UNIVERSITY OF TARTU
Faculty of Social Sciences
Johan Skytte Institute of Political Studies

Laura Oolup

CYBER AS A DETERRENT: UTILIZING OFFENSIVE CYBER CAPABILITIES IN NATO'S DETERRENCE POSTURE

MA thesis

Supervisor: Eoin M. McNamara, MSc.

Tartu 2019

I have written this Master's thesis independently. All viewpoints of other authors, literary sources and data from elsewhere used for writing this paper have been referenced.

.....

/ signature of author /

The defence will take place on ..... */ date /* at ..... / *time /* ..... */ address /* in auditorium number ..... / *number /*

Opponent ..... */ name /* (..... / *academic degree /*), ... */ position /*

Abstract

Due to the lack of attention on the strategic benefits offensive cyber capabilities hold and how they could be used as deterrents, the purpose of this paper is to contribute to the strategic thought on utilizing offensive cyber capabilities as means of cross-domain deterrence and more specifically how NATO could adopt that approach to bolster its deterrence posture. For this a case-study is conducted on NATO and its members who have offered their national cyber capabilities for NATO's use.

It was discovered that NATO has the potential enhancing its deterrence posture through the utilization of offensive cyber capabilities as means of deterrence based on the conditions set by the mainstream deterrence theories. Therefore, NATO should start with acknowledging the offensive cyber capabilities as means of its cross-domain deterrence. Second, it and the Allies should share the same understanding and communicate a clear unified message to the adversary on which effects are they willing to relay and how thereby offensive cyber operations are perceived. However, the classical deterrence theories fall short on explaining how exactly means with clandestine nature can be presented as a deterrent to the enemy. Furthermore, how to create the deterrent cyber threat by holding the functionality of the enemy's infrastructure – which should achieve strategic effects if targeted – at risk.

This confirmed the hypothesis that the classical deterrence theories neglect to explain how to develop offensive cyber capabilities into credible deterrents. Therefore, it was illuminated that the existing deterrence theory needs to be improved by acknowledging particularly two distinct features that offensive cyber capabilities hold: clandestine nature and that depending on the expected effect, the process of deploying the offensive cyber capability can be time consuming. Regarding the second feature, it requires to answer questions on how to hold the enemy at risk by threatening to harm with offensive cyber means its critical infrastructure – which should have greater strategic effect if targeted, but attacking it successfully may require long time to develop the tailored cyber weapon through - and if presence-based offensive approach is required, how to communicate that to the adversary without increasing instability between the actors.

Table of Contents

Introduction

There is an increasing talk about offensive cyber capabilities, particularly under the title of cyber weapons. One can notice it from different book titles "Virtual Weapon" by Lucas Kello (2017) or "The Perfect Weapon" by David E. Sanger (2018) and there is a reason why this topic is being highlighted. Cyberspace is the newest operational domain which includes several features that are also beneficial in the military use. While it holds a spectrum of threats, cyberspace enables to carry out an attack in a more precise and quicker way. We can notice growing number of states developing and acquiring those capabilities as more nations are establishing their cybercommands which also entail having the capability of conducting offensive cyber operations (see i.e.: Pernik 2018; Smeets 2017a).

Understandably, there is a concern over the stability in cyberspace and how to contain and deter those cyber weapons from being used (see i.e.: Rovner 2017; Morgus et al 2018). Especially, when there are still ongoing discussions about the applicability of international law in cyberspace and that deterring cyberattacks is rather problematic (see for example: Gold 2019; Geers 2010:301-302). On the other hand, there has been less discussion about using offensive cyber capabilities for deterrence purposes, namely in the context of cross-domain deterrence. Thereby, this thesis aims to contribute to the strategic thought on this matter and examine how offensive cyber capabilities could be utilized as a deterrent.

One of the reasons why this thesis focuses on utilizing offensive cyber capabilities to bolster deterrence posture is driven from the lack of focus on this potential. It can be noticed how deterrence is talked about in relation to the conventional capabilities without including cyber capabilities. As an example, Haffa (2018:108-109) has written about how NATO should for instance prevent itself from relying on nuclear deterrence when it comes to Russia, and therefore should focus on bolstering its conventional deterrence. Thereby, the cyber means have not been offered as a potential solution by being part of the cross-domain deterrence.

There are handful scholars who have analysed how offensive cyber could be used as means of deterrence (Gaycken & Martellini 2013; Lewis 2015; Smeets 2018b; Smeets &

Lin 2018; Fischerkeller 2017). However, an in-depth research that would examine the explanatory power of the classical deterrence theories in regards of utilizing offensive cyber capabilities has not been conducted. The current thesis aims to provide this knowledge. The intention is to examine the explanatory power of the classical deterrence theory concerning utilizing offensive cyber capability as a deterrent and recommend how NATO could enhance its deterrence posture through the offensive cyber capabilities.

The main research question of this thesis is: how can offensive cyber capabilities be utilized in NATO's deterrence posture? The complementary sub-questions are as follows:

- What are the conditions for successful deterrence based on the mainstream deterrence theories?
- What is the explanatory power of classical deterrence theory in regards of utilizing offensive cyber capabilities as deterrents?
- How the mainstream deterrence theories should be improved to utilize offensive cyber capabilities as means of cross-domain deterrence?

The hypothesis to be tested is that the classical deterrence theory neglects to explain how to develop offensive cyber capabilities into credible deterrents.

In order to achieve the set research goal and, it is necessary to study the nature of the offensive cyber capabilities and become familiar with its features. At the same time, the classical deterrence theories need to be examined and see which conditions they propose to achieve effective deterrence. Subsequently, it should be evaluated how the offensive cyber capabilities fit into that framework and how it applies in real-life. For this, NATO will be used as a case study which enables to test the hypothesis and assess how intact the classical deterrence theory is in regards of using the offensive cyber capabilities as deterrents. Finally, it leads to illuminating how the deterrence theory should be improved to have the necessary explanatory power in regards of offensive cyber capabilities and how NATO could utilize these cyber capabilities as means of cross-domain deterrence.

Driven from the listed research tasks, the thesis is structured into four chapters which all entail subsections. The first chapter is focusing on offensive cyber capabilities. The purpose is to familiarize with what constitutes as offensive cyber capabilities, what are

its features, which kind of strategic value these should have and what are the considerations that need to be acknowledged when using them.

The second chapter is about the classical deterrence theories. This means, among the others, the work of Thomas Schelling (1966), Robert Jervis (1976), and Patrick M. Morgan (1983) on deterrence will be examined in order to understand what deterrence is, what are its different variations and which conditions need to be met in order to ensure effective deterrence.

The third chapter aims to connect the first and the second chapters. The intention is to first give a brief overview of the academic literature related to cyber and deterrence. The purpose is once more to prove the necessity and value of this paper. This will be followed by identifying how based on the conditions set by the classical deterrence theories offensive cyber capabilities should be used to ensure effective deterrence. This also leads to hypothesizing the relation between the classical deterrence theories and offensive cyber capabilities.

Fourth and the final chapter is about conducting the case-study on NATO and the Allies who have offered their sovereign cyber capabilities for the use of NATO. The case-study will be conducted based on the framework concluded in the third chapter. This will be followed by a conceptual analysis on how good of an explanatory power classical deterrence theory have in this regard, how these theories should be improved accordingly, and how NATO could enhance its deterrence posture through the utilization of offensive cyber capabilities as means of cross-domain deterrence.

Concerning the data and the methodology, a qualitative content analysis will be conducted in order to illuminate how the deterrence theory should be improved in order to have better explanatory power on how the offensive cyber capabilities could be used as a deterrent. This requires conducting a small-N case study on NATO and its members who have offered their sovereign cyber capabilities for supporting NATO missions and operations. Empirical data needed for carrying out the case-study is formed by primary and secondary sources which cover NATO's and mentioned Allies' deterrence posture, cyber policy, and offensive cyber capabilities more explicitly. These sources will therefore include cyber and national security strategies, public statements, communiques, and relevant news articles.

It must be acknowledged, that finding the relevant and required information was not easy. Particularly, there was lack of information about the nations' offensive cyber capabilities and which effect they can relay. However, this should not undermine the value of this paper because this data was gathered for the purpose of examining the applicability and the explanatory power of the classical deterrence theories in relation to offensive cyber capabilities. Disclosed information and open communication is the core of deterrence based on the classical theories because the other side – the enemy – must receive the message of which retaliatory measures it could encounter in case of an attack. This obstacle during the data gathering could imply the lack of explanatory power the classical deterrence theories have in this regard.

Hereby, I would like to express my deepest gratitude to my supervisor Eoin M. McNamara who was always ready to assist me when I needed the help and encouraged me to carry on with my work, even if I was losing confidence in myself.

I would also like to thank my family who was always there no matter what and my colleagues at work who gave me their endless support during this process and enabled me to have the valuable time that I could write my thesis.

1. Offensive Cyber Capabilities and Their Strategic Value

The purpose of this section is to understand the nature of the offensive cyber capabilities and what kind of strategic value and military use they possess. This will later on enable to look at and analyse offensive cyber capabilities as a deterrent. The thesis will also present the limitations that need to be taken into consideration in regards of the offensive cyber capabilities.

1.1. Conceptualization of Offensive Cyber Capabilities

Offensive cyber capabilities – often called as cyber weapons – do not have a clear-cut definition, which is an inherent feature of anything related to cyber. According to David Wallace (2018:15) definitions vary depending on the degree of effect, what or who is targeted, and which means are specifically used to carry out an offensive cyber operation. As this paper is strategy-oriented, the broader understanding is hereby important. This means the intention of using a cyber weapon or an offensive cyber capability – both terms will be used interchangeably throughout this paper – is to deliberately inflict harm by aiming to weaken and coerce the enemy (i.e. Belk & Noyes 2012:21; Wallace 2018:15; Kello 2017:61).

Cyber weapon itself is not physical compared to a weapon related to any other domain. The offensive cyber capability is considered to be a malicious computer code that has the ability to disrupt, damage and/or destruct the computer systems or networks by targeting the confidentiality, integrity, or availability of the information (Kello 2017:48; Bellovin et al 2017:60). It is important to underline, though, that cyber espionage – meaning espionage where cyber means are used and hence targets the confidentiality of information – is not considered as an offensive cyber operation, which entails projecting power within or through cyberspace that the utilization of offensive cyber capabilities can cause (Joint Chiefs of Staff 2018:GL-5).

The deployment of offensive cyber capabilities can cause from minor disruptions up to physical destructions. Therefore, the offensive cyber operations can relay two types of effects regarding the physical and virtual space: logical and kinetic effects. Kinetic effect means causing damage through cyberspace in the physical space. Logical effect –

includes also cognitive effect – means conducting an offensive cyber operation in a way that will be consequential only in cyberspace and could also create cognitive effect (Noyes & Belk 2012:18). This is more of an example where the power is projected through cyberspace and information operation is facilitated by cyber means. This kind of cognitive effect can be achieved if the data is manipulated in a way that it remains below the threshold of use of force but still enables to coerce the enemy (Lewis 2018:2).

An example of the offensive cyber operation with a remaining effect in cyberspace is denial of service (DoS) attack which primarily aims to target the availability of information. As a side note, information is not limited here to the content. DoS-attacks disrupt the access or availability of services by flooding the target's system with that many enquiries which lead the system to shut down as they are not capable of handling that much information flow (Shakarian et al 2013:12). DoS-attacks – or distributed denial of service attacks if there is a network of computers involved – do not inflict remarkable damage, though. Although the infamous DDoS-attacks against Estonia in 2007 have been described as significant offences, they did not cause substantial harm (i.e. Tikk et al 2010:20)

There have been a few instances where offensive cyber operations have caused kinetic effect, but there are no examples of where such operations have resulted in casualties. The most well-known case is named after a malicious worm called Stuxnet which was discovered in Iranian nuclear facility in 2010. This sophisticated attack that destroyed certain amount of the facility's nuclear enrichment centrifuges ended up setting back the Iranian nuclear programme by few years (Shakarian et al 2013:233; Zetter 2014). Another impactful event was in 2015 when the Ukrainian energy grid was attacked causing a power outage and leaving nearly 230 000 people without electricity (Zetter 2016). Similar attack reoccurred a year later (BBC 2017).

As it can be acknowledged, the spectrum of the different offensive cyber capabilities is wide. The next task would be to understand what determines the effect. Logically, it depends on the preferences of the attacker. However, the resources determine whether the preferred effect can be materialized or not. The rule of thumb is that the greater effect is expected – kinetic effect as the outcome of the cyber offence is perceived in this paper to

be greater than the logic effect – the more resources are needed. Resources entail time, money, manpower (respective knowledge and skills), etc (Buchanan 2017a:79).

The reason is related to how cyber weapons are developed. They are tailor-made depending on the target (Kello 2017:124). This development process entails several steps which Siedler has described as it follows. First the offender needs to identify which effects it wants to have and select the target accordingly. This should be followed by reconnaissance and gaining access to the chose target's systems to become familiar with its functionality. When the necessary knowledge about the functionality of the system is gathered, the malicious code can be 'written' so that it will work only on the chosen target. After the means for conducting the offensive cyber operation has been created, it can be deployed and activated at the right moment (Siedler 2016:27-28). There might be several other steps in between – like testing the malware out in the lab before the deployment. Yet, the intention was to reflect what precedes the actual cyberattack.

The overview of the offensive cyber capabilities on what they are, which effects they can relay and how they can be deployed enables to identify the distinct features cyber weapons have. First, while the power of conventional weaponry depends on the built-in capacity, the power of cyber weapon depends on the skillset of the person who is writing the code (Rios 2009:151). Second, depending on the effect that is expected the planning and conducting the offensive cyber operation can be very time consuming. Third, as cyber weapons are customized to be reliant on the target, they cannot be used repeatedly. Although, zero-day vulnerability can be exploited exactly until it is patched (Smeets 2018a: 6, 10). Additionally, the malicious codes can be reverse-engineered. To illustrate that, the WannaCry was a modification of the NSA's produced cyber weapon which Snowden had leaked (Bellovin et al 2017:67; Baram 2018; Sanger 2018:xiii). Because cyber weapons are tailor-made, this means, they cannot be showcased before being deployed. Otherwise, they would release the information of the targeted objects and vulnerabilities to be exploited.

1.2. Strategic Value of the Offensive Cyber Capabilities

To make military use out of the offensive cyber capabilities, they must obtain some kind of strategic value. Strategic value can be defined somewhat which supports national

strategy or enables to achieve the preferred outcome of or prevent the conflict in general (Smeets 2018b:92). This can be achieved if something valuable to the opponent is hold at target. In the context of offensive cyber capabilities, this presumes the valuable objects of the potential enemy can be held at risk through cyberspace. In other words, there must be a suitable attack surface that can be exploited to ensure military advantage.

Considering the growing dependence on cyberspace both in civilian and military structures and how dependent military is on the civilian infrastructure on this matter, the attack surface is wide and increasingly expanding (see i.e. Sharma 2009:8; Inkster 2017:28; Bebber 2017:426). We have probably reached to the point, where we are unaware of where cyber component is even included. If we take the military separately, then amongst the others the conventional weapons systems, command and control, communication systems are all connected to cyberspace somehow, which makes them therefore attackable by cyber means (Bebber 2017:426; Inkster 2017:28). As Bebber has put it: "[…] effectively employing cyber power may mean the difference between winning and losing modern battles" (Bebber 2017:426).

What speaks for the military use of the offensive cyber capabilities is the environment those capabilities can be used in. Notably, cyberspace has been considered as offence-dominant (Rattray & Healey 2010:78; Buchanan 2017a: 98; Siroli 2018:114). This means gaining control through aggressive action has greater potential for success than relying on defense. Buchanan has argued this based on the geography and technology in the context of cyberspace. He claims that offensive actions have the edge over defensive ones in a certain operational domain if there are less geographical obstacles. Namely less geographical hurdles enable to attack faster. The other element that confirms the offence-dominance in the domain is the vulnerability of the technology (Buchanan 2017b:104-106; Craig & Valeriano 2016:144).

When applying it to cyberspace, both conditions are met. Geography is essentially not an issue at all, because the cyber operations are not dependent on a location. Secondly, as cyberspace is a man-made domain, it inherently includes flaws: there are exposed vulnerabilities and zero-day ones that can be exploited for the attack purposes (Buchanan 2017b:107-108). The side-effect of the offence-dominance is the desire for pre-emptive or preventive strike to neutralize the potential offender. In order to still have the

advantage, one should have a second-strike capability which is the talk peculiar to nuclear deterrence. Sharma elaborates on the cyber triad approach that should be followed in this situation. The first cyber triad is based on regular military cyber capacity and capabilities in one's country, second one entails having isolated network in an ally's country that can also help to cooperate in case defensive measures need to be activated. Third triad can be a voluntary-based network involving white hackers that can be also from private sector (Sharma 2009:11).

While planning an attack, it is important to consider the features of offensive cyber capabilities which may put certain constraints on. One of the most important aspects is perhaps what Rattray and Healey (2010:79) have pointed out: cyber capabilities are 'tactically fast but operationally slow'. Offensive cyber capabilities have the ability – as presented above – to cause great damage at high-speed but planning the event may take notable amount of time. Particularly, the more valuable object or a system of the enemy has been chosen as the target, the more cyber secure it can be expected to be and thereby requires more effort from the offender to achieve the desired effect (Siedler 2016:27-28). Thus, Buchanan has argued that one needs to be in enemy's selected systems and ready to activate the malicious code before the crisis erupts (Buchanan 2017c:43).

Taking this into account, Moore has offered two approaches how offensive cyber capabilities could be used: presence-based or event-based. Presence-based offensive cyber operation means the cyber weapon is already deployed in the adversary's network and is covertly waiting to be triggered. The consideration here is that the scope of the presence-based attack is limited, but at the same time enables to minimize the potential for the collateral damage (Moore 2018:101-102). This approach should be followed if the intention is to inflict harm that is equivalent to use of force, for instance.

The other option would be event-based offensive cyber operation. This enables to cause immediate effects which should fit better to the battlefield where instant effects are expected (Moore 2018:90, 92). Although, these type of offences – for instance DoS-attacks - can be carried out quickly, they are less sophisticated, because not a lot of effort has been directed to developing and planning those conducts. Although, the 'coercive utility' should still be there (Rid & McBurney 2012:6). Therefore, the event-based attacks

may create tactical short-term effects, but the presence-based offences have a greater potential for long-lasting strategic impact.

Which way to go depends again which effect is expected and thereby what will be the target. Conducting a cyber offence for military purposes requires having the knowledge of the cyber dependencies of the enemy. Including, what constitute valuable and vital assets for the enemy, what are its vulnerabilities, its cyber defensive and offensive capabilities (Sharma 2009:10). The attack surface in general may be broad, but this particularly makes it important to pinpoint those potential targets that would ensure the needed strategic effect.

Meaningful strategic effect can be achieved if the critical infrastructure is chosen as the target (Rios 2009:151). Critical infrastructure holds up the functionality of the society, the everyday life. Thus, if harm is imposed on that, if those critical services are somehow disrupted, it should weaken the state and have the coercive utility in this regard. And that critical infrastructure is wired and connected to cyberspace, hence creating attack surface for cyber offences, has been illustrated through what happened with the SCADA-systems in Iran and Ukraine.

Before turning to the other considerations, it must be underlined that while developing the offensive cyber capabilities and planning to deploy these, it needs to be accompanied with building up and improving its cyber defence as well. If a counter-attack will be experienced, then the state can still resist that (Sharma 2009:10).

1.3. Considerations when Utilizing Offensive Cyber Capabilities

The given overview of the offensive cyber capabilities presents the potential for achieving strategic goals via these means and how they should correspondingly be deployed. However, the limitations of using the cyber weapons must be acknowledged as well and these will be presented next.

The first constraint is related to international law. The desired effects that are intended to be achieved by the offensive cyber operation, need to follow the law (Smeets 2017b:30-31). There are ongoing discussions about how the international law explicitly applies to states' behavior in cyberspace (i.e. Gold 2019; Adams & Reiss 2018). The UN Charter

stipulates that in general the use of force is prohibited, although there are exceptions. One is self-defence and the other is if the Security Council has given a corresponding mandate for the use of force. When there is a necessity for response, it needs to be proportional, but the counterattack does not have to take place in the same domain or with the same means (DeWeese 2015:86-87, 90).

Another point when it comes to restrictions based on international law is that the means to be used cannot be inherently indiscriminate. As Bellovin et al have described it, it essentially means, these kinds of weapons are uncontrollable and do not distinct the proportionality. Putting that in the context of cyber weapon, then when deploying it, it should not affect any other objects than the original target. But even if it will, then the side-effects should be minimized. To ensure that, a thorough reconnaissance must be done in order to make the cyber weapon as precise as possible (Bellovin et al 2017:60-61, 67). However, the potential collateral damage created because of a cyberattack is a topic for a discussion.

There is a reason why we have not experienced that many cyberattacks with kinetic effects: in addition to requiring a lot of resources, but even states who have the capability to do so are self-deterred. The latter is driven from the complexity of cyberspace, the interconnectedness, the high-speed information flow and thereby instant effects that can lead to rapid escalation of the situation (Rattray & Healey 2010:79-80). During the cold war era, the collateral damage that nuclear attack could project, was accepted in the sense, it was predictable what will be the scope of the collateral damage. However, when it comes to cyberattacks – that aim to damage or destroy an object – the effect is harder to be forecasted. Therefore, decision-makers may be less willing to carry an offence out which will relay kinetic effects (Lewis 2010:2).

The offenders could lose control over their operations and it could backfire. In case of WannaCry it was noted how this was a reverse-engineered weapon which belonged to NSA. Furthermore, the scope of impacted objects and subjects the WannaCry and NotPetya ransomwares had, was remarkable. More than 300 000 computers around the world were infected by WannaCry ransomware and NotPetya also hit computer systems across the world (Baram 2018). This presents an example of how the control over preventing the spread of the malicious code is a concerning task. When the operation

Olympic Games was carried out, the Stuxnet worm was designed to affect only the Iranian nuclear facility in Natanz, but it actually infected around 100 000 other computers (Rovner 2017).

However, Rid & McBurney have counterarguments to the fear of escalation. They claim the cyber weapons can easily be controlled and the Stuxnet case is actually a good example of this. Indeed, thousands of computers were infected with the virus and this was intentional to increase the potential to infect the actual targeted system, but those infected computers were not harmed by the malicious worm (Rid & McBurney 2012:9). However, this argument and an example does not rule out the potential for cascading effects. As it has been emphasized beforehand, cyberspace is complex, particularly because it is man-made domain and there are vulnerabilities. Hence, side-effects even when a lot of effort has been into making sure it will only have an impact on the target, can still present themselves.

Another element next to opportunities in cyberspace is related to cyberspace being offence prone. The offence-dominant situation in cyberspace paves the way for instability in the domain. In theory, it should lead states to increase their procurement for offensive cyber capabilities, which can lead to cyber arms race in the context of security dilemma. Yet, it is difficult to sense cyber security dilemma in the classical way. Namely because it is difficult to track down the adversary's cyber arsenal, because it is held in secret and is in a virtual space in the form of code (Craig & Valeriano 2016:144). However, states are still communicating in one way or another that they acquire offensive cyber capabilities – mainly referred to those that can cause kinetic effects. And the preventive and pre-emptive strikes are still matter of issues in this context, which make the situation in cyberspace also more turbulent. Furthermore, Morgus, Smeets and Herr have acknowledged that WannaCry and NotPetya are good examples demonstrating "the destabilizing potential of the proliferation of cyber capabilities" (Morgus et al 2018:163).

This was an overview of what offensive cyber capabilities are, and which strategic benefits they have and at the same time what are the limitations and considerations when those capabilities are to be utilized by the states. In the next chapter the mainstream deterrence theories are to be presented and the intention is to look at how offensive cyber capabilities fit into that framework.

2. Mainstream Deterrence Theories: Conceptualizing the Logic of Deterrence

Under this paragraph, the intention is to conclude with the set of criteria that is necessary for effective and credible deterrence in general. This enables to later examine how the classical deterrence theories can explain the utilization of offensive cyber capabilities as deterrents and where they fail to do it.

First, I am going to elaborate on the existing mainstream theories on deterrence which are introduced by the authors like Thomas Schelling (1966), Colin Gray (2000), and Patrick M. Morgan (1983). In the second subsection, I am going more in detail on what ensures an effective deterrence what are the required elements, and which conditions need to be met to ensure successful deterrence.

2.1. Overview of the Mainstream Deterrence Theories

Deterrence is about preventing the enemy not to attack by persuading that the costs will be higher than the gains if it should act otherwise. The assumption is that the related actors in this instance are rational. This means their decisions are based on the cost-benefit equation and they decide to attack only if the benefits are greater than the costs (Morgan 1983:6-7, 14, 26). Deterrence is a coercive action but should be distinguished from compellence which also falls under this category (Freedman & Raghavan 2013:208). Deterrence is passive in nature because it intends to persuade the enemy not to attack through threats. Compellence, is about executing these threats to make the other side change its actions in a preferred way (Morgan 19833; Freedman & Raghavan 2013:206).

Deterrence can be applied during peace and war time. The difference is, during peacetime, the aim is to prevent an offense being carried out, yet during wartime, the goal is to contain the war (Snyder 1961:11-12). Because the nature of deterrence differs depending on the situation, the scope of this thesis does not allow to analyze the utilization of offensive cyber in both instances. Therefore, the focus will only be on deterrence during peacetime and preventing the enemy from using force.

Deterrence can be approached in different ways. There is a distinction between deterrence by denial and deterrence by punishment (Gray 2003; Snyder 1961: 14-15). The former means that the enemy should be convinced not to attack, because even if it attacks, it will fail because the defender has such resilient systems. The defender can deny the attack and the enemy is therefore not able to achieve its objectives which means it will not gain its expected gains. Deterrence by punishment, on the other hand, implies that if the enemy should attack, it will encounter retaliation. Deterrence by punishment is carried out by threatening the enemy with expensive response and counterattack which means for the enemy that it cannot carry out the offense without expecting any costs posed by the defender.

Regarding the deterrence by punishment, Jervis has noted that not only should the deterrer convince the enemy that in case of an attack it will face retaliation, but this also includes persuading the enemy that there is no offense-dominance. That the cult of the offensive – concept dating back to the *First World War era* where there was a belief in the first-strike advantage which ended up in the eruption of the world war – is not a case (Jervis 1976:67). This is important to consider, because if the enemy believes into domain's offence-dominance, then it is more eager to strike despite the retaliation. Although, if one has a wrong image of the offense-dominance, then in theory even if it acts then it will face costs, but the damage of course is already there, and the conflict potentially is already escalating. The deterrer should at the same time also be clear on whether a domain is offense-dominant or not and in case it is not, then avoid conducting any pre-emptive actions. Morgan underlines that the deterrent threats "must be reactive, not pre-emptive, in nature when implemented" (Morgan 1983:5). Hereby, the pre-emptive action means eliminating the threat in advance by conducting a corresponding offence (Knopf 2009:38).

There is also immediate and general deterrence. Morgan has described immediate deterrence – called as pure deterrence –as the situation where the opponent is posing an immediate threat and the deterrer is in constant readiness to retaliate if the evolvement of actions should require that. General deterrence is a situation when opposing sides "maintain armed forces to regulate their relationship even through neither side is anywhere near mounting an attack" (Morgan 1983:28). In principle the stability of the

situation between two or more actors determines whether general or immediate deterrence is required.

Based on the number of actors involved in the conflictual relation there is also difference between extended and direct deterrence so to speaks. Extended deterrence includes more than two actors in the relation and it means one is deterring a third party from attacking an ally (Morgan 1983:31). And another option is to differentiate types of deterrence depending on in which domain deterrence is applied or which means are used. Two most classical divide and examples of it are conventional and nuclear deterrence.

Nuclear deterrence has been considered as the most effective one, because nuclear threat is very credible, and everybody can imagine the costly consequences (see i.e. Gray 2000:257). However, relying only on nuclear deterrence would not be reasonable because it could cause more instability if every state would start acquiring nuclear capabilities. Secondly, conflict tends to remain below the level of using nuclear weapons as a proportionate way to retaliate the other. Haffa has also argued that conventional deterrence is more effective and credible than nuclear deterrence when it comes to crises where national survival is not threatened (Haffa 2018:105-106) When we think about NATO's deterrence posture in relation to Russia. Not all the Allies would perceive Russia's potential attack on Baltic countries for instance as a level of crisis where national survival is threatened to ask for nuclear response. Basically, the US – the main security guarantor for Europe – does not suffer under crisis that would undermine the national survival if Russia should carry out an attack against NATO member state, hence the probability of the US deploying its strategic nuclear weapons as a response to Russia seems to be low. Hence, NATO should not rely on nuclear deterrence only.

The most relevant type of deterrence in the context of this paper is cross-domain deterrence. This means in case of retaliation, one could launch an attack from one domain that targets something in the other. In terms of cyber the more valid definition would be that the attack launched from one domain relays effects on forces in another domain (Manzo 2011: 2). An example of that kind of situation would be taking down a drone through a cyberattack. The attack itself still happens in cyberspace, because the system being targeted is part of cyberspace, but taking the physical object from air domain down, creates the cross-domain situation.

Deterrence theory has not been freed from criticism though, and especially conventional deterrence which has failed. Criticism of deterrence has referred to uncertainty whether nuclear deterrence still holds, the rationality can be overrated particularly due to psychological bias depending on the decision-maker(s), deterrence could cause instability instead, and there are examples where conventional deterrence has failed (Haffa 2018:98; Paul 2009:3).

For instance, deterrence is criticized for its conflictual nature. In the sense that the practitioner of deterrence is not that much bearing in mind the common interests, but instead how to raise costs for the other to prevent int hat kind of threatening way it from attacking (Jervis 1976:107). Essentially, the deterrer is not thinking about cooperation, so in that regard the common interests are not part of the strategy/mindset.

More substantial critique concerns security dilemma. The enemy could receive wrong impression or perception on the deterrer's actions to bolster its deterrence posture. Namely, the opponent could perceive these steps as non-deterrent aggressive behaviour (Morgan 1983:14). This could lead to security dilemma that Jervis has described as part of spiral model.

> "They [decision-makers] frequently assume that the arms of others indicate aggressive intentions. So an increase in the other's military forces makes the state double insecure – first, because the other has an increased capability to do harm, and, second, because this behaviour is taken to show that the other is not only a potential threat but is actively contemplating hostile actions" (Jervis 1976:68).

"The spiral theorists are right to argue that the level of tensions and arms is not under the complete control of any one country" (Jervis 1976:89). Thus, the threat of security dilemma cannot be avoided and often it is coming from the deterrer neglecting which impression the enemy gets from any deterrent measures taken on (Jervis 1976:69-70). Here a good and clear communication could also enable to mitigate the problem. But this criticism does not hold as well. Even if we think that in order to avoid further escalation of arms race, for instance, and we decide to drop the weapons, we cannot be sure that the enemy will do the same. And the reason why enemy might not want to do it, is because now it has better change to gain more benefits when attacking because the defender has become more vulnerable (Jervis 1976:84-86).

Furthermore, it is suggested that an alternative to deterrence is a pre-emptive or preventive attack. Because deterrence is a strategy of influence which means the decision to attack or not is up to the enemy. However, carrying out a pre-emptive or preventive attack by yourself enables you to control the situation. Practicing controlling strategy may sound more concrete and manageable yet conducting an offense in this context may not bring along the expected results and may end up being costlier (Knopf 2009: 45, 51).

At the end of the day, it is easier to point out where deterrence has failed than where has it been successful. Unless an attack by an enemy has been conducted, it means the latter. Counting these successes is quite complex task, though. Additionally, Stein has argued that deterrence has failed as a theory only in case if the one being deterred acts despite knowing the costs will be higher than the gains. Although, in this case it could be argued that the opponent is not a rational actor then, which is, however, the presumption for deterrence and thereby failure of deterrence in this instance is not a faulty aspect of the deterrence theory – the actor just does not meet the requirement, or the assumption deterrence has as a theory (Stein 2009:60-61). Schelling argues that deterrence fails only if somebody is not committing fully to retaliate in case the enemy should attack (Schelling 1966:42).

In the following section we will elaborate more on how effective deterrence can be achieved and how to prevent the problems from occurring that the criticism of deterrence sets forth.

2.2. Mapping the Requirements for Effective Deterrence

Gray argues that deterrence theory remains the same despite which type of deterrence is applied – referring here to the type of means that are used as a deterrent. Although, he does admit the nuclear deterrence is the most reliable one, because it is hard to see that a nuclear attack as a retaliatory measure would remain at the cost level that would not overrule the gains (Gray 2000:257). Stone (2012:119) and Rhodes (2000:222) have both argued the same that it is difficult to top the nuclear deterrence, but this does not mean threat of using conventional capabilities - or other means besides nuclear weapons – cannot constitute as a costly threat to the enemy. It just requires a different approach and more work perhaps, to convince the enemy what these capabilities can cause.

There are different aspects that should be factored in when one is constructing or creating its deterrence posture. First, deterrer needs to define who is to be deterred, whether it is non-state or a state-actor. Although deterrence is built on rational thinking, it must be taken into account that with non-state actor the situation can be more complexed. Secondly, is the threat by the adversary immediate or not (Haffa 2018:97). Depending on the answer this determines whether an immediate or general deterrence is needed. Thirdly, countries may have different adversaries to be deterred and depending on the seriousness of their posed threat, deterrer's can categorize those threats and respective deterrence as type A or type B deterrence. Haffa has described those even as basic and extended where the former means your own deterrence whereas the latter encompasses contribution to deterrence to defend your allies and partners (Haffa 2018:97).

Snyder has presented more meaningful and clearer picture on the conditions required for successful deterrence (Snyder 1961: 10). Hereby, successful deterrence is considered as a situation where the enemy decides not to carry out an offense because it sees the punishment too costly or its actions will be denied which would not lead to the wished results (Paul 2009:2-3). Although, the focus from here onwards will be on ensuring successful cross-domain deterrence by punishment because the idea of this thesis is to see the use of offensive cyber capabilities as a means of deterrence.

> "Deterrence works on the enemy's intentions; the deterrent value of military forces is their effect in reducing the likelihood of enemy military moves. Defence reduces the enemy's capability to damage or deprive us […] defence value is denial capability plus capacity to alleviate war damage" (Snyder 1961:3-4).

Snyder concludes in short that successful deterrence entails three components. First, the deterrer needs to have control over the opponent by threatening its core values in case it should take offensive act. Second, the threat must be credible in the sense the enemy must be convinced the deterrer is able to retaliate in a way that can target the opponent's values which generates more costs to the enemy. What bolsters deterrent threat of retaliation are the previous conducts. Namely, the aggressor can make a prediction of the credibility of the threat based on deterrer's previous responses to aggressions, policy declarations, existing capabilities and public communication etc. Third, to bolster the credibility of the threats, one needs to showcase the will to execute the threats if the situation should require

this (Snyder 1961:10). However, Snyder also admits, there are other factors which could affect the success of deterrence, i.e. personality traits of the decision-makers (Snyder 1961: 10, 27).

Jervis emphasizes that the enemy must have a strong belief in the strength of its potential target. That the deterrer has the capability to retaliate that will be costly. If the enemy should believe the deterrer is weak, this could lead the adversary to test the limits and see how far it can go. To prevent that, the deterrer needs to convince the aggressor not to act by increasing the costs. How those costs can be increased happens only if the deterrer reflects its ability and readiness to retaliate. Jervis therefore underlines the importance of power and that firmness enables to gain leverage over the opponent. The concessions can only be made after the deterrer has outpowered the opponent (Jervis 1976: 58; 71-72). In a situation of extended deterrence, where one country is deterring a country that is posing a threat to the third state, the deterrer needs to rely on nuclear deterrence. But this is relevant instance when conventional forces cannot be used (Jervis 1976:112).

To elaborate on these conditions even more, lets start with having a clear communication line with the enemy. First, the message and thereby the threat must be clearly communicated so that the one being deterred understands it as well. This is necessary to keep in mind and to avoid mixing the preparedness and deterrence together. Namely, one could have the capabilities and therefore the ability to retaliate, but until it is not directly communicated to the other side that these weapons will be used if one should conduct an offense to its direction, the other will not feel itself deterred (Morgan 1983:33-34). Thing that should be taken into account is that while forming the message, it must be thought through how the enemy might interpret it and how it can believe the threat is credible. If those questions are answered that can be used to form a message (Jervis 1976:112-113).

The threatening should not be limited to words. It must be reflected in certain military preparations. And as noted, if the government had previously been engaged in a conflict and thereby has record using force, it only increases the credibility (Jervis 1976: 59, 61; Morgan 1983:28, 35; Paul 2009:19). Schelling has stated how actions enable to make the threats more credible, because they ‘are less ambiguous’ as these literally showcase the will and the capabilities to execute a threat (Schelling 1966:150). Yet, the importance of verbal communication enables to draw the red lines and express what is unacceptable

behaviour and clarify how things would turn out if an offense would be conducted against one (Schelling 1966:154). Verbal communication has the power to prevent any misunderstandings, which only the deeds could otherwise lead to.

Furthermore, the verbal message and the necessary military capability needs to be coupled with the political will of the deterrer to literally indicate that the retaliatory measures will be used in case of an attack (Jervis 1976: 58; Morgan 1983:38). What Paul considers as one of the prerequisites for deterrence is that there is a constant potential for war at the times of 'deterrent relationship' (Paul 2009:7).

Concerning communicating a clear message on what will be the retaliation, there is also a suggestion to keep those threats ambiguous in order to prevent the subject of deterrence to know what exactly are the deterrer's capabilities. This knowledge could put the deterrer in a vulnerable position as this could be exploited by the enemy. On the other hand, if the threats or the content of the threats remains ambiguous, it could lead to miscalculations that could result in the escalation of the conflict (Crawford 2009:290).

The capabilities used as means of deterrence, should also be used in a wise way. Knopf has proposed that all the morally acceptable means, including non-traditional capabilities, should be used for the purposes of deterrence (Knopf 2009:36). The question here is what is morally acceptable and what is not. Second, when it comes to capabilities, the amount of them is not necessarily the most important aspect. As Gray has argued, deterrence does not work in a linear way. This means, deterrence will not become twice as more successful if the number of weapons is doubled (Gray 2000:257). Stone has suggested that in order to bolster the credibility of conventional deterrence, the narrative around the respective means and what they can cause, is necessary (Stone 2012:117). It is a matter of constructing the effect of the weapon and how one is communicating the threat caused by that to the enemy. But as mentioned before, words are not enough, it is also important to demonstrate the capability of these weapons (Stone 2012:117).

Morgan also points out the importance of considering the psychological traits and aspects of the enemy which have significant impact on one's decision-making process (Morgan 1983:32). Stein underlines that the limitations of deterrence are the individual psychological features of decision-maker(s) and the different political and hence strategic culture (Stein 2009:78). The nature of the decision-maker(s) needs to be factored in and

thereby try to alter the decision-making and the cost-benefit calculations that lead to the decision (Morgan 1983:33, 50). Moreover, it is also important, who is the leader of the country that is practicing deterrence. That leader needs to be credible with its threats as well in order it would impress the one being deterred (Morgan 1983:51).

While the assumption is that our enemy is a rational actor and our aim with deterrence is to make the costs that high to our enemy, so it will not attack, then we need to know what constitutes as a cost to our enemy. Morgan points out that for this we need to know about the enemy's goals, resources, and alternatives. Moreover, what constitutes as the opponent's most important values are "national survival, retention of power and prestige, and sovereign independence" (Morgan 1983:58; 72).

What also affects the success of deterrence, is about the leadership structures and who makes the decision. For instance, Morgan argues that groupthink tends to lead to taking greater risks (Morgan 1983:61). There are also psychological biases depending on the decision-maker(s). This could create instances where the costs may clearly be higher than gains, but the decision-maker may be a great risk-taker or there may be other reasons why despite the odds, the enemy still decides to attack and could lead to the failure of deterrence. Paul does, however, differentiate two types of decision-makers based on their rationality: instrumental and value-based. The ones who have value rationality, are more committed to attack and accept higher risks (Paul 2009:5-6).

Although, psychological aspects are important, and they need to be factored in. This is what Jervis has argued: "We should not overlook the extent to which statesmen look to the future, seek to manipulate the levels of tension and hostility in order to reach their goals, and frequently succeed" (Jervis 1976:90)". Yet, taking the more general approach, there are other perhaps more technical conditions that need to be met before taking the next step and starting to tailor the deterrence approach to be suitable for the specific enemy. This paper argues the way how one practices deterrence comes from who is to be deterred. Therefore, the psychological aspects determine how deterrence should be 'packaged' in every case, but the core aspects – credibility, communication, and capability - of deterrence still remain there despite who is the deterree in psychological terms.

How to mitigate the issue of security dilemma, but at the same time practice deterrence? Jervis suggests using the right weapons. One should procure the weapons in a reasonable quantity, which would not create the image of the deterrer being aggressive (Jervis 1976:111). Although, identifying the fine line there is a complex issue. Keeping in mind the essence of deterrence – increasing the level of costs by threatening to retaliate in case the enemy decides to attack – then retaliating is in some way aggressive. But, there is a difference between proportionally improving your weaponry in relation to enemy's or doing that disproportionally. Hereby, the communication is also the key by letting the other side know why certain weapons are procured. What Paul also argues is that each category of a weapon has a different deterrent value. Therefore, the threat-level differs depending of the class of the weapon (Paul 2009:7). This raises questions on how credible are certain type of weapons against a different one? Does asymmetry of weapons work in the deterrent relationship? That's a question that will be kept in mind later on when the intent is to cover the question from the cyber perspective: is cyber weapon a credible tool to deter enemy's actions carried out by conventional capabilities?

The question is more, when the threat is perceived costly by the enemy. First, the threats are pertinent if the enemy is weak, it values highly its citizen's quality of life, it is risk-averse, and it neglects to have a long-term strategy (Jervis 1976:100-101). Second, the threats work if the enemy has the image of the deterrer as the opposite that was just described under the first circumstance. In other words, the deterrer is strong, it is ready to retaliate at the expense of its citizens, it has long-term strategy and is risk taker (Jervis 19767:101). Third situation where threats - therefore deterrence - work is when the enemy considers the "costs of retreating" low because no ,core values, principles are threaten for instance (Jervis 1976:101).

Schelling has argued "Deterrence rests today on the threat of pain and extinction, not just on the threat of military defeat. […] . If the weapons themselves are vulnerable to attack, or the machines that carry them, a successful surprise might eliminate the opponent's means of retribution" (Schelling 1966:23). Schelling's 'today' may have been 50 years ago, but his stance is that the cost must be damaging in its nature (Schelling 1966:3-4, 10).

What Schelling also emphasizes is that when forming the threats, deterrer needs to be aware of what the opponent values. What are the spots that it cares about. What makes it suffer and feel the pain if it should be under attack and damaged significantly. Also, next to making sure the opponent knows about the costs it could face in case it should inflict an attack the deterrer must also be clear about what are the assurances and thereby, what are the red lines and what can be done to avoid experiencing any retaliation (Schelling 1966: 3-4, 23).

Schelling argues that threat can be made through commitment: "[…]to incur political involvement, to get a nation's honour, obligation, and diplomatic reputation committed to response" (Schelling 1966:35). What needs to be considered when deterrent threats are being formed? Snyder suggests the enemy is taking into account four elements to do the risk calculation: what are the war objectives, what will be the retaliatory costs, will there be a response by the deterrer and is it possible to end up as a winner after the sequence of responses previously (Snyder 1961:12).

Threats are credible if the opponent can be convinced that the deterrer has accepted the risk of war which may be the result of the execution of its threats in case of an attack (Schelling 1966:99). To make sure, the opponent has this understanding, the deterrer needs to make transparent and deliberate steps, but without pushing the situation too far. The metaphor Schelling uses is trip-wire. He believes that laying it down in a tolerable location and reflecting in a clear manner to the deterrer that in case that should be crossed, there will be an automated response and therefore potential war (Schelling 1966:100). There is no room for uncertainty if you want deterrence to work (Schelling 1966:101). Thereby communicating the message in a clear manner to the enemy what are the red lines, what happens if these are crossed and how the present military actions is must have element.

On the other hand, uncertainty may serve the benefits for deterrence as well. Schelling argues that if there would not be a clear prospect on how the execution of threats could act – whether the results remain in the scope what was expected or they get out of control – is actually necessary to have. To put in in another way, the requirement is to be clear on that the opponent will face retaliation in case it should attack. However, it is beneficial to have an ambiguous vail over where the execution of threats could lead to: whether it

will lead to war or not. This serves the purposes because, if there would be clear understanding of the results of the retaliation and that there will be no war, then the costs for the opponent will also decrease and it sees conducting an offense as more beneficial. On the other hand, if it is certain that war will break out anyhow, then it would be smarter to begin with it directly (Schelling 1966:104). The logic is if the risk is unclear, it intimidates more and increases the costs. In comparison, the deterrer's risk calculation is based on Snyder's understanding rather similar. The deterrer as a rational actor as well aims to minimize the costs for itself when selecting the way to retaliate (Snyder 1961:13).

To conclude, the core aspects of deterrence are capability, credibility, communication. If one wants to practice deterrence, it needs to have appropriate weapons and communicate clearly that if the opponent should attack, it will encounter great costs because there is the intent and political will to inflict retaliation (Freedman and Raghavan 2013:208; Jervis 1976: 79; Morgan 1983:58; Paul 2009:2). Or as Knopf has written:

> "To turn deterrence from an abstract concept to a specific strategy or tactic, one has to become more specific about the ends, ways, and means. What ends does not seek to prevent, what means will be employed to do so, and in what way or ways will one seek to influence decision making" (Knopf 2009:41)?

At the end of the day, there is no detailed deterrence equation that would definitely result in successful deterrence, because it is not possible to entirely calculate what constitutes as costs to the one aimed to be deterred. Moreover, a threat perceived by one may not pose a threat to another – each enemy is different (Morgan 1983:72; Jervis 1976:112). As Schelling has written, "deterrence involves setting the stage – by announcements, by rigging the trip-wire, by incurring the obligation – and waiting. The overt act is up to the opponent" (Schelling 1966:71).

3. Cyber as a Deterrent: Theoretical Overview

In this section, first an overview on the existing literature about the relation between cyber and deterrence is given. It will be acknowledged that there has primarily been more focus on deterring cyber-attacks and less on utilizing offensive cyber capabilities as a deterrent in cross-domain deterrence. This overview will be followed by applying the mainstream deterrence theory to offensive cyber capabilities and creating respective framework on how the offensive cyber capabilities should be used as deterrents. This framework will be used as the basis for analysing later on NATO's potential for bolstering its deterrence posture through offensive cyber capabilities and what is the explanatory power of the classical deterrence theories in this regard.

3.1 Academic Discussion on Cyber and Deterrence

Academic literature on cyber and deterrence has put noticeable effort on tackling the question whether and how cyberattacks can be deterred – concept that is also known as cyber deterrence (see i.e.: Kello 2017: 196-211; Libicki 2009; Morgan 2010) – and less seeking to examine how offensive cyber capabilities could be utilized as a deterrent in other operational domains besides cyber. Despite the ongoing debate on deterring cyber-attacks, no consensus seems to have been reached on a right approach which could be driven from the different nature of cyberspace and cyberattacks (Friis & Ringsmose 2016:3; Kello 2017:167, 198; Saltzman 2013:44). For instance, one of the hurdles in that regard is attribution. It is not the easiest to find primarily technical evidence on who was responsible for the attack and hence, it is difficult to identify who is supposed to be retaliated (see i.e. Geers 2010:301). While deterring cyberattacks is still being undertaken for understandable reasons, more attention should be given to how the offensive cyber capabilities could be used in the cross-domain deterrence. On that note and how Allies have offered their national offensive cyber capabilities for NATO's use, Herr & Schneider (2018) have said:

> "Sharing offensive cyber capabilities raises the question of whether cyber operations can extend effective deterrence to NATO partners. There seems to be little focus on using these operations to deter conventional or nuclear attacks on NATO countries, but this may evolve."

There are some scholars who have written about utilizing cyber as a deterrent. Gaycken and Martellini (2013) present in their paper different approaches in this regard. They conceptualize cybered deterrence or cyber as a deterrent by utilizing "hacking capabilities to threaten to attack an adversary's information technology" (Gaycken & Martellini 2013:3). The more accurate definition of this phenomenon is presented by Jason Rivera who defines it "as the mechanism through which nation-states can communicate proportionate, reciprocal, and credible military power effects through cyberspace that strategically affect their adversary's decision making calculus" (Rivera 2015:8).

It is not surprising that foremost these actors can be held at risk with a cyber threat who are highly dependent on cyberspace in their everyday governance at the wider spectrum (Gaycken & Martellini 2013:3). This is so because there are potentially more vulnerabilities that can be exploited and therefore more ways to hold the actor at risk. Gaycken and Martellini list various potential doctrines one can adopt for creating its cybered deterrence posture. For instance, the deterrer could try to create general threat in cyberspace or in order to avoid escalation, one could threaten to target only certain systems or threaten with information operations where cyber means are used (Gaycken & Martellini 2013:4-5).

Fischerkeller (2017:104) argues that when thinking of incorporating offensive cyber operations into conventional deterrence, certain elements need to be taken into account. These include the nature of the cyber capabilities and cyberspace; the potential credibility of the use of offensive cyber capabilities; "the need to effectively communicate resolve; and the ways in which imposed and incurred costs can be estimated" (Fischerkeller 2017:104). Gaycken and Martellini argue that the credibility of cyber threat can be proven through the investments into the specialized personnel who handle the cyber weapons and as a second tier, is showcasing which cyber effects they can create (Gaycken and Martellini 2013:6). To add, Smeets & Lin – who wrote about the advantages offensive capabilities can serve as a military power - claim in regards of deterrence that only states with credible reputation in offensive cyber capabilities could be effective in deterring adversary's military actions by cyber means (Smeets & Lin 2018:57-58). Fischerkeller additionally underlines the importance of reflecting the subject of deterrence if there is a risk of escalation, how would it end up (Fischerkeller 2017:104).

James A. Lewis (2015) has written about NATO and its relationship with the offensive cyber operations. Particularly, he raises concern over NATO's failure of incorporating offensive cyber capabilities into its military strategy. In that regard he poses an accurate question: "can any military force credibly claim to have advanced capabilities if it does not include offensive cyber operations in its arsenal?" (Lewis 2015: 2). We will president the evidence later, but as the article was written in 2015, since then NATO has taken steps towards incorporating offensive cyber capabilities into its force structure. Establishing the Cyber Operations Centre and Allies offering their offensive cyber capabilities for the use of NATO illustrate that (NATO 2018; NATO 2019:2). Yet, the question he posed remains valid and with his work he has given notable contribution to the debate on seeking to make the better use of the offensive cyber capabilities. Lewis expresses the belief that if offensive cyber capabilities bolster the deterrence posture if these are integrated into NATO's force structures (Lewis 2015:2-3).

The necessity and value of considering cyber as a deterrent and especially in the context of cross-domain deterrence is driven from two moments particularly. First, as it has been already studied, cyber means can be utilized as individual weapons to cause strategic effects or in compliance with using the conventional means for instance. Second, offensive cyber capabilities should have a great deterrent value exactly because it might have cascading effect and not only affect the target. Why these features can be beneficial, is because Schelling (1966:99, 104) argued that if the deterrer accepts the risks of escalation, this would bolster the credibility of the threat. Furthermore, as the offensive cyber capabilities can create effects at a wide spectrum it is appropriate to talk about offensive cyber capabilities and utilizing those as means of deterrent to ensure stability. Fischerkeller (2017:103) has argued that because of the high degree damage they can generate, the offensive cyber capabilities should increase the cost level for the adversary.

It is necessary and justified to look at utilizing offensive cyber capabilities as deterrent. However, the academic discussion today misses the input on discussing how intact the classical deterrence theories are to offensive cyber capabilities and how well existing theories explain and guide how offensive cyber capabilities should be used to ensure effective cross-domain deterrence. Therefore, this paper intends to fill this conceptual void.

Next, the set of conditions that need to meet in order to have successful deterrence based on the mainstream deterrence theories will be applied to offensive cyber capabilities to see how these should act as deterrents.

3. 2 Cyber as a Deterrent based on the Classical Deterrence Theories

After getting familiar with the offensive cyber capabilities and the mainstream deterrence theories, it will be examined how offensive cyber means should be utilized as a deterrent based on the classical deterrence theories. Later this framework will be tested on NATO which enables us to identify where the classical deterrence theories remain thin to explain how offensive cyber capabilities can be successfully used as deterrents. This subsection will be concluded with presenting a hypothesis on whether the classical deterrence theories are enough for determining how offensive cyber capabilities can be utilized as means for successful cross-domain deterrence.

As this thesis is talking about the utilization of offensive cyber capability as a deterrent, then these capabilities are considered as retaliatory measures. This means, the utilization of offensive cyber capabilities is analysed in the context of deterrence by punishment. To ensure the effectiveness of this type of deterrence, largely three conditions need to be met that were identified in the second chapter: acquiring the relevant offensive capabilities, confirming the credibility of using them as retaliatory measures and lastly communicating this threat in a clear manner.

Regarding the first condition, there is a wide array of offensive cyber capabilities which were presented above. Which kind of cyber weapons are needed for the deterrent purposes, depends on what constitutes important to the adversary. There could be different options, but for military use and to achieve strategic effect which will be costly for the enemy, then disrupting, damaging or destroying enemy's critical infrastructure should achieve that (see i.e. Rios 2009:151). Therefore, the offensive cyber capabilities that should be procured should have the ability to cause also kinetic effects. At the same time, having the capabilities to relay logic effects should not be denied because the intention is to make it costly for the enemy. And what constitutes costly to the enemy, depends on what does the enemy value (see i.e. Sharma 2009:10). Critical infrastructure

fits into that category because the functionality of the society and the military rely on it. This means, one needs to have the capability to attack an industrial control system.

To make the threat credible, the existence of those capabilities and that they are operational need to somehow be presented. Sharma proposes war games and even conducting certain attack against the adversary that is being deterred (Sharma 2009:11-12). An option would be to conduct exercises and showcase in that kind of test environment the ability to attack successfully SCADA-system for instance. Previously carried out offences also bolster the credibility. Hence, Smeets and Lin (2018:55) have said that offensive cyber capabilities are effective in deterrence if the deterrer has credible reputation in this area. However, the actual ability and readiness to conduct a cyber offence is difficult to be proven because of the clandestine nature of those. Otherwise, the target would be exposed, and the adversary can patch the vulnerability.

This leads to another complex issue of how to clearly communicate to the adversary that the threat is there, and one is ready to materialize it, if any kind of an attack should be carried out. The problem stems from the offensive cyber operation resulting effects instantly, but the preparation and planning for it takes time (see i.e. Siedler 2016:27-28). This means, if an attack against critical infrastructure is considered a as a retaliatory measure, the respective cyber weapon needs to be deployed into the systems in advanced and be ready to be activated. However, disclosing the presence in one's systems of critical infrastructures is a fragile approach. On the one hand, indeed, it is a clear message of the capability to retaliate. Readiness to actually activate it, is another question. However, demonstrating the presence in the adversary's systems can cause instability in general.

Hereby, it is hypothesized that the mainstream deterrence theories neglect to explain how offensive cyber capabilities can be used as a deterrent for successful deterrence by punishment. Particularly, it is a complex matter making the threat credible without initiating instability.

4. Towards Theory Proposing on Utilizing Cyber as a Deterrent: Case-study on NATO

With this section the aim is to on the one hand identify, how NATO could bolster its deterrence posture by utilizing offensive cyber capabilities as deterrents in the cross-domain deterrence. At the same time, the idea is to illuminate how the classical deterrence theory should be improved to have the explanatory power for utilizing offensive cyber capabilities as means of successful cross-domain deterrence.

To achieve the described goal, a case-study on NATO's cyber policy will be conducted. Particularly, NATO's cyber policy in the context of cross-domain deterrence – looking at the potential of utilizing cyber as a deterrent to prevent the adversary (Russia) from using force against NATO's Ally - will be studied. The aim is to see which conditions identified in the previous section NATO is able to meet and which it does not and what NATO respectively should do in order to use offensive cyber capabilities as means of its deterrence posture. Based on that, the findings for illuminating the classical deterrence theory in regards of utilizing offensive cyber capabilities as deterrents will be presented.

4.1. Research design

A case-study will be carried out in order to identify how NATO could utilize offensive cyber capabilities to bolster its deterrence posture and illuminate how classical deterrence theory should be improved to have a stronger explanatory power for utilizing offensive cyber capabilities as deterrents in the cross-domain deterrence. Case-study findings enable us to identify newly emerged conditions or variables the developed theory does not include but should (George and Bennett 2005:109-110; 115).

Rationale for choosing NATO as the subject of the case study is largely based on three aspects. First, numerous of its members have developed offensive cyber capabilities and established cyber commands or respective military units – including the US as the most credible cyber power among the others – which reflects NATO's potential offensive cyber capabilities (Pernik 2018). Furthermore, the US as a member of NATO has conducted a cyber offense called Operation Olympic Games that caused physical destruction on Iran's nuclear facility (Zetter 2014). This is relevant to ponder as it reflects country's credibility

in offensive cyber capabilities that Smeets and Lin considered important in the context of deterrence (Smeets & Lin 2018:64).

Moreover, NATO itself is becoming more proactive in the use of cyber capabilities which has resonated with declaring cyberspace as a separate operational domain and establishing cyberspace operations centre (NATO 2016; NATO 2018). Finally, bearing in mind the current threat environment and in respect to whom NATO's deterrence posture is directed to, it would be strategically valuable to know whether and how it could utilize its capabilities in a full spectrum to enhance its deterrence posture.

This does not only require knowing NATO's general cyber policy when it comes to carrying out offensive cyber operations, but also perceptions and the respective capabilities of the allies themselves. Therefore, small-N case study will be conducted, which is driven from NATO being an intergovernmental organization. Case selection is based on purposive sampling and it includes those member states who have offered their offensive cyber capabilities for NATO's use and announced it at the Brussels summit in 2018. These are the United States, the United Kingdom, the Netherlands, Estonia, Denmark (Arts 2018:2).

The necessary data required for conducting the small-N case study is formed by primary and secondary sources which cover NATO's and mentioned Allies' deterrence posture, cyber policy, and offensive cyber capabilities more explicitly. These sources will therefore include cyber and national security strategies, public statements, communiques, and relevant news articles. Qualitative content analysis will be carried out – the used coding system is presented as figure 1 - because it helps to systematize the information in a clearer manner on which conditions (Saldana 2013:9; Schreier 2012:2-3) – presented in the previous chapter - NATO meets with its cyber policy in terms of achieving effective cross-domain deterrence based on the classical deterrence theories. For obtaining the required data from the mentioned documents and sources, a programme MAXQDA is used as it facilitates and makes it easier to create a clear coding system and allocate segments from the texts accordingly.

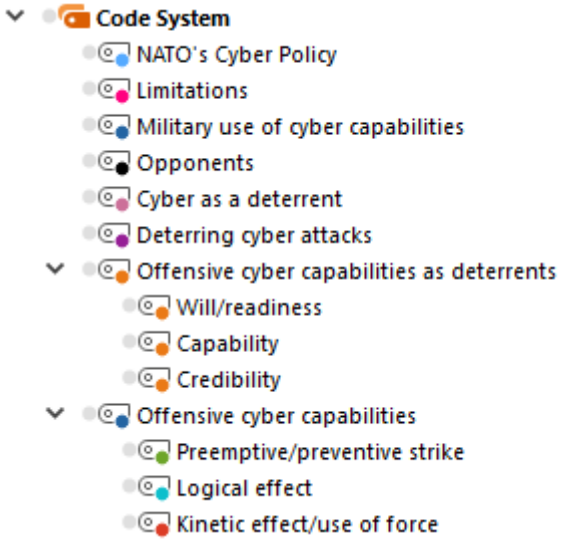

Figure 1. *Coding System (Author).*

The case-study will be followed by a conceptual analysis which will have twofold outcomes. First, the intention is to present how NATO could utilize the offensive cyber capabilities as deterrents as part of the cross-domain deterrence. Second, it will be illuminated how classical deterrence theory should be improved to better explain the utilization of offensive cyber capabilities. As the purpose is to make a valuable contribution to the strategic thought on the issue of utilizing offensive cyber capabilities as a deterrent, it is justified based on the recommendations by George and Bennet (2005: 266-267, 271), to deconstruct the abstract model – that the classical deterrence theory is - and see the variations of it which are driven from distinct characteristics of the offensive cyber capabilities.

> "…, a general concept is not itself a strategy; rather, it needs to be converted into a particular strategy. There is only one concept of deterrence and one concept of coercive diplomacy, but there are quite a few different deterrence and coercive diplomacy strategies" (George & Bennett 2005:271).

There are two reasons for doing theory illuminating, rather than theory-testing on the deterrence theory. First, we do not have evidence where offensive cyber capabilities have been utilized as deterrents in cross-domain deterrence. Therefore, we do not have a case to test the theory on. However, the empirical data in regards of NATO and its today's relation with the offensive cyber capabilities is expected to draw a picture on how these capabilities are presented to the publics, which distinct characteristics of the offensive

cyber capabilities can be sensed in that regard and how these correspondingly align - or do not - with the set of conditions classical deterrence theories suggest for having effective deterrence.

Secondly, illuminating deterrence theory in regards of the utilization of the offensive cyber capabilities as a deterrent, enables to make the first step towards middle-range theory. Based on George & Bennet's (2005:266-267) claim – who have written a book on theory development in social sciences – middle-range theory would have better explanatory power on this phenomenon than general theory of deterrence would have. However, the intention with this thesis is not to develop a middle-range theory on utilizing offensive cyber capabilities as a deterrent because it would be beyond the scope of this paper. Rather, the intention is to give input for developing such kind of theory by presenting where the classical theory on deterrence could be improved correspondingly.

4.2. NATO and Offensive Cyber Capabilities

When cyber is discussed in the context of deterrence within NATO, it is primarily limited to deterring cyberattacks and not as a means in cross-domain deterrence. This can be noticed for instance in NATO's Strategic Context adopted in 2010 (NATO 2010) and its Readiness Action Plan which also encompasses a message that challenges in the Eastern and Central European can be mitigated through measures limited to land, sea, and air (NATO 2017). Yet, the intention with this section and thesis is to broaden the strategic thought on incorporating offensive cyber capabilities in a way they would deter the opponent – Russia – from conducting an attack in any operational domain on NATO member.

NATO's focus with its cyber policy has been on cyber defence (see i.e. NATO 2014; NATO 2018; NATO 2019:1; Arts 2018:3). Despite the focus on the defensive side and deterring cyberattacks, NATO's cyber policy has evolved in a way that gives substance to incorporating offensive cyber capabilities into NATO's military structures in a way that those could be utilized as means of cross-domain deterrence that would enhance NATO's deterrence posture correspondingly. As the NATO official Dan Lewis has said regarding Allies offering their offensive cyber capabilities for NATO, "NATO's resolve

to deter aggression against its member states hasn't changed. It simply now extends from the physical world to the virtual one" (Lewis 2019).

NATO's most remarkable cyber-related milestones originate from its summits of 2014, 2016, and 2018. At the Wales Summit in 2014, it was declared that cyber-attack can be the reason for triggering the clause of Article 5; at Warsaw Summit 2016 cyberspace was declared as the separate operational domain like the air, land, and sea are; and lastly, during the Brussels summit in 2018, five Allies announced their readiness and willingness to give their sovereign cyber capabilities for the use of NATO (Davis 2019: 1; NATO 2014; NATO 2016; NATO 2018; NATO 2019). These actions mean NATO is integrating cyber into its general missions and operations (Davis 2019:6). What further facilitates this is the decision of establishing Cyber Operations Centre in Mons. This Centre, as its deputy director Don Lewis has described it, "functions as the theatre component for cyberspace, just as the geographic commands do for their respective operational domains" (Lewis 2019).

Concerning the offensive cyber capabilities, it must be underlined that NATO is not going to develop those on its own but as some allies already had done it, they can offer their cyber capabilities to support the NATO's operations and missions. When the cyber capabilities are to be used in the context of NATO's area of operation, Allies have the control over the utilization of these capabilities (NATO 2019:2). The Cyber Operations Centre has the coordination role in this context and it has been underlined that the actions still remain defensive and will be in compliance with the international law (NATO 2019:1). However, there is ambiguity around when those cyber effects are to be used which the Stoltenberg's statement right after the Brussels summit in 2018 also presents:

> "When and if and how we will use our national cyber capabilities in NATO missions and operations I think it will be very wrong if I started to speculate now about that. That will only create unnecessary uncertainty, so we will decide when we use that in the different missions and operations depending on the circumstances" (Stoltenberg 2018).

The initial five Allies that have offered their offensive cyber capabilities for NATO, were Estonia, Denmark, the Netherlands, the United Kingdom, and the United States (Danish Ministry of Defence 2019; The Danish Government 2018:7; ERR 2018; Arts 2018:2;

Mattis 2018). It is also known that Estonia, France, Germany, the US, Italy, the Netherlands, Spain and Turkey have established their own cyber commands or equivalent services and almost all of them in addition to Czech, Denmark, Finland, the UK and Norway possess or are developing offensive cyber capabilities (Pernik 2018:1). Because the Allies' capabilities constitute as NATO's capabilities, it is necessary to look at what can these five aforementioned Allies offer in terms of offensive cyber capabilities and what are their impressions on utilizing those.

Denmark has a unit within the structures of the Danish Defence Intelligence Service that can carry out defensive and offensive cyber operations (Danish Ministry of Defence 2019; Defense News 2015). These operations ought to be carried out whether independently or "in support of other military means" (Danish Ministry of Defence 2019). Estonia has established its own cyber command in the structures of the Estonian Defence Forces. The Estonian cyber command is missioned to secure the functionality of the information and communication systems of the area of governance of the Estonian ministry of defence, and its allies and in necessity be ready to conduct active cyber defence (Pernik 2018:5-6). Their activity thereby includes developing offensive cyber capabilities and Estonia also has offered its sovereign capabilities for NATO as well (Majandus- ja Kommunikatsiooniministeerium 2019: 5; Riigikantselei 2017:2). The Netherlands has the Defence Cyber Command within the structures of the Royal Army (Ministry of Defence 2019). The offensive cyber capabilities, which are only intended to use against the military targets, are being developed and they include the capability of "infiltrating computers, computer networks and weapons and sensor systems so as to influence information and systems" (Ministry of Defence 2019; Royal Netherlands Army 2018:15). As part of the NATO's enhanced Forward Presence (eFP) mission, the Netherlands has deployed its Cyber Mission Team as a military contribution. It has not been disclosed, though, whether it also has offensive cyber capabilities (Folmer 2018; Pernik 2018:7).

The UK tends to use the offensive cyber capabilities in the context of deterring cyber-attacks (Fallon 2016; HM Government 2016). However, the UK does declare it has the offensive cyber capabilities which should be flexible in nature and function as a deterrent but as an operational capability as well (Compotroller & Auditor General 2019:6; HM Government 2016:10; 51).

> "Offensive cyber capabilities involve deliberate intrusions into opponents' systems or networks, with the intention of causing damage, disruption or destruction. Offensive cyber forms part of the full spectrum of capabilities we will develop to deter adversaries and to deny them opportunities to attack us, in both cyberspace and the physical sphere. Through our National Offensive Cyber Porgramme, we have a dedicated capability to act in cyberspace and we will commit the resources to develop and improve this capability" (HM Government 2016:51).

The UK has a National Offensive Cyber Programme through which the offensive cyber capabilities are developed (Fallon 2016). It was marked in the 2016 cyber security strategy that in order to have the necessary offensive cyber capabilities, more investments will be made into the National Offensive Cyber Programme and that Armed Forces will also be educated and trained so that they have the required skillset to deploy offensive cyber capabilities which are being integrated into military planning (Fallon 2016; HM Government 2016: 51).

What is notable illustration of the UK's will and capability conducting offensive cyber operations which should boost its credibility accordingly, is the cyber-war gaming it did in 2018. This entailed the UK defence officials practicing causing power outage in Moscow (Detrixhe 2018). Additionally, the UK has carried out cyber offences as real operations. For instance, it has launched cyber campaigns against ISIS in Syria and Iraq (Bond 2018; Smeets 2017a). The latter operation has also been underlined by Stoltenberg:

> "Some Allies have successfully used their cyber capabilities against ISIS in Iraq and Syria: to suppress terrorist propaganda, hinder their ability to coordinate attacks, and to protect forces on the battlefield […] We have been able to disrupt the cyber networks of Daesh to reduce their ability to recruit, to fund, to communicate. And these capabilities have been used by NATO Allies against Daesh and these are the same kind of capabilities we now are creating the framework to integrate into NATO missions and operations" (Stoltenberg 2018).

The US has been considered the cyber power who "has the most advanced cyber capabilities within NATO" (Arts 2018:2). Therefore, it is not surprising that when the Defence Secretary Mattis at the time pointed out during the announcement of the US

offering its cyber capabilities for the use of NATO is already willing to do so today (Mattis 2018). The US new cyber strategy allows military to carry out cyber operations to protect its systems, networks and national critical networks in general (Nakashima 2018). Furthermore, it seems that the utilization of the offensive cyber capabilities is not considered limited to deterring only cyberattacks as it is said, the intention is also to "ensure the US military's ability to fight and win wars in any domain, including cyberspace" (Department of Defense 2018:1-2).

The offensive cyber capabilities the US is developing, have the purpose to counter cyber-attacks, but at the same time be considered as any other means during war time. The offensive cyber capabilities should be flexible. This means, the US should have in its use various offensive cyber capabilities that can cause different types of effects depending on the situation and necessity (Department of Defense 2018:3). They are aimed to use as retaliatory measures in kind to cyberattacks but also as means to enhance the US military advantage in any way. Therefore, in the strategy it is mentioned that "during wartime, US cyber forces will be prepared to operate alongside our air, land, sea, and space forces to target adversary weaknesses, offset adversary strengths, and amplify the effectiveness of other elements of the Joint Force" (Department of Defence 2018:1).

However, there is not that much information out there what exactly are the capabilities the US obtains. Although, certain public announcements give some ideas in this regard. For instance, it has been announced that the US is procuring a Unified Platform that should support as a mission capability the US cyber command in its defensive and offensive cyber operations (Pomerlau 2019; Northrop Grumman 2018). Moreover, to develop the offensive cyber capabilities and to in general improve the work and operability of the US Cyber Command, it has allocated $75 million – which is 70% more compared to previous year - in the fiscal year of 2019 to do that (Pomerlau 2019).

The US has examples of conducting offensive cyber operations that reflect both the capabilities and willingness to create logical and kinetic effect. The most recent example concerning logical effect is related to the US cybercommand's actions in regards of the Russian Internet Research Agency. The US assault on Russian Internet Research Agency (IRA) located in St. Petersburg was a pre-emptive approach to prevent Russia's troll factory to conduct information operations and thereby meddle with the US midterm

elections in 2018. The strike entailed cutting the IRA out of internet. This was a notable operation, because it was the first kind of the US to launch that kind of offense against Russia (Nakashima 2019).

The Stuxnet case that has been brought up in this paper for several times now is the example of the US being able to conduct an offense that relays kinetic effects. This was the US-Israel operation against Iran by using the worm called Stuxnet that was configured to target only certain computers targeting Iranian uranium enrichment centrifuges to halt the Iranian nuclear bomb development program. It was successful in the sense it caused physical destruction, was first of its kind, and set the Iranian nuclear program behind by two years (Zetter 2014).

The exercises and trainings NATO has conducted, are primarily meant to enhance the defensive capabilities in cyberspace and improve the cyber resilience, but they have entailed offensive dimension as well in order to test the counter-attack capabilities. For instance, the Cyber Coalition exercise – which the last time took place in December 2018 in Estonia – did not only include utilizing defensive capabilities, but also offensive ones in order to counter-attack (Shaw 2018). Exercise called Crossed Swords is however, purely offensive (CCDCOE 2019).

Allies like Germany and France should also acquire offensive cyber capabilities and Germany has offered its capabilities for the use of NATO as well which was announced during the NATO's defence ministerial meeting in February 2019 (Paganini 2019). What we do know about Germany in this regard, is that within its military forces a special service focusing on the cyber and information domain matters was established. It is called Cyber and Information domain service (CIR), which will reach to its full capacity by 2021 (Pernik 2018:13; Werkhäuser 2017). To ensure the CIR will have the best personnel, there has been established a 'Cyber Cluster' at the Bunderswehr's University in Munich, for instance (Werkhäuser 2017).

France has also its cyber command (Pernik 2018:1). Furthermore, in January 2019, France published its first offensive cyber operations doctrine. This is remarkable, because there has not been a public discussion on France's respective capabilities. Nor have there been clear examples of France actually carrying out offensive cyber operations (Delarue et al 2019). What is interesting is that France's offensive cyber doctrine seems to only

consider offensive cyber operations in the context of attacking the availability or the confidentiality of data (Laudrain 2019).

4. 3. Analysis

The purpose of this analysis is to examine NATO's potential to utilize offensive cyber capabilities as means of deterrence, find out the compliance of NATO's current cyber policy and relation with these capabilities with the set of criteria for utilizing these capabilities in the context of cross-domain deterrence. Subsequently, the applicability and the explanatory power of the classical deterrence theories in regards of utilizing offensive cyber capabilities as deterrents will be assessed in the broader context. This will be followed by recommendations in the following subsection on how NATO could improve the potential of utilizing the offensive cyber capabilities as deterrents and how the classical deterrence theory should be improved to have better explanatory power in this kind of phenomenon.

Before going into depth with NATO's current cyber policy and approach to offensive cyber capabilities, it must be acknowledged that as expected there was lack of information available in the public sources about the offensive cyber capabilities. There was particularly less information from the side of Estonia, Denmark and the Netherlands. This, however, should not undermine the value of the research. If we talk about deterrence, then overt information is the core of it to make it function as it should. That there is not substantial information disclosed on these capabilities may already imply that the classical deterrence theory lacks the explanatory power in this context. However, it does also say that for the future purposes carrying out interviews with the representatives of these countries who are in some way responsible for the respective national cyber policies would be useful in order to gain better understanding of their respective cyber postures.

Starting off with NATO's general cyber policy, the utilization of offensive cyber capabilities in relation to deterrence is discussed primarily in the context of deterring cyberattacks but not in terms of the cross-domain deterrence. The Secretary General Stoltenberg referred to that at the press conference during the Brussels summit 2018 "NATO will continue strengthen its defence and deterrence in the cyber domain"

(Stoltenberg 2018). Although, this statement could be interpreted also as deterrence will be provided through cyberspace which means utilizing cyber capabilities as deterrents.

At the same time, among the allies there are signals of willingness to not to limit oneself only utilizing offensive cyber capabilities as a response to cyberattack. For instance, in the UK cyber security strategy it is said:

> "We will ensure that we have at our disposal appropriate offensive cyber capabilities that can be deployed at a time and place of our choosing, for both deterrence and operational purposes, in accordance with national and international law" (HM Government 2016:51).

The US has also expressed wider approach in terms of the utilization of these capabilities by saying in its Department of Defence cyber strategy that the intention with the offensive cyber capabilities is to "ensure the US military's ability to fight and win wars in any domain, including cyberspace" (Department of Defense 2018:2). In case of Estonia, it is not clearly mentioned how the offensive cyber capabilities once developed will be incorporated to the military planning and which strategic purposes they will serve (Riigikantselei 2017:2; Majandus- ja Kommuniaktsiooniministeerium 2019:5).

Concerning the offensive cyber capabilities Allies should possess, it is hard to tell, which cyber effects they can produce explicitly. NATO does not develop nor possess the offensive cyber capabilities on its own, therefore, understanding NATO's potential power in cyber requires understanding the corresponding power of the Allies. Though, this is rather difficult task because the examined states have not revealed it that bluntly. Particularly, we do not have that kind of information about Denmark, the Netherlands and Estonia. The UK and the US, however, have given some sense in words and in deeds which capabilities they might possess and which effects they are able to produce.

The UK does declare it has the offensive cyber capabilities which ought to be flexible in nature, function as a deterrent, and as an operational capability (Compotroller & Auditor General 2019:6; HM Government 2016:10; 51).

> "Offensive cyber capabilities involve deliberate intrusions into opponents' systems or networks, with the intention of causing damage, disruption or destruction. Offensive cyber forms part of the full spectrum of capabilities we will

> develop to deter adversaries and to deny them opportunities to attack us, in both cyberspace and the physical sphere. Through our National Offensive Cyber Porgramme, we have a dedicated capability to act in cyberspace and we will commit the resources to develop and improve this capability" (HM Government 2016:51).

What backs up the words are the respective deeds. The UK has conducted a cyber campaign against ISIS and recently it carried out an exercise which entailed attacking Russian electric grid in Moscow (Detrixhe 2018; Smeets 2017a). The latter is perhaps the most valuable example and reflection regarding the UK's cyber arsenal and that for two reasons. First, the target of the simulated attack was the country that is the subject of NATO's deterrence. Second, the attack was a high-level one by carrying out SCADA-attack that causes kinetic effects.

The US has been widely acknowledged as the global cyber power which is at the forefront with the offensive cyber capabilities. Therefore, the US is extremely important asset for NATO to have credibility and capability imposing retaliatory threat in cyberspace. The US has not been clear in words either which capabilities exactly it possesses, but the actions give a taste of it. The SCADA-attack against the Iranian nuclear facility in Natanz that caused kinetic effects is a significant reflection of it (Zetter 2014). What can be noted here is that the offensive cyber capabilities have been presented through their deployment.

If we also take a look at what Stoltenberg said in regards of the sovereign cyber capabilities certain Allies have given for the use of NATO, he does not give a clear answer to how the capabilities will be used as part of NATO's missions and operations. However, he does refer to the capability and will to use it in regards of disrupting networks, in other words attacking the availability of data.

> "We have been able to disrupt the cyber networks of Daesh to reduce their ability to recruit, to fund, to communicate. And these capabilities have been used by NATO Allies against Daesh and these are the same kind of capabilities we now are creating the framework to integrate into NATO missions and operations" (Stoltenberg 2018).

Additionally, the existence of and participation in exercises like the Crossed Swords organized primarily by the Cooperative Cyber Defence Centre of Excellence accredited by NATO, enables Allies to improve their offensive cyber capabilities and mirrors to the enemy which capabilities are being obtained. During this year's exercise, the participants from cyber commands and special operation forces tested their offensive skills on attacking industrial control systems and also unmanned ground vehicles (CCDCOE 2019).

So far, we can see that in general NATO should have the potential for utilizing offensive cyber capabilities as a deterrent, because the necessary capability seems to exist. This is driven from Allies acquiring offensive cyber capabilities which have been also presented through previously conducted cyber campaigns, certain Allies have offered their sovereign cyber capabilities for the use of NATO, the skills for creating offensive cyber capabilities are being developed, NATO is working towards incorporating cyber component into force structures. However, when it comes to the credibility of the cyber threat from the viewpoint of the enemy, there are some problems.

First two issues have already been touched upon above as well which entail lack of knowledge regarding which kind of offensive cyber capabilities are exactly possessed or being developed by the Allies and secondly, ambiguous message by NATO's Secretary General about in which cases and to what extent NATO would use the offered offensive cyber capabilities. Considering the conceptualized classical deterrence theory, the deterrer needs to be clear on its means, how they will be used and which effects they could cause (see i.e. Knopf 2009:41). Certain ambiguity could be acceptable in regards of the red lines, as otherwise, the enemy can play too easily around the boundaries. But the deterrent message should have more substance than just saying one is acquiring capabilities to carry out counterattacks in case of a necessity and that there have been few instances where those capabilities have been utilized. This does not seem enough to influence the decision-making equation of the enemy because it does not mirror what could be the costs in case of the aggression. It may especially turn out to be so if the adversary should happen to be risk-acceptant.

Third issue shadowing credibility of the potential cyber threat is stemmed from the previous two and this is that different 'languages' in the broader sense are being used by

the member states offering their capabilities for NATO's use. This does undermine the credibility of the deterrent threat, because in case of an Alliance, common language must be used by the members of it to ensure that there is no room for uncertainty and misperceptions. Talking about offensive cyber capabilities as a retaliatory measure, unified message by all the member states reflects the willingness to retaliate and gives the enemy the impression that the Alliance together stands by its words.

Different languages used can be noticed on how the nations have named the institutions in their military structures that are responsible for carrying out the offensive cyber operations. Estonia and the US name their commands as Cyber Commands. The Netherlands has the word 'defensive' in it: Defence Cyber Command. Denmark does not have a cyber command explicitly, whereas in Denmark the Danish Defence intelligence Service is responsible for the cyber operations. Why this could be a problem, is because of which effects they might produce: when cyber command is universal title and could entail both offensive and defensive operations, then "Defence Cyber Command" may refer only to defensive operations. This could undermine the credibility of the retaliatory threat in cyberspace in that regard. However, bigger concern than this is how the offensive cyber capabilities and the respective operations have been conceptualized by the member states.

The UK has described offensive cyber capabilities in a rather classical and all-inclusive way as they "[…]involve deliberate intrusions into opponents' systems or networks with the intention of causing damage, disruption or destruction" (HM Government 2016:51). In the case of Netherlands, the perception of the offensive cyber operations has a subtler tone compared to what the UK and the US have. The Dutch point out that while using those only against the military targets, they entail" infiltrating computers, computer networks and weapons and sensor systems so as to influence information and systems" (Ministry of Defence 2019; Royal Netherlands Army 2018:15).

Although France is not the country that has offered its capabilities for the use of NATO but still is the member of NATO, it is valuable to acknowledge that French perception of the offensive cyber capabilities differs also rather significantly. They perceive the offensive cyber operations as attacking the availability or the confidentiality of the data only, but not the integrity (Laudrain 2019). This creates the concerning ambiguity which

cyber effects the allies are willing to relay. Because of the unclear answer to this, it might explain why Stoltenberg was also unclear about how the offensive cyber capabilities could be used in the NATO's area of operation. This situation could also mean that the states may not have the same level of confidence in carrying out the offensive cyber operations and they may experience the self-deterrence in this regard as they might fear the escalation.

In conclusion, NATO has focused on cyber defence and the utilization of offensive cyber capabilities has not been mentioned as a retaliatory measure regarding cross-domain deterrence. As NATO itself does not possess offensive cyber capabilities, but its members do, the cyber power of NATO depends on the cumulative cyber capabilities of the Allies. While examining the five Allies who have offered their sovereign cyber capabilities for NATO's use and looking for the potential of utilizing these capabilities to bolster NATO's deterrence posture, several non-alignments with the set of requirements posed by the classical deterrence theory can be identified.

There is lack of information which capabilities these member states acquire or are developing. Particularly, it is the case concerning the three smaller countries. In terms of the UK and the US, the previously conducted cyber campaigns reflect which cyber effects they can relay and these entail kinetic effects as well. Therefore, the capability to retaliate should exist and the global acknowledgment of the US capabilities explicitly should ensure the credibility of the cyber threat at least to a certain extent on behalf of the Alliance.

Yet, it is undermined on the other hand by the fragmentation of how offensive cyber capabilities and respective operations have been described by the nations in their strategies. This could explain why NATO has given a vague answer on how the offered offensive cyber capabilities will be utilized. That subsequently would mean, there is uncertainty about the willingness – which also downgrades the credibility of offensive cyber capabilities acting as a deterrent – to use offensive cyber capabilities, especially those that would relay kinetic effects as a retaliatory measure. If there is different language on this matter, this means there might not be a unified position in NATO which would mean the enemy can be less worried about the cost potential produced by the offensive cyber operation on behalf of the Alliance. Although, the US has presented its

readiness and most recently in relation to Russia to deter it from meddling with the Mid-term elections (Nakashima 2019). Having the US on board, is perhaps the most important aspect in this case.

4.4. Theory Illuminating on utilizing Offensive Cyber Capabilities as Deterrent & Recommendations for enhancing NATO's Deterrence Posture

What can be learned from the analysis above, is that the classical deterrence theories remain valid also in case of utilizing offensive cyber capabilities. Because, NATO and its allies still can to meet the conditions that the classical deterrence theories have proposed to effectively utilize offensive cyber capabilities as means of deterrence. But, due to the distinct features of offensive cyber capabilities, the conceptualized mainstream deterrence theory neglects to explain how to ensure the credibility of these capabilities as deterrents. This confirms the posed hypothesis as well. Particularly, it is thereby proposed that the classical deterrence theory should be improved by taking into consideration the clandestine nature of offensive cyber capabilities and that deploying a cyber weapon can be a long-term process.

This conclusion can be made based on the lack of information about the Allies' offensive cyber capabilities. This is driven from the clandestine nature of these capabilities as in case they would be disclosed, they would reveal which vulnerabilities were to be exploited and what was the target. This information, however, would enable the enemy to patch these vulnerabilities and thereby make the developed cyber weapon non-usable. To overcome this hurdle and ensure the credibility of the words about the possession of offensive cyber capabilities, participation in relevant exercises and previous offensive cyber operations is important. Despite not knowing about the UK's and the US cyber capabilities in detail, their previously conducted cyber campaigns presented their willingness and necessary resources to deploy cyber weapons which could also relay kinetic effects.

In this context, classical deterrence theory in regards of utilizing offensive cyber capabilities as a deterrent, should be improved by considering the secretive nature of offensive cyber capabilities and not requiring their exposure the same way as it is expected from using conventional means as deterrent. In this context, it should be more

emphasized that the capability and willingness of relaying different types of cyber effects is there. This can be done through exercises but also through previously conducted offensive cyber operations in other domains.

Another feature that the classical deterrence theories do not address - but need to in order to explain how the offensive cyber capabilities can be used as means of deterrence - is taking into account the time constraint. The latter in the sense that deploying those cyber weapons which have the potential to generate greater strategic effects by targeting the functionality of critical infrastructure for instance, tends to be a long-term process. In order to instantly retaliate the enemy with this kind of operation, the deterrer needs to be in the adversary's systems beforehand. Notably, as it was described in the theoretical section above, developing a sophisticated cyber weapon that could inflict damage on the industrial control system for instance, involves numerous time-consuming steps. The question that needs to be considered in this regard is how to hold the enemy at risk by threatening to harm the critical infrastructure through offensive cyber means in case it should decide to attack. Subsequently, if it requires the presence-based approach, then how to communicate that to the adversary to ensure the credibility of the threat, but without increasing instability between the actors?

However, in general, the mainstream deterrence theories seem to remain applicable to utilizing offensive cyber capabilities as means of deterrence. Because despite the different means to be used, it is still necessary to reflect to the potential enemy which kind of retaliatory capabilities one has and thereby which costs the enemy can expect in case it decides to attack. Therefore, the following recommendations can be given to NATO on how it could bolster its deterrence posture through the utilization of offensive cyber capabilities as means of deterrence.

First, NATO should take a step further and not limit itself considering the offensive cyber capabilities only as measures to deter the enemy from carrying out malicious activity in cyberspace. The strategic value of offensive cyber capabilities has been presented in this paper and thereby NATO should seek for options to include offensive cyber capabilities as means of cross-domain deterrence. This should accordingly be reflected in its strategy documents. However, for effective deterrence the identified credibility issues need to be mitigated.

NATO and its member states – particularly those that have offered their capabilities for the NATO's use – need to achieve a common terminology and understanding of the offensive cyber capabilities and offensive cyber operations. Analysing the public documents from this angle, it was identified that the degree of effects Allies considered to be generated through the offensive cyber operations did differ. These different perceptions need to be aligned to make sure the enemy perceives that the Alliance has unified position on how the offensive cyber capabilities could be deployed and what kind of cyber effect it is willing to relay.

Third recommendation would be to have a clearer message on which kind of costs the enemy could expect from the deterrer's offensive cyber capabilities. The actions alone are not enough. Words complement the actions and enable to prevent misperceptions and thereby mitigate the potential security dilemma that may occur. As noted in the theoretical part, relaying kinetic effects has greater strategic value, especially by targeting the critical infrastructure that the military also relies on. In this case – as it was also illuminated on the existing deterrence theory – it could be necessary to have access in the enemy's systems before the crisis should erupt. Because NATO has emphasized its defensive posture also while talking about the offensive cyber capabilities, then it is particularly important to create the right narrative to avoid increasing the instability, contributing to security dilemma, and enabling the enemy to have a misperception on this. Finding the right balance here is probably the most difficult task. Thus, having an improved version of deterrence theory that can explain and guide how to make the cyber threat credible without increasing the instability, would be extremely valuable.

However, logic effects should not be left aside. Depending on the target, this could be the way to go as well. Concerning Russia – the subject of NATO's deterrence – should be vulnerable to logic effects that intend to affect the stability of internal politics. This is presumed based on Rivera's work on to which kind of cyberattacks countries are vulnerable to based on their power position and social cohesion (Rivera 2015:9-11). However, this should be further examined in the future on what would be strategically the most valuable targets to hold at risk as part of the deterrent threat related to Russia.

To sum up, NATO has the potential to bolster its deterrence by considering the offensive cyber capabilities as means of deterrence. It can be partly achieved by starting with

meeting the conditions classical deterrence theories have set, like having a clear and unified message about the cyber capabilities as retaliatory measures. Yet, to ensure the total effectiveness, the classical deterrence theory needs to be improved by acknowledging the secretive nature of offensive cyber capabilities and answering questions on how to hold the enemy at risk by threatening to harm its critical infrastructure through offensive cyber means and if presence-based approach is required, how to communicate that to the adversary without increasing instability between the actors.

Summary

The aim of this paper is to contribute to the strategic thought on utilizing offensive cyber capabilities as means of cross-domain deterrence and how NATO could adopt that. This was driven from the lack of attention given to the strategic benefits the offensive cyber capabilities entail and how they could therefore be used for deterrence purposes. Thereby, not to deter only cyber-attacks, but potential aggressions in other operational domains also as part of the cross-domain deterrence.

To achieve the research goal, a case-study on NATO and its members - who have offered their national cyber capabilities for NATO's use - was conducted. The intention of the study was to draw conclusion on how intact the classical deterrence theories seem to be to explain the utilization of the offensive cyber capabilities as means of cross-domain deterrence. Examining this based on how NATO and its members have reflected on these capabilities to the publics, enabled to illuminate how the classical deterrence theory should be improved and which actions NATO should take to also bolster its deterrence accordingly. In conclusion, the proposed hypothesis was confirmed as the classical deterrence theories failed to explain how to make the cyber threat credible, but the mainstream deterrence theories remain still valid.

The results of the case-study reflected that NATO has the potential to utilize offensive cyber capabilities as means of deterrence, but today there is a lot of ambiguity around how the offensive cyber capabilities will be used while the focus is more on defending against cyberattacks and deterring malicious activity in cyberspace. There was also lack of information about what kind of cyber capabilities the five Allies that have offered their capabilities for the use of NATO even possess. This is most probably driven from the requirement to keep these capabilities covert in order to not to expose which vulnerabilities are used and what respectively is targeted which enables to neutralize the power of the capability by the enemy. Another undermining factor of the credibility are mixed and vague messages by the Allies and NATO on how offensive cyber capabilities and operations are perceived. Moreover, when and how the offered cyber capabilities by the member states will be used in support of NATO's missions and operations. The lack

of clear communication in this regard leaves room for interpretation and weakens the deterrence posture.

Certain credibility issues can be mitigated based on the classical deterrence theories. For instance, NATO should start with acknowledging offensive cyber capabilities as means of cross-sector deterrence and incorporate that policy into its strategy. Secondly, NATO and its allies need to have common language and understanding on the offensive cyber capabilities and which effects the Alliance is willing to generate with these. However, the classical deterrence theory falls short in explaining how NATO could present its offensive cyber capabilities and how to create the deterrent cyber threat by holding the functionality of the enemy's infrastructure – that should achieve strategic effects if targeted – at risk.

Therefore, it was identified that classical deterrence theory has to a certain extent explanatory power on how to utilize offensive cyber capabilities as means of cross-domain deterrence. It is the case, because certain conditions set by the classical deterrence theories were not met by NATO's current approach, but could, because they were not related to the distinct features of offensive cyber capabilities. However, the posed hypothesis was also proven true which was that the classical deterrence theories on the other hand neglect to explain how to make the offensive cyber capabilities as credible deterrents. Namely, the classical deterrence theories have not taken into consideration distinct features the offensive cyber capabilities hold: clandestine nature and that depending on the effect the process of deploying the cyber weapon can be very time-consuming. Therefore, it was proposed that the classical deterrence theory should be improved by taking into account those two distinct features. Particularly, in regards of the latter, it is necessary to find answers to how to hold the enemy at risk by threatening to harm its critical infrastructure through offensive cyber means and if presence-based offensive operation is required, how to communicate that to the adversary without increasing instability between the actors.

This paper has given the initial contribution to the academic discussion on this topic and input to the policy-makers as well considering the recommendations regarding NATO's deterrence posture. However, this research has potential to be carried on in the future and there are several options for it.

It could be valuable to conduct interviews with the national representatives of the US, the UK, the Netherlands, Denmark, and Estonia to gain better understanding of their national offensive cyber capabilities, what is their policy on utilizing those, how they perceive the offensive cyber operations, and what is their thought on integrating offensive cyber capabilities as a means of cross-domain deterrence? Answers to these questions would enable to test also the recommendations made in this thesis on how NATO could bolster its deterrence posture through the offensive cyber capabilities.

Second option would be to further elaborate and conduct an in-depth analysis on the illuminations presented on how the classical deterrence theories could be improved to explain more in detail the utilization of the offensive cyber capabilities as means of deterrence. The outcome of this could be a middle-range theory on using offensive cyber capabilities as a deterrent based on the classical deterrence theories.

For future analysis, the third option would be to conduct a Russia-specific research which this thesis could not include due to the limited space and time. However, this kind of research could entail detailed analysis on what deters Russia in cyberspace, how it could be hold at risk via offensive cyber capabilities.

Bibliography

Adams, Michael J. & Megan Reiss. 2018. “International Law and Cyberspace: Evolving Views”, *Lawfare*, March 4th. https://www.lawfareblog.com/international-law-and-cyberspace-evolving-views (Accessed May 19th, 2019)

Arts, Sophie. 2018. “Offense as the New Defense: New Life for NATO’s Cyber Policy”, Policy Brief, *The German Marshall Fund of the United States*, No 039.

Baram, Gil. 2018. “The Theft and Reuse of Advanced Offensive Cyber Weapons pose a Growing Threat”, *Council on Foreign Relations,* June 19th. https://www.cfr.org/blog/theft-and-reuse-advanced-offensive-cyber-weapons-pose-growing-threat (Accessed May 5th, 2019)

BBC. 2017. “Ukraine Power Cut ‘was Cyber-attack’, January 11th, https://www.bbc.com/news/technology-38573074 (Accessed May 5th, 2019)

Bebber, Robert. 2017. “Cyber Power and Cyber Effectiveness: An Analytic Framework”, *Comparative Strategy,* 36(5): 426-436.

Belk, Robert & Matthew Noyes. 2012. “On the Use of Offensive Cyber Capabilities: A Policy Analysis on Offensive US Cyber Policy”, Belfer Center, https://www.belfercenter.org/sites/default/files/files/publication/cybersecurity-pae-belk-noyes.pdf (Accessed May 4th, 2019)

Bellovin, Steven M.; Susan Landau & Herbert S. Lin. 2017. “Limiting the Undesired Impact of Cyber Weapons: Technical Requirements and Policy Implications”, *Journal of Cybersecurity,* 3(1):59-68.

Bond, David. 2018. “Britain preparing to launch new Cyber Warfare Unit”, Financial Times, September 21st. https://www.ft.com/content/eef717f2-bb6e-11e8-8274-55b72926558f (Accessed to May 10th, 2019)

Buchanan, Ben. 2017a. “How Network Intrusions Threaten” in *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations*, Oxford Scholarship Online. http://www.oxfordscholarship.com/view/10.1093/acprof:oso/9780190665012.001.0001/acprof-9780190665012-chapter-5?print=pdf (Accessed May 4th, 2019)

Buchanan, Ben. 2017b. “The Failure of Traditional Mitigations” in *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations,* Oxford Scholarship Online. http://www.oxfordscholarship.com/view/10.1093/acprof:oso/9780190665012.001.0001/acprof-9780190665012-chapter-6?print=pdf (Accessed May 4th, 2019)

Buchanan, Ben. 2017c. “The Intruder’s View” in *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations,* Oxford Scholarship Online. http://www.oxfordscholarship.com/view/10.1093/acprof:oso/9780190665012.001.0001/acprof-9780190665012-chapter-3?print=pdf (Accessed May 4th, 2019)

CCDCOE. 2019. “Crossed Swords 2019 integrates Cyber into Full Scale of Operations”, https://ccdcoe.org/news/2019/exercise-crossed-swords-2019-integrates-cyber-into-full-scale-of-operations/ (Accessed May 18th, 2019)

Compotroller & Auditor General. 2019. “Progress of the 2016-2021 National Cyber Security Programme”, *National Audit Office.* https://www.nao.org.uk/wp-content/uploads/2019/03/Progress-of-the-2016-2021-National-Cyber-Security-Programme.pdf (Accessed to May 10th, 2019)

Craig, Anthony & Brandon Valeriano. 2016. “Conceptualising Cyber Arms Races” in N. Pissanidis, H. Rõigas & M. Veenendaal (Eds.) 2016 8th International Conference on Cyber Conflict: Cyber Power”, Tallinn: NATO CCD COE, 141-158.

Crawford, Timothy W. 2009. “The Endurance of Extended Deterrence: Continuity, Change, and Complexity in Theory and Policy” in T. V. Paul, Patrick M. Morgan & James J. Wirtz (Eds.) *Complex Deterrence: Strategy in the Global Age*. The University of Chicago Press: Chicago & London, 277-303.

Danish Ministry of Defence. 2019. “Offensive Cyber Effects”, https://fmn.dk/temaer/nato/Documents/2018/cybereffects-NATO-2018.pdf (Accessed to May 10th, 2019)

Davis, Susan. 2019. “NATO in the Cyber Age: Strengthening Security & Defence, Stabilising Deterrence”, Science and Technology Committee, NATO Parliamentary Assembly, April 18th. https://www.nato-pa.int/download-file?filename=sites/default/files/2019-04/087_STC_19_E%20-%20NATO.pdf (Accessed to May 11th, 2019)

Defense News. 2015. "Denmark to Develop Offensive Cyber Capability", January 8th. https://www.defensenews.com/2015/01/08/denmark-to-develop-offensive-cyber-capability/ (Accessed to May 10th, 2019)

Delerue, Francois; Alix Desforges & Aude Gery. 2019. "A Close Look at France's New Military Cyber Strategy", War on the Rocks, April 23rd. https://warontherocks.com/2019/04/a-close-look-at-frances-new-military-cyber-strategy/ (Accessed May 10th, 2019)

Department of Defense. 2018. "Summary: Department of Defence Cyber Strategy", https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF (Accessed to May 10th, 2019)

Detrixhe, John. 2018. "The UK is practicing Cyberattacks that could Black Out Moscow", *Quartz*, October 7th. https://qz.com/1416362/the-uk-war-games-cyberattacks-that-could-black-out-moscow/ (Accessed to May 10th, 2019)

DeWeese, Geoffrey S. 2015. "Anticipatory and Preemptive Self-Defense in Cyberspace: The Challenge of Imminence" in M.Maybaum, A.-M. Osula & L.Lindström (Eds.) 2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace, Tallinn: NATO CCDCOE Publications, 81-92.

ERR. 2018. "Luik: Eesti on vajadusel valmis andma oma kübervõimed NATO käsutusse", October 4th. https://www.err.ee/866519/luik-eesti-on-vajadusel-valmis-andma-oma-kubervoimed-nato-kasutusse (Accessed to May 10th, 2019)

Fallon, Michael. 2016. *Defence Secretary's speech at the second RUSI CYber Symposium*, October 20th. https://www.gov.uk/government/speeches/defence-secretarys-speech-at-the-second-rusi-cyber-symposium (Accessed May 9th, 2019)

Fischerkeller, Michael. 2017. "Incorporating Offensive Cyber Operations into Conventional Deterrence Strategies", *Survival*, 59:1, 103-134.

Folmer, Hans. 2018. "Demystifying Cyber Operations", Ministry of Defence, https://puc.overheid.nl/mrt/doc/PUC_248329_11/1/ (Accessed to May 9th, 2019)

Freedman, Lawrence & Srinath Raghavan. 2013. “Coercion” in Paul D. Williams (Ed.) *Security Studies – An Introduction,* 2nd edition. Routledge, Taylor & Francis: London & New York. 206-220.

Friis, Karsten & Ringsmose, Jens. 2016. “Introduction” in Karsten Friis and Jens Ringsmose (Eds.) *Conflict in Cyber Space: Theoretical, Strategic and Legal Perspectives*. London & New York: Routledge, Taylor & Francis Group, pp 1-6.

Gaycken, Sandro & Martellini, Maurizion. 2013. “Cyber as Deterrent” *in* M. Martellini (Ed.) *Cyber Security,* Springer Briefs in Computer Science, 1-17.

Geers, Kenneth. 2010. “The Challenge of Cyber Attack Deterrence*.” Computer Law & Security Review*, 26:298-303.

George, Alexander L. & Andrew Bennett. 2005. *Case Studies and Theory Development in the Social Sciences*. BCSIA Studies in International Security, Cambridge, Massachusetts, London, England: MIT Press.

Gold, Josh. 2019. “Toward Norms in Cyberspace: Recent Progress and Challenges”, *Canadian International Council*, January 7th. https://thecic.org/en/toward-norms-in-cyberspace-recent-progress-and-challenges/ (Accessed May 19th, 2019)

Gray, Colin S. 2000. “Deterrence in the 21st century”, Comparative Strategy, 19(3): 255-261

Gray, Colin S. 2003. “Maintaining Effective Deterrence”, *Strategic Studies Institute, https*://ssi.armywarcollege.edu/pdffiles/PUB211.pdf (Accessed February 19th, 2019)

Haffa, Robert P. Jr. 2018. “The Future of Conventional Deterrence: Strategies for Great Power Competition”, *Strategic Studies Quarterly,* 12(4): 94-115.

Herr, Trey & Jacquelyn Schneider. 2018. “Sharing is Caring: The United States’ New Cyber Commitment for NATO”, *Council on Foreign Relations*, October 10th. https://www.cfr.org/blog/sharing-caring-united-states-new-cyber-commitment-nato (Accessed May 8th, 2019)

HM Government. 2016. “National Cyber Security Strategy”, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment

_data/file/567242/national_cyber_security_strategy_2016.pdf (Accessed to May 10th, 2019)

Inkster, Nigel. 2017. “Measuring Military Cyber Power”, *Survival,* 59(4):27-34.

Jervis, Robert. 1976. *Perception and Misperception in International Politics*, Princeton & New Jersey: Princeton University Press.

Joint Chiefs of Staff. 2018. “JP 3-12, Cyberspace Operations” http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-06-19-092120-930 (Accessed May 4th, 2019).

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

Knopf, Jeffrey W. 2009. “Three Items in One: Deterrence as Concept, Research Program, and Political Issue” in T. V. Paul, Patrick M. Morgan & James J. Wirtz (Eds.) *Complex Deterrence: Strategy in the Global Age*. The University of Chicago Press: Chicago & London, 31-57.

Laudrain, Arthur P.B. 2019. “France’s New Offensive Cyber Doctrine”, Lawfare, February 26th. https://www.lawfareblog.com/frances-new-offensive-cyber-doctrine (Accessed to May 10th, 2019)

Lewis, Don. 2019. “What is NATO really doing in Cyberspace?”, War on the Rocks, February 4th. https://warontherocks.com/2019/02/what-is-nato-really-doing-in-cyberspace/ (Accessed May 8th, 2019)

Lewis, James A. 2010. “Crioss-Domain Deterrence and Credible Threats”, *Center for Strategic and International Studies*. https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/100701_Cross_Domain_Deterrence.pdf (Accessed May 7th, 2019)

Lewis, James A. 2015. “The Role of Offensive Cyber Operations in NATO’s Collective Defence”, The Tallinn Papers, No 8, https://ccdcoe.org/uploads/2018/10/TP_08_2015_0.pdf (Accessed May 6th, 2019)

Lewis, James Andrew. 2018. “Cognitive Effect and State Conflict in Cyberspace”, CSIS https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180924_Cognitive_Effect_Cyberspace.pdf?R6FPUdDaOystuUCWsMCXUhKTBg.4CW.D (Accessed May 4th, 2019)

Libicki, Martin C. 2009. „Cyberdeterrence and Cyberwar.“ RAND Corporation. http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf (Accessed: November 1st, 2018).

Majandus- ja Kommunikatsiooniministeerium. 2019. “Küberturvalisuse strateegia 2019-2022”, https://www.mkm.ee/sites/default/files/kuberturvalisuse_strateegia_2019-2022.pdf (Accessed to May 10th, 2019)

Manzo, Vincent. 2011. “Deterrence and Escalation in Cross-domain Operations: Where do Space and Cyberspace fit?”, *Strategic Forum: National Defense University*, No 272. https://ndupress.ndu.edu/Portals/68/Documents/stratforum/SF-272.pdf (May 7th, 2019)

Mattis, James N. 2018. News Conferency by Secretary Mattis at NATO Headquarters, Brussels, Belgium. *US Department of Defense,* October 4th https://dod.defense.gov/News/Transcripts/Transcript-View/Article/1654419/news-conference-by-secretary-mattis-at-nato-headquarters-brussels-belgium/ (Accessed to May 10th, 2019)

Ministry of Defence. 2019. “Defence Cyber Command”. https://english.defensie.nl/topics/cyber-security/cyber-command (Accessed to May 9th, 2019)

Moore, Daniel. 2018. “Targeting Technology: Mapping Military Offensive Network Operations” in T. Minarik, R. Jakschis & L. Lindström *2018 10th International Conference on Cyber Conflict,* Tallinn: NATO CCD COE, 89-107.

Morgan, Patrick M. 1983. “Deterrence: A Conceptual Analysis”, Sage Publications.

Morgan, Patrick M. 2010. “Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm” in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (Washington, D.C.: National Academies Press, 55–76.

Morgus, Robert; Max Smeets & Trey Herr. "Countering the Proliferation of Offensive Cyber Capabilities", Memo No 2, *GCSC Issue Brief,* 161-187. http://maxsmeets.com/wp-content/uploads/2018/09/GCSC-Briefings-from-the-Research-Advisory-Group_New-Delhi-2017-161-187.pdf (Accessed May 5th, 2019)

Morgus, Robert; Max Smeets & Trey Herr. "Countering the Proliferation of Offensive Cyber Capabilities", GCSC Issue Brief, Memo No 2, http://maxsmeets.com/wp-content/uploads/2018/09/GCSC-Briefings-from-the-Research-Advisory-Group_New-Delhi-2017-161-187.pdf (Accessed May 19th, 2019)

Nakashima, Ellen. 2018. "White House authorizes 'offensive cyber Operations' to deter Foreign Adversaries", *The Washington Post,* September 20th . https://www.washingtonpost.com/world/national-security/trump-authorizes-offensive-cyber-operations-to-deter-foreign-adversaries-bolton-says/2018/09/20/b5880578-bd0b-11e8-b7d2-0773aa1e33da_story.html?utm_term=.8ee0cafa1aff (Accessed to May 8th, 2019)

Nakashima, Ellen. 2019. "US Cyber Command Operation disrupted Internet access of Russian troll factory on day of 2018 midterms", *The Washington Post,* February 27th. https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html?utm_term=.5f9f3a035c12 (Accessed May 8th, 2019)

NATO. 2010. "Active Engagement, Modern Defence: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation adopted by Heads of State and Government in Lisbon", November 19th. https://www.nato.int/cps/en/natohq/official_texts_68580.htm (Accessed to May 10th, 2019)

NATO. 2014. "Wales Summit Declaration." https://www.nato.int/cps/ic/natohq/official_texts_112964.htm (Accessed October 28th, 2018).

NATO. 2016. “Warsaw Summit Communique”, July 6th https://www.nato.int/cps/su/natohq/official_texts_133169.htm (Accessed: October 28th, 2018)

NATO. 2017. “Readiness Action Plan”, NATO, September 21st. https://www.nato.int/cps/en/natohq/topics_119353.htm (Accessed to May 10th, 2019)

NATO. 2018. “Brussels Summit Declaration”, July 11th. https://www.nato.int/cps/em/natohq/official_texts_156624.htm (Accessed: October 28th, 2018)

NATO. 2019. “NATO Cyber Defence”, *North Atlantic Treaty Organization,* https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_02/20190208_1902-factsheet-cyber-defence-en.pdf (Accessed May 8th, 2019)

Northrop Grumman. 2018. “Unified Platform will enable a Full Spectrum of Integrated Cyber Capabilities across Domains for US Cyber Command”, October 29th. https://news.northropgrumman.com/news/releases/us-air-force-selects-northrop-grumman-for-uscybercom-unified-platform (Accessed to May 11th, 2019)

Paganini, Pierluigi. 2019. “Germany makes its Cyber Capabilities available for NATO Alliance”, *Security Affairs,* February 15. https://securityaffairs.co/wordpress/81125/cyber-warfare-2/germany-nato-alliance-warfare.html (Accessed to May 8th, 2019)

Paul, T. V. 2009. “Complex Deterrence: An Introduction” in T. V. Paul, Patrick M. Morgan & James J. Wirtz (Eds.) *Complex Deterrence: Strategy in the Global Age*. The University of Chicago Press: Chicago & London, 1-27.

Pernik, Piret. 2018. “Preparing for Cyber Conflict: Case Studies of Cyber Command”, *ICDS,* https://icds.ee/wp-content/uploads/2018/12/ICDS_Report_Preparing_for_Cyber_Conflict_Piret_Pernik_December_2018-1.pdf (Accessed May 5th, 2019)

Pomerlau, Mark. 2019. "Cyber Command's 2019 plan for New Tools", Fifth Domain, February 19th. https://www.fifthdomain.com/dod/cybercom/2019/02/19/cyber-commands-2019-plan-for-new-tools/ (Accessed to May 9th, 2019)

Rattray, Gregory & Jason Healey. 2010. “Categorizing and Understanding Offensive Cyber Capabilities and Their Use” in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*. Washington, DC: The National Academies Press. https://www.nap.edu/read/12997/chapter/8 (Accessed May 4th, 2019)

Rhodes, Edward. 2000. “Conventional Deterrence”, *Comparative Strategy*, 19(3): 221-253.

Rid, Thomas & Peter McBurney. 2012. “Cyber-Weapons”, The RUSI Journal, 157(1):6-13

Riigikantselei. 2017. “Riigikaitse arengukava 2017-2026, arengukava avalik osa”, https://www.riigikantselei.ee/sites/default/files/content-editors/Failid/rkak_2017_2026_avalik_osa.pdf (Accessed to May 10th, 2019)

Rios, Billy K. 2009. “Sun Tzu was a Hacker: An Examination of the Tactics and Operations from a Real World Cyber Attack”, in C. Czosseck & K. Geers (Eds.) *The Virtual Battlefield: Perspectives on Cyber Warfare*. Amsterdam, Berlin, Tokyo, Washington, DC: IOS Press, 143-155.

Rovner, Joshua. 2017. “Are Cyber Weapons too Dangerous to use?”, *War on the Rocks*, August 22nd. https://warontherocks.com/2017/08/are-cyber-weapons-too-dangerous-to-use/ (May 5th, 2019)

Royal Netherlands Army. 2018. “Vision of the Army – Security through Foresight”, November 5th. https://english.defensie.nl/downloads/publications/2018/11/05/vision-of-the-army (Accessed to May 10th, 2019)

Saldana, J. 2013. "Chapter 1: An introduction to codes and coding." In *The coding manual for qualitative researchers*. Thousand Oaks, CA: SAGE. 1-40.

Saltzman, Ilai. 2013. “Cyber Posturing and the Offense-Defense Balance”, Contemporary Security Policy, 34(1): 40-63.

Sanger, David. 2018. *The Perfect Weapon*. London & Melbourne: Scribe.

Schelling, Thomas C. 1966. *Arms and Influence.* New Haven and London: Yale University Press.

Schreier, M. 2012. "Chapter 1: Introduction: What is qualitative content analysis?" In *Qualitative content analysis in practice*. Los Angeles, London, New Delhi, Singapore, Washington DC: SAGE.1-19.

Shakarian, Paulo; Jana Shakarian & Andrew Ruef. 2013. *Introduction to Cyber-Warfare: A Multidisciplinary Approach.* Amsterdam, Boston, Heidelberg, London, New York, Oxford, Paris, San Diego, San Francisco, Singapore, Sydney, Tokyo: Syngress.

Sharma, Amit. 2009. "Cyber Wars: A Paradigm Shift from Means to Ends" in C. Czosseck & K. Geers (Eds.) *The Virtual Battlefield: Perspectives on Cyber Warfare*. Amsterdam, Berlin, Tokyo, Washington, DC: IOS Press, 3-17.

Shaw, Mitchell C. 2018. "NATO Practicing Cyber-Warfare Games", *New American,* December 2nd. https://www.thenewamerican.com/tech/computers/item/30799-nato-practicing-cyber-warfare-games (Accessed to May 9th, 2019)

Siedler, Ragnhild Edresen. 2016. "Hard Power in Cyberspace: CAN as a Political Means" in N. Pissanidis, H. Rõigas & M. Veenendaal (Eds.) *2016 8th International Conference on Cyber Conflict: Cyber Power",* Tallinn: NATO CCD COE, 23-36.

Siroli, Gian Piero. 2018. "Considerations on the Cyber Domain as the New WorldWide Battlefield", *The International Spectator,* 53(2):111-123.

Smeets, Max & Herbert S. Lin. 2018. "Offensive Cyber Capabilities: To What Ends?" in T. Minarik, R. Jakschis & L. Lindström *2018 10th International Conference on Cyber Conflict,* Tallinn: NATO CCD COE, 55-71.

Smeets, Max. 2017a. "Europe Slowly Starts to talk Openly about Offensive Cyber Operations", Council on Foreign Relations, November 6th. https://www.cfr.org/blog/europe-slowly-starts-talk-openly-about-offensive-cyber-operations (Accessed May 9th, 2019)

Smeets, Max. 2017b. "Organisational Integration of Offensive Cyber Capabilities: A Primer on the Benefits and Risks" in H. Rõigas, R. Jakschis, L. Lindström & T. Minarik

(Eds.) 2017 9th International Conference on Cyber Conflict, Tallinn: NATO CCD COE, 25-42.

Smeets, Max. 2018a. “A Matter of Time: On the Transitory Nature of Cyberweapons”, Journal of Strategic Studies, 41(1):6-32

Smeets, Max. 2018b. “The Strategic Promise of Offensive Cyber Operations”, Strategic Studies Quarterly, 12(3):90:113.

Snyder, Glenn H. 1961. *Deterrence and Defence: Toward a Theory of National Security*. Princeton University Press: Princeton & New Jersey.

Snyder, Glenn H. 1961. *Deterrence and Defence: Toward a Theory of National Security,* Princeton University Press: Princeton & New Jersey.

Stein, Janice Gross. 2009. “Rational Deterrence against ‘Irrational’ Adversaries? No Common Knowledge” in T. V. Paul, Patrick M. Morgan & James J. Wirtz (Eds.) *Complex Deterrence: Strategy in the Global Age*. The University of Chicago Press: Chicago & London, 58-84.

Stoltenberg, Jens. 2018. Press Conference by NATO Secretary General Jens Stoltenberg following the meetings of NATO Defence Ministers, NATO, October 4th, https://www.nato.int/cps/su/natohq/opinions_158705.htm?selectedLocale=en (May 9th, 2019)

Stone, John. 2012. “Conventional Deterrence and the Challenge of Credibility”, *Contemporary Security Policy,* 33(1): 108-123.

The Danish Government. 2018. “Foreign and Security Policy Strategy 2019-2020”, https://www.dsn.gob.es/sites/dsn/files/2018_Denmark%20Foreign%20and%20security%20policy%20strategy%202019-2020.pdf (Accessed to May 10th, 2019)

Tikk, Eneken, Kadri Kaska, Liis Vihul. 2010. *International Cyber Incidents: Legal Considerations*. Tallinn: Cooperative Cyber Defence Centre of Excellence.

Wallace, David. 2018. “Cyber Weapon Reviews under International Humanitarian Law: A Critical Anlaysis”, *Tallinn Paper No* 11, Tallinn: NATO Cooperative Cyber Defence

Centre of Excellence. https://ccdcoe.org/uploads/2018/10/TP-11_2018.pdf (Accessed May 4th, 2019)

Werkhäuser, Nina. 2017. "Germany Army launches New Cyber Command", Deutche Welle, April 1st. https://www.dw.com/en/german-army-launches-new-cyber-command/a-38246517 (Accessed to May 9th, 2019)

Zetter, Kim. 2014. „An Unprecedented Look at Stuxnet, the World's First Digital Weapon.", *Wired*, March 11th, .https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/ (Accessed May 5th, 2019)

Zetter, Kim. 2016. „Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid."Wired, March 3rd. .https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ (Accessed May 5th, 2019)

Non-exclusive licence to reproduce thesis and make thesis public

I'_____

(author's name)

1. Herewith grant the University of Tartu a free permit (non-exclusive licence) to reproduce, for the purpose of preservation, including for adding to the DSpace digital archives until the expiry of the term of copyright,

_____

_____

_____

(title of thesis)

supervised by_____.

(supervisor's name)

2. I grant the University of Tartu a permit to make the work specified in p. 1 available to the public via the web environment of the University of Tartu, including via the DSpace digital archives, under the Creative Commons licence CC BY NC ND 3.0, which allows, by giving appropriate credit to the author, to reproduce, distribute the work and communicate it to the public, and prohibits the creation of derivative works and any commercial use of the work until the expiry of the term of copyright.

3. I am aware of the fact that the author retains the rights specified in p. 1 and 2.

4. I certify that granting the non-exclusive licence does not infringe other persons' intellectual property rights or rights arising from the personal data protection legislation.

Laura Oolup

20/05/2019