because they are only activated upon interaction with specific files in a predetermined number of ways, exempting such systems from determining whether it can respond or not. This translates into the need for stronger workplace training and awareness so that legitimate users can distinguish and avoid the weaponized files, something that NATO can afford thanks to its cyber training facilities.

Acceptability

The acceptability of cyber deception is a generally complex matter. The means required to achieve it are not beyond NATO's capacity, and the resource burden for its development and initial use can be covered by Allied nations when faced with the potential benefits, however longevity remains an issue. According to NATO documents, the Alliance was subjected to an average of 500 incidents per month that required a response during 2016, an increase of 60% when compared with 2015. [233] As NATO's deterrence by denial is also in effect, only a small percentage (if any) of these incidents would result in an intrusion and cause cyber deception to be applied. Even so, a small number of intrusions already leads to the upgrading or replacing of any capabilities activated - an effort that requires significant resources and skill - and with a yearly increase that can go as high as 60%, it is natural that contributing nations show concern over a possible resource strain and resent the ones who benefit but do not contribute due to a lack of investment, leading to conflict of interests.

[233] North Atlantic Treaty Organization. 2016. "NATO Cyber Defense", 1.

The struggle to accept cyber deception becomes clearer when viewing it from an internal perspective. Adding to the potentially unsustainable long-term resources required to apply the strategy, the burden-sharing conflicts and the precedent that would be established in international law, there is also the implication of user interaction for a system response: NATO does not have control over which or how many of these tools are used. As only a handful of Allied nations are capable of developing offensive cyber capabilities[234], cyber deception is likely to be cast aside for a more cost-effective solution.

Externally, the adoption of this strategy would cause mixed feelings in the U.N., and most likely divide the international community, including the Security Council. Those with the prospect of bolstering their own cyber defenses would support the use of weaponized files, while those with a large offensive focus and investment in cyberspace, particularly China[235], would condemn it..

[234] Lewis, James A. 2015. "The Role of Offensive Cyber Operations in NATO's Collective Defense". Tallinn Paper No. 8. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 7.

[235]„There is significant evidence that the Chinese government, together with the Chinese military, private corporations, and unaffiliated citizens, conduct intrusions against major Western powers as well as in the neighbouring region every day, targeting academia, industry and government facilities for the purpose of amassing technological secrets." See Raud, Mikk. 2016. "China and Cyber: Attitudes, Strategies, Organization". Tallinn: NATO Cooperative Cyber Centre of Excellence.

7. Summary of Results

After relating each strategy's respective components to NATO and making the respective risk assessment, the results of the analysis are provided by answering the three questions asked in the Lykke Model:

- Is the concept aligned with the objectives, and will completing those objectives with the determined concept produce or lead to the desired effects (Is it suitable?)
- Can the concept be implemented with the available resources and current level of organizational structure (Is it feasible?)
- Are the costs and methods that each concept carries justified by their respective desired effect, and acceptable to the internal and external political bodies? (Is it acceptable?)

In regards to punctuated deterrence, the findings in this paper's analysis suggest the strategy seems capable of addressing and going beyond NATO's objectives in a way that contributes to the Alliance's desired effect (although conditioned by the state of international affairs). The organization also has the required resources to implement the strategy, and the shortcomings brought to light in the analysis may affect efficiency but not its attainment. Punctuated deterrence seems to have everything to be successful for NATO, however, emerging divisions among Allied nations due to conflicts of interests greatly raise the chance of failure of this strategy and renders it internally unacceptable, and as a consequence, invalid.

Continuing the analysis, the strategy of cyber persistence shows itself as technically compatible with international norms and presents an effective use of offensive capabilities. Nevertheless, NATO's dependence on Allied contributions and commitment to international law make this strategy's unsuitable. Another issue seems to be that the technology level required to fully implement this strategy has yet to be achieved. Combined with the resource strain it may cause to contributing Allies and the legal grey area it operates in, the concept of cyber persistence is therefore not achievable with current NATO resources, rendering cyber persistence unfeasible. Likewise, this strategy is unlikely to be acceptable in the eyes of both member and non-member states, as well as international bodies, due to taking advantage over the lack of agreed definitions when applying international norms to cyberspace[236]and its highly aggressive and resource demanding stance.

In cyber deception, the strategy's requirements - when combined with the Alliance's internal discrepancies and higher chance of human error - can compromise the objectives established, and therefore cannot be considered suitable for NATO. Created not as a stand-alone strategy, but as a complementing one to existing defensive efforts, the theoretical resource cost is lower than in the other two strategies, with the biggest demands being staff training and development/implementation of the required automated systems. Although these automated systems and the lack of control towards the frequency of use of Allied capabilities cast a large shadow on the long-term survivability of this strategy, NATO currently has the required structure and resources to implement it, which makes cyber deception feasible. Arriving at the last category, NATO member states are unlikely to accept this strategy due to its lack of resource viability and prospect of possible accidents with severe consequences. The international community is also unlikely to take the adoption of this strategy in a good light, mainly due to its inability to agree whether in such a situation the responsibility for any damage caused lies with the intruding or the defending state.

[236] Buchanan, Ben. 2017. The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations. New York: Oxford University Press, 134.

8. Conclusion

In its most relevant moves towards using offensive cyber capabilities, NATO has recognized cyberspace as an operational domain, and more recently announced the adoption of its members' capabilities upon request to tackle future cyber threats. However, the Alliance still lacks an articulated strategy for the use of offensive cyber capabilities compatible with its defensive efforts in cyberspace, and until recently its European counterparts have been unaware or uninterested in emerging concepts that approach the use of offensive cyber tools for the purpose of self-defense. The point of this thesis was to determine if any of the selected approaches were compatible with NATO by using them to formulate a potentially valid operational strategy, and if they could retain their theoretical strategic value.

Beginning with the strategy of punctuated deterrence, its ambition in scope and transparency to international norms are only matched by the unity and cooperation required for its success. The prospects of conflicting interests and distrust between Allied national agencies reveal the naivety of a concept that requires international recognition of its interpretation on international law and nearly unconditional cooperation among Allied nations to work. Although a strategy of punctuated deterrence is evidently more suitable and feasible than the other evaluated strategies in this thesis, as well as alluring to many NATO countries, its acceptability is questionable in practice. On one hand, China's and North Korea's continued offensive-shaped cyber strategies, as well as Russia's growing use of cyberspace for military purposes and disinformation campaigns, make the costs recurring from applying a strategy of punctuated deterrence more than acceptable to the Allies. This acceptance however is highly subjective to NATO recognizing the importance of mitigating the strategy's risk by signaling its potential adversaries through measures such as the development of a publicly accessible framework of cumulative penalties, strong diplomatic efforts in the UN, and most of all unity and cooperation between Allied nations. Issues like criticism of protectionist policies and NATO emanating from the current U.S. administration, the rise of populist anti-establishment governments within the EU, increasing Russian interference in western democracies through disinformation campaigns, intelligence and cyber operations, are contributing to the erosion of the very unity and cooperation that NATO requires to function properly. In spite of all three components being valid, this potential unbalance in acceptance greatly raised the overall degree of risk in the strategy, making it susceptible to failure.

Despite this, the use of offensive capabilities through punctuated deterrence still has the largest strategic value for NATO among all three. It provides a potential solution that follows NATO's principles and objectives, tackles attribution issues, and if committed to can ideally help cement the unity it requires, as well as provide effective protection and renewed purpose to the organization by extending its response and deterrent effect to Allied nations' networks.

Moving onto the strategy of Cyber Persistence, we are faced with a stark contrast to punctuated deterrence. The views expressed through this strategy take a skeptical approach and see a universal agreement towards the rules of conduct in cyberspace as unlikely, and operational restraint as a naive mistake. The concept, originally created with the United States in mind, suits the logic behind the nation-state very well, but if applied to NATO it develops into an ill-fitted strategy. The exploitation towards the lack of international consensus over the issue of sovereignty in cyberspace is not unheard of, in fact the benefits of operational flexibility and lack of oversight from international regulatory bodies still far outweigh the costs of leaving this legal area unsolved in the eyes of most cyber capable states. The use of this strategy by NATO however - even if technically not breaking international law - undermines its reputation and erodes its constantly outspoken commitment to international norms. The advance in AI and attribution technologies has not yet reached a point that would allow a semi to fully autonomous system to quickly and accurately attribute an intrusion, and then take into consideration all the factors required to act upon it during the intrusion itself. This decision-making process - although already enhanced by machine-learning - still requires human intervention, and the extensive time plus resources that forensic tools still required to correctly identify the origin and intruder of a cyber OAA means real-time accurate attribution is currently nearly impossible, and carries a high chance of extensive collateral damage. Even if attribution would not be in question and NATO had the technology, the dehumanization of this process would carry repercussions not yet envisioned or sufficiently studied, thus binding the invalidity of this strategy. And while a policy of continuous operational contact provides cyber persistence with a real-time application advantage when compared to the other two, it failed to bring any significant strategic value to NATO at this point.

Lastly, the strategy of Cyber Deception presented a more unorthodox path. Instead of practicing operational restraint due to concerns over unintended repercussions, this strategy does not issue any direct response in the first place, which leads to the source of both its biggest strengths and greatest weaknesses. The integration of offensive cyber capabilities within NATO's already existing defensive systems in the form of a virtual minefield falls in a grey area of international law, and implies that NATO consider that the responsibility regarding any damage caused by the weaponized files belongs to the intruder, as the latter performed the actual transmission of malware into its own cyber infrastructure. This simultaneously acts as a deterrent but also as a catalyst towards attempts to delegitimize NATO in the eyes of the international community, as well as heated debates in the U.N.

Cyber deception suffers from several other setbacks. Initiative stays with the adversary, and the strategy will only work if the intruder is successfully lured or compelled to interact with an infected file. This also means that NATO would have little to no control over the frequency of use of the capabilities it would request, pushing away Allied support for the strategy. Secondly, this uncertainty regarding long-term viability is further intensified when faced with the possibility of human error, one that carries serious consequences, raising the overall degree of risk and compromising the acceptability of the strategy, and by extension, its validity and application.

The analysis in this paper thus determined that none of the selected concepts on the use of offensive cyber capabilities for self-defense led to a valid strategy that could be applicable to NATO. Additionally, while both concepts of cyber persistence and cyber deception managed to retain a certain degree of strategic value following their operationalization, punctuated deterrence represents the closest strategy to being valid and applicable out of the three according to the Lykke Model. Suitable, feasible and theoretically acceptable for NATO, the strategy of punctuated deterrence is vulnerable to failure due to a single fact: no state is willing to put NATO's security and integrity above its own national security, especially when it comes to intelligence and capability sharing. Putting weaker and less financially-committed nations under the protection of a collective defense organization that requires the information and technological resources that only a handful of members possess would simply not be presently approved. The sharp criticism regarding the lack of overall commitment of other members in terms of the number of troops pledged and obligatory financial contributions brought by the current administration of NATO's most powerful member, the U.S., proves this point. Based on this paper's analysis, this weakness can be partially addressed by adopting some of the characteristics of cyber persistence and cyber deception. As peacetime cyber espionage is not prohibited by international law, the policy of constant operational contact can be applied to a limited degree, in terms of capabilities used and automation sophistication, in order to conduct cyber espionage operations for the purpose of information gathering. The weaponization of files can also be restricted to aiding attribution efforts and collecting information. Rather than crippling or damaging cyber infrastructure, the transmitted malware would broadcast the location of the adversary's systems and/or create backdoors for surveillance purposes. This enhancement of the strategy of punctuated deterrence would help the Alliance become less dependent on intelligence sharing from its member states and strengthen attributive efforts. The potentially valuable intelligence produced could also encourage Allied capability contributions.

Although an analysis of NATO's internal situation or of Allied cooperation were both beyond the scope of this thesis, the fact remains that NATO must solve its financial contribution and cyberpower discrepancy before it is able to properly apply a strategy for the use of offensive cyber capabilities, or else the Alliance's future strategic efforts will prove to be potentially fruitless in cyberspace.

There is still room for improvement and development in this field of research, seeing that further studies as well as more practical examples are required to better assess the use of offensive capabilities in support of NATO military operations or in case of military conflict, as well as to approach the issue of how can NATO uphold international order in cyberspace and still thrive when several international norms are still not universally accepted, and at times exploited by several cyber-aggressive nations. Since the findings of this paper cover only a part of NATO's role in the international stage, a further step in research could be to expand the model to include other NATO domains and explore the relationship between them and the evolving policies of NATO in the field of cybersecurity.

Bibliography

Almeshekah, Mohammed H. and Eugene H. Spafford. 2016. "Cybersecurity Deception", in: Jajodia, Sushil (ed.), et al. Cyber Deception: Building the Scietific Foundation. Geneva: Springer International Publishing, 23-49.

American Journal of International Law Unbound, Vol. 111:213. URL: https://ssrn.com/abstract=3024405

Bragetto, Pascal; Kaska, Kadri and Matthijs Veenendaal. 2016. "Is NATO Ready to Cross the Rubicon on Cyber Defence?" Tallinn: NATO Cooperative Cyber Defence Center of Excellence, Cyber Policy Brief. URL: https://ccdcoe.org/sites/default/files/multimedia/pdf/NATO%20CCD%20COE%20policy%20paper.pdf (07.06.2018).

Buchanan, Ben. 2017. The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations. New York: Oxford University Press.

Burton, Joe. 2015. "NATO's cyber defence: strategic challenges and institutional adaptation", Defense Studies, Vol. 15:4, 297-319. URL: 10.1080/14702436.2015.1108108 (25.07.2018).

Canbolat, Mustafa and Emrah Sezgin. 2016. "Is NATO Ready For a Cyber War?". Master Thesis, Naval Postgraduate School, Monterey. URL: https://calhoun.nps.edu/bitstream/handle/10945/51662/16Dec_Canbolat_Sezgin.pdf?sequence=1&isAllowed=y (15.05.2018).

Carl Von Clausewitz On War, ed. and trans. by Michael Howard and Peter Paret, Princeton University Press (1976), pp. 177.

Caton, Jeffrey L. 2016. NATO Cyberspace Capability: A Strategic and Operational Evolution. Strategic Studies Institute and U.S. Army War College Press.

Clark, David R and Susan Landau. 2010. "Untangling Attribution", in: National Research Council (ed.). Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy. Washington, DC: National Academies Press, 25-40.

D. C., Alexander.2014. "Cyber Threats against the North Atlantic Treaty Organization (NATO) and Selected Responses". Istanbul: Gelisim University Social Sciences Journal, Issue 1, 1-36. URL: http://dergipark.gov.tr/download/article-file/89251 (28.07.2018).

Eccles, Henry E. 1965. Military Concepts and Philosophy. New Brunswick: Rutgers UP.

Edwards, Benjamin; et al. 2017. "Strategic aspects of cyberattack, attribution, and blame", Proceedings of the National Academy of Sciences of the United States of America, Vol. 114:11, 2825-2830. URL: http://www.pnas.org/content/114/11/2825 (28.07.2018).

Emmott,Robin. 2017. “NATO mulls 'offensive defence' with cyber warfare rules”.[NATO CCDCE Head of Strategy Michael Widmann, interview with REUTERS

], REUTERS. URL: https://uk.reuters.com/article/uk-nato-cyber/nato-mulls-offensive-defence-with-cyber-warfare-rules-idUKKBN1DU1GV. (22.07.2018).

European Commission. 2017. "Joint Communication to the European Parliament and the Council. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU". Brussels: High Representative of the Union for Foreign Affairs and Security Policy. URL: https://publications.europa.eu/en/publication-detail/-/publication/794f8627-985b-11e7-b92d-01aa75ed71a1/language-en (20.06.2018).

Even, Shmuel and David Siman-Tov; Rosen, Judith (ed.). 2012. Cyber Warfare: Concepts and Strategic Trends. Memorandum 117. Tel Aviv: Institute for National Security Studies. URL: https://www.files.ethz.ch/isn/152953/inss%20memorandum_may2012_nr117.pdf (28.07.2018).

Evera, Stephen Van. 1984. “The Cult of the Offensive and the Origins of the First World War”. Massachusetts: MIT Press. International Security, Vol. 9:1, 58-107. URL: https://www.jstor.org/stable/2538636 (02.04.2018).

Friedman, Allan and Peter W. Singer. 2014. Cybersecurity and Cyberwar: What Everyone Needs to Know. New York : Oxford University Press.

Galinec, Darko; Moznik, Darko and Boris Guberina. 2018. "Cybersecurity and cyber defence: national level strategic approach". London: Informa UK Limited. Automatika vol. 58:3, 273-286. URL: https://doi.org/10.1080/00051144.2017.1407022 (28.07.2018).

Gartzke, Erik. 2013. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth". Massachusetts: MIT Press. International Security, Vol. 38:2. URL: https://doi.org/10.1162/ISEC_a_00136 (15.05.2018).

Geer, Daniel; et al. 2003. “Cyberinsecurity: The Cost of Monopoly—How the Dominance of Microsoft’s Products Poses a Risk to Security”. Independent Report published by the Computer and Communication Industry Association. URL: http://cryptome.org/cyberinsecurity.htm (20.06.2018).

Geers, Kenneth. 2017. Strategic Cyber Security. Tallinn: NATO Cooperative Cyber Defense Centre of Excellence.

General William Shelton In Briggs, Z. Fryer. 2012. "U.S. military goes on cyber offensive", [U.S. General William Shelton, interview with Defense News]. 24 March 2012, Defense News. URL: https://www.defensenews.com/article/20120324/DEFREG02/303240001/U-S-Military-Goes-Cyber-Offensive/ (07.06.2018).

Ghavam, Z'hra M. 2016. "NATO's Preparedness For Cyberwar". Master Thesis, Naval Postgraduate School, Monterey. URL: https://www.hsdl.org/?view&did=801548 (28.07.2018).

Glaser, Charles L. and Chaim Kaufmann. 1998. "What is the Offense-Defense Balance and Can We Measure it?". Massachusetts: MIT Press. International Security, Vol. 22:4, 44-82. URL: https://www.jstor.org/stable/2539240 (28.07.2018).

Harknett, Richard J. 2017. "Cyber Persistence: Re-thinking Security and Seizing the Strategic Cyber Initiative", in Townsend, Elizabeth; et al. Emerging Trends and

Methods in International Security: Proceedings of a Workshop. Washington, DC: The National Academies Press, 24-28.

Harknett, Richard J. and Michael P. Fischerkeller. 2017. "Deterrence is Not a Credible Strategy for Cyberspace", Orbis, Vol. 61:3, 381-393. URL: https://www.sciencedirect.com/science/article/pii/S0030438717300431 (28.07.2018).

Hart, Basil H. Liddel. 1967. Strategy. A., Fredrick (g.e.). Second Revised Edition. New York: Praeger Publishers.

Healey, Jason and Leendert Van Bochoven. 2011. "NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow". Washington, DC: Atlantic Council. URL: http://www.atlanticcouncil.org/images/publications/NATOs_Cyber_Capabilities.pdf (28.07.2018).

Her Majesty's Government. 2015. National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom. London: HM Government. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/478936/52309_Cm_9161_NSS_SD_Review_PRINT_only.pdf (28.07.2018).

Herz, John H. 1950. "Idealist Internationalism and the Security Dilemma". Princeton: Cambridge University Press. World Politics, Vol. 2:2, 157-180. URL: http://www.jstor.org/stable/2009187 (28.07.2018).

Howard, Michael (g.e.) and Peter Paret (g.e.). 1976. Carl Von Clausewitz. On War. Princeton: Princeton University Press.

International Telecommunications Union. 2010. "ITU Toolkit for Cybercrime Legislation", Report commissioned by ITU Development Sector of Cybersecurity. Geneva: ITU. URL: http://docplayer.net/17880697-Itu-toolkit-for-cybercrime-legislation.html (28.07.2018).

Jasper, Scott. 2017. Strategic Deterrence: The Active Cyber Defense Option. New York: Rowman & Littlefield.

Júnior, J. Boone Bartholomees. 2008. "A Survey of The Theory of Strategy", in: Júnior, J. Boone Bartholomees (g.e.). U.S. Army War College Guide to National Security Issues. Volume I: Theory of War and Strategy, 3rd Edition. Washington, DC: Department of National Security and Strategy, 13-15.

Kello, Lucas. 2017. The Virtual Weapon and International Order. New Haven: Yale University Press.

Knapp, Kenneth and William Boulton. 2006. “Cyber-Warfare Threatens Corporations: Expansion to Commercial Environments” Information Systems Management Journal, Vol. 23:2, 76-87. URL: http://www.infosectoday.com/Articles/cyberwarfare.pdf (28.07.2018).

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

Lee, Robert M. 2015. "The Sliding Scale of Cybersecurity". SANS Analyst Whitepaper. Swansea: SANS Institute. URL: https://www.sans.org/webcasts/sliding-scale-cyber-security-100517 (20.06.2018).

Lewis, James A. 2015. "The Role of Offensive Cyber Operations in NATO’s Collective Defense". Tallinn Paper No. 8. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence. URL: https://ccdcoe.org/sites/default/files/multimedia/pdf/TP_08_2015_0.pdf (28.07.2018).

Libicki, Martin C. 2009. Cyberdeterrence and Cyberwar. Santa Monica: Research ANd Development Corporation (RAND). URL: https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf (30.07.2018).

Lin, Herbert. 2014. "Cyber Conflict and National Security", In: Art, Robert J. and Robert Jervis (Eds.). International Politics: Enduring Concepts and Contemporary Issues. Pearson. Boston: Pearson 12th Edition, 476-489.

Lindsay, Jon R. and Erik Gartzke. 2015. "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace". Security Studies, Vol. 24:2, 316-348. URL: https://doi.org/10.1080/09636412.2015.1038188 (28.07.2018).

Locatelli, Andrea. 2013. "The Offense/Defense Balance In Cyberspace". Milano: Istituto per gli Studi di Politica Internazionale, Analysis No. 203. URL: https://pdfs.semanticscholar.org/2855/2916015050d058d5e8d8662f8e4900887c23.pdf (28.07.2018).

Lynn, William J. 2010. “Defending a New Domain: The Pentagon’s Cyberstrategy”, Foreign Affairs, Vol. 89:5, 97-110. URL: https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain (28.07.2018).

Meiser, Jeffrey W. 2017. "Are Our Strategic Models Flawed? Ends + Ways + Means = (Bad) Strategy". US Army War College: Parameters, Vol. 46:4, 81-91. URL: https://ssi.armywarcollege.edu/pubs/parameters/issues/Winter_2016-17/10_Meiser.pdf (28.07.2018).

NATO Cooperative Cyber Defense Center of Excellence. 2014. "International Cyber Developments Review" Tallinn: Incyder news. URL: https://ccdcoe.org/sites/default/files/publications/articles/INCYDER%202014Q2.pdf

NATO Cooperative Cyber Defense Centre of Excellence. " Cyber Definitions". URL: https://ccdcoe.org/cyber-definitions.html. (28.07.2018).

North Atlantic Treaty Organization. 2016. "NATO Cyber Defense". URL: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf (28.07.2018).

North Atlantic Treaty Organization. 2016. "Resilience: a core element of collective defence". NATO Review magazine, North Atlantic Treaty Organization. URL: https://www.nato.int/docu/review/2016/Also-in-2016/nato-defence-cyber-resilience/EN/index.htm (20.06.2018).

North Atlantic Treaty Organization. 2017. "United Kingdom and NATO deepen cyber defence cooperation". NATO Industry Cyber Partnership. URL: http://www.nicp.nato.int/united-kingdom-and-nato-deepen-cyber-defence-cooperation/ (20.06.2018).

North Atlantic Treaty Organization. Last updated: 16 Jul. 2018. “Cyber Defence”. URL: http://www.nato.int/cps/en/natohq/topics_78170.htm (30.07.2018)

North Atlantic Treaty Organization. Lisbon Summit Declaration. Brussels: North Atlantic Treaty Organization, 2010. URL: https://www.nato.int/cps/en/natohq/official_texts_68828.htm (28.07.2018).

North Atlantic Treaty Organization. November 2017. "Press conference by NATO Secretary General Jens Stoltenberg following the meeting of the North Atlantic Council at the level of Defence Ministers". URL: https://www.nato.int/cps/en/natohq/opinions_148417.htm?selectedLocale=en (July 30, 2018)

North Atlantic Treaty Organization. Prague Summit Declaration. Brussels: North Atlantic Treaty Organization, 2002. URL: https://www.nato.int/cps/en/natohq/official_texts_19552.htm (15.03.2018).

North Atlantic Treaty Organization. Riga Summit Declaration. Riga: North Atlantic Council, 2006. URL: https://www.nato.int/cps/su/natohq/official_texts_37920.htm (28.07.2018).

Nye Jr., Joseph S. 2017. "Deterrence and Dissuasion in Cyberspace", Massachusetts: MIT Press, International Security, Vol. 41:3 44-71. URL: https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00266 (28.07.2018).

Oltsik, Jon and Jack Poller. 2017. "Automation and Analytics versus the Chaos of Cybersecurity Operations". ESG Research Insight Paper commissioned by McAfee, Enterprise Strategy Group. URL: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-esg-security-ops-and-analytics.pdf (20.07.2018).

P. Fidler, David; Pregent, Richard and Alex Vandurme. 2013. "NATO, Cyber Defense, and International Law". Indiana: Articles by Maurer Faculty, Paper 1672, URL: https://www.repository.law.indiana.edu/facpub/1672/?utm_source=www.repository.law.indiana.edu%2Ffacpub%2F1672&utm_medium=PDF&utm_campaign=PDFCoverPages. (02.02.2018).

Raud, Mikk. 2016. "China and Cyber: Attitudes, Strategies, Organization". Tallinn: NATO Cooperative Cyber Centre of Excellence. URL: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016.pdf

Rühle, Michael. 2011. "NATO and Emerging Security Challenges: Beyond the Deterrence Paradigm". American Foreign Policy Interests, Vol. 33:6, 278-282. URL: 10.1080/10803920.2011.632308 (19.03.2018).

Saltzman, Ilai. 2013. “Cyber Posturing and the Offense-Defense Balance", Contemporary Security Policy, Vol. 34:1, 40-63. URL: 10.1080/13523260.2013.771031 (25.07.2018)

Schaller, Christian. 2017. "Beyond Self-Defense and Countermeasures: A Critical Assessment of the Tallinn Manual's Conception of Necessity". Texas Law Review, Vol. 95:1619, 1619-1638. URL: https://texaslawreview.org/wp-content/uploads/2017/11/Schaller.pdf (20.06.2018).

Schmitt, Michael N. (g.e.). 2017. Tallinn Manual 2.0 On The International Law Applicable To Cyber Operations. Tallinn: Cambridge University Press.

Schmitt, Michael N. and Vihul Liis. 2017. "Sovereignty in Cyberspace: Lex Lata Vel Non?"

Schnobrich, Peter J. 2014. "Breaking Out Tactics: The Strategic Value Model and Thinking Critically at The Operational Level of War", Research Report, US Air Command and Staff College. Air University, Alabama. URL: http://www.dtic.mil/dtic/tr/fulltext/u2/1023216.pdf (28.07.2018).

Segal, Adam. 2017. "Europe Slowly Starts to Talk Openly About Offensive Cyber Operations", Council on Foreign Relations. URL: https://www.cfr.org/blog/europe-slowly-starts-talk-openly-about-offensive-cyber-operations. (22.07.2018).

Shalal, Andrea. Grebler, Dan (ed.) and Mark Heinrich (ed.). 2016. "Massive cyber attack could trigger NATO response: Stoltenberg", REUTERS [Berlin], 15 June 2016. URL: https://www.reuters.com/article/us-cyber-nato/massive-cyber-attack-could-trigger-nato-response-stoltenberg-idUSKCN0Z12NE?m...d1FFaHZNRldGb3BEd01LQk1QeFprWWxDWVAycTRNdlNLaVU4WT0ifQ%3D%3D (28.07.2018).

Slayton, Rebecca. 2017. "What is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment". Massachusetts: MIT Press. International Security, Vol. 41:3, 72-109. URL: https://doi.org/10.1162/ISEC_a_00267 (12.04.2018).

Slayton, Rebecca. 2017. "Why Cyber Operations Do Not Always Favor the Offense". Massachusetts: MIT Press. International Security, Policy Brief Issue February 2017. URL:

https://www.belfercenter.org/sites/default/files/files/publication/Cyber%20Ops%20Offense%20-%20final.pdf (29.07.2018).

Starr, S. H. 2009." Towards an Evolving Theory of Cyberpower", in Czosseck, C. and Kenneth Geers. The Virtual Battlefield: Perspectives on Cyber-Warfare. Amsterdam: IOS Press, 18-52.

Szentgáli, Gergely. 2013. "The NATO Policy on Cyber Defense: The Road so Far". AARMS Vol. 12:1, 83-91. URL: https://folyoiratok.uni-nke.hu/document/uni-nke-hu/aarms-20131-szentgali.original.pdf (19.03.2018).

Tankard, Colin. 2011. "Advanced Persistent Threats and how to monitor and deter them", Network Security, Vol. 2011:8, 16-19. URL: https://www.sciencedirect.com/science/article/pii/S1353485811700861 (28.07.2018).

Trujillo, Clorinda. 2014. "The Limits of Cyberspace Deterrence". Joint Force Quarterly, Issue 75. Washington, D.C.: National Defense University Press. URL: http://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-75/Article/577560/the-limits-of-cyberspace-deterrence/ (28.07.2018).

Walt, Stephen M. 2010. “Is the Cyber Threat Overblown?” Foreign Policy. URL:http://walt.foreignpolicy.com/posts/2010/03/30/is_the_cyber_threat_overblown. (28.07.2018).

Yarger, Harry R. 2008. "Toward a Theory of Strategy: Art Lykke and the U.S. Army War College Strategy Model", in Júnior, J. Boone Bartholomees (g.e.). U.S. Army War College Guide to National Security Issues. Volume I: Theory of War and

Strategy, 3rd Edition. Washington, DC: Department of National Security and Strategy, 43-51.

Yarger, Harry R. Strategic 2006. Theory For The 21st Century: The Little Book On Big Strategy. Strategic Studies Institute, US Army War College.

Yuill, James Joseph. 2007. "Defensive Computer-Security Deception Operations: Processes, Principles and Techniques", PhD dissertation, Raleigh: North Carolina State University. URL: https://repository.lib.ncsu.edu/handle/1840.16/5648 (07.06.2018).