



IMSIS
International Master
Security, Intelligence
& Strategic Studies



**Erasmus
Mundus**

Cyber deterrence as a challenge to International Security: How could a conceptual framework formulate national deterrence strategies to prevent warfare actions in the cyber domain?

May 2020

Glasgow Student ID: 2399044

Dublin Student ID: 18114423

Charles Student ID: 65102261

Gueorgui Dimitrov

**Presented in partial fulfilment of the requirements for the Degree of
International Master in Security, Intelligence and Strategic Studies**

Word Count: 23934

Supervisor: Vít Střítecký

Date of Submission: 30/07/2020



CHARLES UNIVERSITY

Table of Content.

ABSTRACT.....	2
INTRODUCTION.....	2
CHAPTER 1: DETERRENCE: THEORY AND CONCEPT	5
1.1 CLASSICAL DETERRENCE THEORY	7
1.2 CONTEMPORARY DETERRENCE THEORY.....	11
1.3 DETERRENCE CONCEPTS AND THE CYBER DOMAIN.....	14
1.4 DETERRENCE AND NATIONAL CYBERSECURITY STRATEGIES	18
CHAPTER 2: CHALLENGES TO CYBER DETERRENCE	23
2.1 INTERNATIONAL CYBER DETERRENCE INITIATIVES	25
2.2 CASE STUDIES OF NATION-STATE ACTIONS IN THE CYBER DOMAIN	29
2.3 NON-STATE ACTORS IN THE CYBER DOMAIN	33
2.4 ATTRIBUTION: HOW SURE SHOULD A STATE BE TO ATTRIBUTE A CYBER-ATTACK? 36	
CHAPTER 3: CYBER DETERRENCE STRATEGY FRAMEWORK	39
3.1 CYBER DETERRENCE: BY DENIAL	42
3.2 CYBER DETERRENCE: BY PUNISHMENT.....	45
3.3 CYBER DETERRENCE: CUMULATIVE DETERRENCE.....	49
3.4 CONCEPTUAL FRAMEWORK FOR NATIONAL CYBER DETERRENCE STRATEGIES	53
3.5 LIMITATIONS	57
CONCLUSION	58
APPENDICES.....	61
BIBLIOGRAPHY.....	63

Abstract.

This thesis aims to determine the role of deterrence in the digital age, where nation-states can threaten strategic assets through just a couple of keyboard strokes. It will examine classical and contemporary deterrence strategies for the purpose of assessing their applicability and meaning to the cyber domain. The research aims at establishing the feasible concepts from these conventional strategies that are suitable within cyberspace. Building on concepts from both classical and contemporary deterrence theories, this work ultimately proposes a conceptual framework for separate doctrines or national cyber deterrence strategies that would be helpful in preventing warfare actions in the cyber domain.

Introduction.

The challenge of the present digitally enabled age is not in defining deterrence. It is already a well-established strategy that has been examined and experienced through time, especially during the dawn of the nuclear age. The current challenge is in fact to understand the role of Information and Communication Technologies (ICT) in the broader aspect of deterrence strategy. This role appears to be very significant since these technologies managed to establish a whole new military domain, which brings subordinate challenges. The ever-changing field often referred to as ‘cyberspace’, is further characterized by the growing difficulty to deter actions within it. Deterrence in one military domain rarely operates independently, especially since the occurrence of the cyber domain, which serves to interconnect all other four conventional military domains of land, water, air, and space (Brantly, 2018).

Much of the existing studies on cyber deterrence concentrates on domain deterrence. Yet, this limitation raises some risks and reduces the likelihood of success. This thesis aims to establish a conceptual framework that could ideally serve to formulate separate doctrines or national cyber deterrence strategies. The purpose will be to determine which of the proven and effective deterrence concepts derived from examining the classical and contemporary deterrence theories are suitable for the cyber domain. They will be then structured into the proposed conceptual framework, which would ideally be helpful to prevent warfare actions in cyberspace.

The main body of the thesis will consist of three chapters. The first chapter will address existing literature on deterrence by examining both classical and contemporary theories and concepts, grouping them into categories, based on how they function. Focusing on classical concept groups,

like deterrence by denial, for instance, would help demonstrate both the difference and similarities between deterrence in the nuclear age and post-Cold War deterrence, which acknowledges cyberspace as a domain of military operations (Min rik, et.al., 2018). The utilization of classical deterrence theories to the cyber domain necessarily requires a thorough consideration of how state actors achieve, develop, and assess costs and benefits within this domain. Corresponding to the concepts laid out by the classical deterrence theory, for example, a total war would be too massive and too consuming to be allowed (Brodie, 1959). However, this philosophy of deterrence does not reflect on the possibility of preventive wars for less than ultimate military actions, which is a notion that was not relevant in the 1950s but gained attention in the US after 9/11. In the thesis, similar arguments will be of use to get a better grasp of the differences between deterrence in the nuclear age, contemporary deterrence, and cyber deterrence. Bernard Brodie's (1959) work was unable to sort out the dilemmas of the classical deterrence and what to do if it failed but he captured these dilemmas far better than most, which would allow the thesis to determine which of these deterrence concepts are applicable in the cyber domain. Establishing the efficiency of classical deterrence theories and their inability to be fully translated into the cyber domain would be used as part of the argument-formulation.

As it comes to contemporary deterrence theory, it will also focus on existing concepts grouping them based on how they function. For example, deterrence by punishment concepts will be clustered based on their offensive characteristics. Furthermore, since the focal point in this thesis will be to review and question the possibility of creating national cyber deterrence strategies, a broad number of documents would also need to be examined through a content analysis approach, such as NATO Tallinn Manual (Schmitt, 2017), several National Cybersecurity strategies (Baezner and Cordey, 2019), and many different government publications related to deterrence. One of the most important aspects that will be addressed within this thesis is the distinction between deterrence in general and deterrence in cyberspace. Particularly, it is important to make a clear outline of the need for national cyber deterrence strategies. Tim Stevens (2012) supports this notion of necessity for separating such strategies, as his work demonstrates the US efforts to develop strategic cyber deterrence that can reduce adversarial actions in cyberspace. Different national efforts have failed to transform into effective cyber deterrence strategy or doctrine, due to the distinct operational nature of cyberspace and the over-dependence on Cold War concepts of

deterrence, which is evident through the examination of National Cyber Security Strategies of selected states.

To further support this analysis and to provide more evidence to the critiques formed in the process, the second chapter will address some of the challenges regarding cyber deterrence. Several International initiatives for regulating cyberspace will be examined and determined, if and why they failed to be successfully recognized by the international community. Specific examples of cyber offensive operations, such as the case of Stuxnet and the attacks on Ukrainian power grids, will also be studied. This will help to assess how the previously examined classical and contemporary deterrence concepts are implied in specific cases, their effectiveness, as well as the consequences of these actions. Furthermore, a closer look at the issue of attribution in cyberspace will also take place in this chapter. Studying these problems will demonstrate some of the technical difficulties related to cyber deterrence, such as establishing the responsible actor behind cyber-attacks. Deterrence in the cyber domain has been discussed by various scholars and authors across the fields of International Relations (IR) and cyber-security, as it will become evident from the first two chapters of the thesis. There are a lot of studies on cyber deterrence theories, that rely solely on the direct application of IR theories, which are often deficient in the complex technical understanding required by the cyber domain to comprehend how it functions. On the other hand, many technically advanced publications lack the overall perspective of IR. The first two chapters of the main body will attempt to serve as a synthesis between these two fields, to derive better comprehension for deterrence concepts and how they could be applied to the cyber domain. The main goal of this fusion will be to establish a separate framework of proven and effective deterrence concepts that could ideally serve to formulate national doctrines or cyber deterrence strategies.

The final chapter will engage the synthesis, build on the content analysis and empirical evidence, by indulging in selected deterrence concept groups explaining how they fit in the proposed framework. This chapter will present the results of the thesis, where the conceptual framework will take shape. It will do so by firstly looking at the deterrence by denial cluster and its implementation in the cyber narrative. Especially state utilization of military capabilities to achieve deterrence of warfare action, by both classical and contemporary concepts. It will argue that 'by denial' deterrence differs from other domains by being unique and substantial. Subsequently, the

focus will fall on deterrence by threats and punishment concepts. It will investigate state usage of assets in punishing or threatening enemies' intent on taking cyber warfare actions. It will also evaluate cyberspace compatibility, of classical nuclear deterrence and contemporary concepts of punishment, to determine their applicability. The lack of a simple solution will also be examined by looking further than traditional concepts into a cumulative deterrence approach. This will combine offensive and defensive aspects of previous deterrence concepts to improve the conceptual framework. This will all be synthesized into a proposed conceptual framework for cyber deterrence. The last supportive part will provide the limitations concerning the proposed framework.

Chapter 1: Deterrence: theory and concept.

This part is the backbone of the research. It focuses on both classical and contemporary deterrence theories with the main goal of highlighting relevant concepts that would be suitable for the proposed conceptual framework. Furthermore, by investigating these theories and their criticisms, it will be established which concepts can apply to this newly shaped cyber domain. Ultimately, this chapter aims to determine what changes are required for the implementation of classical and contemporary deterrence strategies and their concepts to cyberspace.

To begin with, the use of military threats is one way of deterrence against global military disasters and war, which has been a fundamental part of international security for more than a couple of centuries. From Carl von Clausewitz's concepts of offensive and defensive war (Clausewitz, et.al., 1989) to Bernard Brodie (1959) and Thomas Schelling's (1966) perceptions of nuclear deterrence, its contemporary state is still being researched and debated. The basic definition of deterrence could be attributed to deploying certain measures by one party to persuade another party to cease any form of initiation of hostile action (Huth, 1999: 28). Generally, deterrence strategies refer to threats of military retaliation towards the aggressor in the international security sphere, but this is not limited only to a military response. The retaliation could also be economic, political, or in any other form that has the potential to prevent warfare action against the threatened state. In other words, successful deterrence could be considered not only in military terms, but also in politics, especially in the field of IR, diplomacy, and foreign policy. A successful deterrence normally refers

to avoiding warfare actions that could deteriorate peacetime diplomatic and military cooperation. In military terms, if deterrence fails the situation may escalate into a crisis or armed conflict with the possibility of becoming a full-scale war. Nevertheless, the avoidance of military crises or wars is not the only purpose of deterrence. Additionally, to ensure successful deterrence, defending states must be able to withstand both, the military and the political demands of their potential adversary. In cases when defending states are unable to withstand that pressure and warfare actions are avoided through a diplomatic agreement where the attacking nation receives its maximum demands, it cannot be claimed that deterrence has been fully successful.

Furthermore, it could be argued that there are two main sets of features for successful deterrence: (1) a defensive deterrence strategy that balances credible coercion, minimizes international and domestic constraints, and has deft diplomacy consistent with several concept criteria; (2) the amount of vulnerability of the attacking state reflected in its internal economic and political conditions (Jentleson and Whytock, 2006: 47-86). In broader terms, a state that wishes to rely on deterrence strategies is more likely to succeed if these two elements are attained. Firstly, if the cost of non-compliance a state can impose on another is greater than the cost of compliance. Then likewise, if the benefit of compliance is greater than the benefit of non-compliance. This is reflected in the deterrence concept criteria, which consists of proportionality, reciprocity, and coercive credibility.

The first is about the relationship between the defending state's nature of objectives, and the capabilities accessible for their accomplishment. In practical terms proportionality in deterrence is focused on the correlation between the scope, objectives, and leverage applied to pursue them. If a defending state imposes demands over an aggressor state, the cost of compliance for the aggressor will increase proportionally to the need of the defender to raise its cost for non-compliance, and thus the benefits of being compliant. This is considered a challenge, as deterrence can be a strategy of limited means, since it may, but not required to, go beyond those limits. Such means are the political and economic actions mentioned above, where the use of force is the limit. If military power is indeed deployed, then it must be limited and abstain from further actions that could lead to full-scale war (George, 1991: 3-14). In any other case, the deterrence strategy has failed.

Reciprocity is outlined as the second concept standard in deterrence theory. It is closely related to proportionality, as it involves a clear comprehension of the connection between the defender state's incentives and the attacker state's concessions. Practically, reciprocity emphasizes on the balance, that often prevails in neither offering too little too late for too much in return, nor offering too much too soon for too little in return.

Lastly, coercive credibility necessitates a combination of calculating both, the benefits as well as the costs of cooperation, and the effort of defenders to convince attackers that non-cooperation could lead to dire consequences. This can be assured through threats, use of force, and economic sanctions, however, they need to be appropriately reliable to successfully increase the supposed costs of non-compliance of the attacker. Nevertheless, defending states having military or economic superiority alone would not be enough to ensure deterrence credibility. Fully successful deterrence is often achieved if other international organizations, like NATO and the United Nations, are supportive towards the defending state, as well as if the stability in that state's internal politics is evident. Another crucial consideration that falls under coercive credibility is the political and economic status of the attacking state. These conditions must be considered since they might affect the attacker's vulnerability to deterrence policies and its capability to recompense unfavourable power balances. The first factor of consideration is whether international political support and regime security are firm, or if there are domestic political gains to be made from improving relations with the defending state. This concept criteria can be further examined in the nuclear age when deterrence was vital for international peace. It is the cornerstone of what is known today as classical deterrence theory, which will be studied in the next part.

1.1: Classical Deterrence theory.

Deterrence as an aim of the strategic policy is certainly not something new. The kind of deterrence practised today involves different features and elements compared to the classical deterrence period during the Cold War. For instance, this period, also known as the nuclear age, introduces one such difference, which is the requirement that deterrence must be absolute, therefore it must not fail in any way (Brodie, 1959: 246). This is a result of the available military capabilities during

the Cold War, namely weapons of mass destruction (WMD), more specifically nuclear warheads. Deterrence thus continues to be effective, although it had no practical chance to prove its efficiency. Nevertheless, deterrence capability is not always war-winning, therefore it must be distinguished in certain important respects. Depending on the case, the maximum possible deterrence may necessitate war-winning capability, such as WMD, but much less force may also possess significant deterrent value (Brodie, 1959: 266). However, the attacking side always possesses great motivation to secure the defender's destruction, especially when the attacker strikes first. In that sense, such motivation must be countered in the only certain way possible, which is to guarantee strong retaliation. This summarizes the basis of classical deterrence as put forward by Brodie (1959). Thomas Schillings (1966: 229) also describes it similarly by arguing that deterrence is pointed at the rational calculator in full control of capabilities and forces. Classical deterrence also involves some issues applicable today, such as the problem of choice among weapons, vehicles, and targets. Contrarily to the issue it induces, it may as well be advantageously falling under deterrence capabilities. They are influenced considerably by the state of civil defence, armaments limitation, and control. The difference, however, is that since the dawn of the nuclear age, 'deterrence' has developed not only special importance but also a distinctive meaning as a strategic term.

In that sense, the nature of classical deterrence may provoke different military solutions that aim to settle every defence issue in one's favour for the most minimal cost possible. One such solution might be the idea of preventive war, which assumes that total war is inevitable and 'strike first' capability is a decisive advantage. Brodie (1959: 7) categorizes this idea as defunct in the nuclear age, due to the nature of WMDs, but also suggests that it might be relevant in the future. This concept is rightfully classified as obsolete since the inevitability of total nuclear war was questionable given the potential costs of hitting first. The moral issue also cannot be denied, especially in a democracy, as Brodie (1959: 8) puts it: "... we have to face the fact that as a nation we are not well equipped to make decisions of this sort." Another solution in the same nature of classical deterrence is the Pre-emptive war, which is less reserved by moral and political considerations compared to preventive war. However, this concept depends heavily on having excellent intelligence and being highly responsive to it. It does so because it is based on a 'pre-emptive attack' scenario, where the attacker has already set in motion its strategic attack, but the

defendant attacks before the attacker's first strike. This is classified as a retaliation of some sort, but it does require highly reliable intelligence sources to be functional.

The final solution of the classical deterrence nature is the massive retaliation concept. The term was brought up in 1954 by US Secretary of State John Foster Dulles, who stated that: "Local defences must be reinforced by the further deterrent of massive retaliation power" (1954, NY Times: 2). Dulles was referring to policy decisions made by the National Security Council that emphasized on depending primarily upon a military capacity to retaliate instantly. This concept of massive retaliation was welcomed with criticism at first, but it was later recognized as the basic orientation of the early Cold War deterrence policy, at least in the United States. Reviewing this concept as a response to less than massive aggressions is in many instances obvious that the attacker may find it hard to believe that the defendant means such retaliation (O'Smith, 1955: 68).

These three concepts of deterrence were all reviewed and applied to some extent during the Nuclear age. Some of them are applicable today, and others are firmly related to the classical deterrence period. In all cases, classical deterrence aims to prevent all-out war in different ways. For one, it relies on nuclear weapons as a type of defensive threat that must be fully effective, allowing no fails. The punishment for a breakdown might result in total annihilation, which is not intended for repeatable actions. A single use of it would bring devastating consequences. Deterrence of the nuclear age means it is a functional strategy, only when states are assured that the retaliatory instrument upon which it relies will not be deployed in any case, as it could lead to a nuclear end of the world. Nevertheless, nuclear weapons guarantee defensive deterrence, thus it must be upheld at a high standard of effectiveness. In short, it is expected that the system will always be ready for deployment while being permanently idle.

Deterrence is often mistaken with war-winning capacities. During the nuclear age, winning would require either a critical and entirely safe superiority in air and nuclear power or success in obtaining it. Since simple superiority in numbers of airplanes or nuclear bombs, for instance, might be of strategic importance, the misperception between deterring and winning is augmented. However, classical deterrence does not rely solely on superiority per se. Before the nuclear age, according to Brodie (1959: 274), forces that were inferior to their rivals might have some real deterrent value. Another author provides an appropriate example of this with the Winter War between the Soviet Union and Finland claiming that if Stalin had a better estimation of the Finnish defensive

capabilities, he would not be so eager to attack them (Lightbody, 2004:55). It seems that the motivation to attack might not have been involved in conquering new territories, but rather the wish to declare to them and the rest of the world a loud diplomatic statement of the Soviet Unions' capabilities. What this example shows is that deterrence was not absolute, and it was conceptually relative before the nuclear age. Its efficiency should be determined not only according to the power it holds but also according to the motivation of aggression which shapes the pressure behind that power. Classical deterrence philosophies may diverge from 'win the war' concepts in several aspects. For instance, they are likely to deviate from their priority. The purpose of establishing a higher level of deterrence is more important than the purpose of guaranteeing capabilities to win a war, the main reason being that the first is likely to be a prerequisite to the second. To achieve deterrence, states should usually want to legalize the least provocative security policies, even where it might result in a sacrifice of some effectiveness.

The first point to be derived from classical deterrence is that the rejection of preventive war has obligated the main actors in the Cold War to a deterrent strategy. This has bound them to make it efficient, avoiding total nuclear war. However, it does not exclude the possibility of failure in classical deterrence. The threat of total war in the nuclear age made states solve unavoidable conflicts by the means of limited war. However, the concept of mutual deterrence remained evident, since such mutuality would have ensured stability in the Cold War situation. Still, with advanced thermonuclear technology, the risk of instability raises exponentially, and therefore mutual deterrence is less likely to be achieved (Schillings 1966: 245). Such nuclear weapons may also be defenceless against unexpected long-distance surprise attacks unless they are purposely intended to withstand such attacks. Schillings also provide the hypothesis that mutual deterrence would only work if all countries were to be self-sufficient bodies with no nuclear technology, at least in their military arsenal. In this hypothetical scenario, even if a nation was determined to attack, it would not care to initiate it. In fact, the Cold War reality was quite different, as states emphasized on acquiring first-strike capability and proliferation, which impaired the stability that mutual deterrence could provide.

The classical deterrence period of the nuclear age brought other ideas related to the concept of mutual deterrence, such as arms control and disarmament. The former pursues the re-establishment of military arsenal with a way to stabilize reliable and mutual deterrence, whereas the latter

allegedly eliminates them (Kolodkin, 2012). The success of either depends on the stability of mutual deterrence. It is just as important in relationships between disarmed countries as it is between armed rivals.

Schillings (1966: 258) argues that to achieve military deterrence is to accept deterrence based on fear. His argument perfectly illustrates the reality of the classical deterrence in the nuclear age since it is based on the fear of nuclear oblivion. However, the implied contrast between stabilized deterrence and total disarmament is not convincing enough. In this respect, if there is no fear of consequences, nothing would be able to prevent small wars to escalate into big ones. The extent of the fear involved in any deterrence concept was crucial to its efficiency in the nuclear age. The consequences of breaching deterrence based on fear, are simply the worst outcome for all parties involved. Little depended on who would strike first. After all, these consequences were taken for granted and called a "balance of prudence." (Schillings, 1966: 259).

Despite these arguments, the bridge between classical and contemporary deterrence remains the strategy of containment, which is the policy seeking to protect certain values like personal freedom, democratic institutions, fellow democracies, etc. Classical deterrence concepts have always been an instrument, through which one state aims to protect these values and deter another from attacking by political or military means, which could inflict severe damage. This is also relevant for contemporary deterrence, which will be examined further in the next part.

1.2: Contemporary Deterrence theory.

Deterrence, as a conceptual strategy has significantly progressed throughout the Cold War. As it was shown in the previous part, classical deterrence was generally meant to prevent nuclear hostility. After the end of the nuclear age, the risk of such war between major world powers has decreased to the lowest point in contemporary history (Cohen, 2011). However, the changing nature of threats became evident, especially to the United States and its allies. This has motivated a significant broadening of deterrence concepts, which will be addressed as contemporary

deterrence theory from now on. While some of the post-Cold war objectives of deterrence have remained untouched, others have extended through implying new ideas and models. The objective to deter the deployment of nuclear weapons and other WMDs has remained intact together with preventing aggression against any allied vital interests and security as well. However, these objectives have evolved to become the contemporary deterrence model known as extended deterrence that covers threats against the free use of warfare domains, such as the seas, airways, land, and space, as well as the essential resources to security and welfare (National Research Council, 1997). This concept refers to the protective umbrella extended over allies to defend their territory from attacks. During the Cold War period, extended deterrence covered mostly nuclear attacks. However, NATO deterrence policy does not differentiate between a nuclear attack and a conventional attack. Although the threat of such attacks is low, the NATO protective umbrella remains crucial for preserving peace. Since the threat is lower, the relationship that builds this vital framework could weaken unless they receive consistent consideration.

To achieve such deterrence objectives, the possibility of hostile actions must be anticipated in advance. The attacker must then be deterred from undertaking such actions by posing a credible threat of punishment. Doing so aims to punish the attacker for striking first, guaranteeing the prevention of further aggressive actions (Jervis, 1982: 17). This concept might seem familiar to the classical deterrence based on fear. However, the approach to contemporary deterrence may also involve a range of activities in other spheres – political, diplomatic, economic, as well as military – independently or coherently. A modern strategy of deterrence, therefore, could encompass activities that can affect almost all kinds of foreign policy actions. Nevertheless, the potential or actual use of military force downgrades all other deterrence efforts within other spheres of foreign policy.

Post-Cold War deterrence has become more complex, as the tactics referring to circumstances that demand deterrent actions may vary and must be more systematic and adaptive. The probability of involvement in warfare actions using conventional military capabilities that are initiated by states non-major political powers, in matters involving less than national survival, has increased, while the role of using nuclear weapons has decreased to be minimal (Nalebuff, 1988: 420). Such a drastic change puts more emphasis on efforts to block proliferation rather than the actual use of nuclear weapons. Therefore, conventional military capabilities are becoming gradually more

important for deterrence in the strategic aspect of avoiding proliferation. Moreover, other conventional military arsenals that can inflict mass casualties, such as chemical and biological weapons, are also posing concerns, since they could be acquired more easily than nuclear weapons, and therefore controlled by rogue states or terrorist organizations who do not obey to the international law.

Considering the other major political power of the Cold War, the USSR suggests a reorientation towards minimal deterrence policy. This has resulted in the acceleration of 'perestroika' towards the end of the conflict in 1988-1989. According to this proposition, states can possess no more WMDs than necessary to deter adversaries from proportionally attacking (Kristensen et. al., 2009: 21). However, other studies suggest that even though the Intermediate-Range Nuclear Forces Treaty (INF) agreement has initiated the disposal of some nuclear weapons, and the Strategic Arms Reduction Treaty (START), which eliminated nearly all Soviet anti-silo capabilities, there are still more than 20,000 nuclear weapons and 5,000 strategic missiles remaining, which does not match the concept of minimal deterrence (Gergorin, 1991: 4). The collapse of the Soviet bloc had a profound impact on the international environment, as it was not clear which direction would the former Union take. At the time, several scenarios were considered by Gergorin (1991), but the most accurate one seems to be predicting autocracy. He suggests that: "[...] economic crisis would, in the short or medium term, incur the downfall of the democratic forces and the imposition of a nationalist, authoritarian and autarkical group or person" (Gergorin, 1991: 7). Such prediction is close to the reality of the 21st century since the Russian autocratic regime has been able to rearm in two critically important areas, namely strategic nuclear arms, and conventional weapons. However, the international arms control treaties and regulations prevent some of the Cold War's classical deterrence problems, like the risk of a surprise attack.

The implications of such rapid geopolitical changes are also important regarding national interests since they are not as largely recognized as other kinds of threats. An appropriate example might be the situation in the Middle East. While some might assume that deterrence failed to prevent the Gulf war, due to the lack of international intervention, others anticipate that the following US invasion was crucial and prevented the further threat to the Western world's oil supply. (Stein, 1992: 163). Thus, perceptions of national interest are dependent on the global political context, opened by the dynamics of rapidly changing events, such as wars. Deterrence strategies are unable

to be established on the principle of static international relations, in which a commonly accepted posture can endure indefinitely (National Research Council, 1997: 21).

Ultimately, in the two decades after the Cold War, Western deterrence has been focused on three key types of threats. Firstly, the Soviet threat has essentially vanished, at least in the form of a surprise attack. Hence, there was a necessity to preserve the balance for the West, since the Russian potential has been increasing, and it might need to be deterred if it reshapes as a new potentially aggressive strategy. Secondly, the danger of non-state actors became evident in the form of terrorist organizations and rogue states. Such actors are hard to deter, as international law does not apply to them. Lastly, one of the primary risks refers to regional destabilization by countries or organizations which could potentially obtain dangerous ballistic, chemical, or nuclear weapons. Such is the case of the Middle East, where the combination of religious fundamentalism and the oil industry creates a potentially dangerous environment, which is also hard to deter.

Contemporary deterrence is influenced by other perspectives as well. Humanity is at the dawn of a new digital era, which is changing everything, including the military. The technical revolution that is happening will essentially change the way of using military forces, partially based on advancing military technologies. Moreover, it develops on information-based extents of understanding the disposition and actions of both the opponent's military arsenal and their critical command and control systems. This would include knowing their detailed location and possessing the capabilities to strike at them with great precision, from an extensive distance, and in a short timeframe. Such technologies are rapidly integrating into new operational concepts for deterrence. Some of the more significant aspects of this digitalization may include information warfare, precision strike, and other military operations, which are inevitably going to all take place in the fifth warfare domain - cyber. The challenge for states is to be able to apply these new capabilities and concepts credibly, in prospect to specific situations that they wish to deter, like their opponents from deploying them, or at least mitigate their effects.

1.3: Deterrence concepts and the cyber domain.

According to Western military doctrine, including NATO and the US Department of Defence (DoD), there are four classical warfare domains, which consist of land, sea, air, and space. They

are all classified as conventional, having in common that they are naturally physical environments that are subject to the laws of nature and can be only partly modifiable by people. However, in recent years both the DoD and NATO have declared that ‘cyber’ is also an operational warfare domain, which is equal to the conventional domains. Dictionaries define ‘domain’ as a sphere of knowledge, influence, or activity (Definition of DOMAIN, n.d.). The DoD defines cyber as “A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.” (Department of Defence, 2017). From these definitions, it can be confirmed that ‘cyber’ is an autonomous operational warfare domain, in the same way as the other conventional domains. The layouts of all these conventional domains are being dynamically digitalized, although at a different rate. It is definite that a ‘cyber layer’ is being established into all conventional domains. Gian Piero Siroli (2018: 112) argues that the cyber domain is becoming a background that causes military infrastructures to integrate the modern battlefield and coordinate the inter and cross-domain operations. In other words, the conventional domains are all compatible with and connected by the newly emerged cyber domain. However, the key difference between the cyber and conventional domains remains the geography, or the location of cyberspace, which is completely human-made. The natural properties of this domain are exclusively in the hands of mankind, while land, sea, air, and space are subject to physical and natural laws of the environment. The layout of the cyber domain is very flexible and vulnerable. Cyberspace dimensions can both, appear or disappear with a single command or when they are under attack. Furthermore, ‘cyber’ is relatable to both weapons and targets, in the sense that the virtual space itself in which the weapons are situated can be affected by conventional or cyber weapons. If cyber weapons can be considered within their virtual domain, the mobility, calculation of speed, and manoeuvrability of their operations are very high (Siroli, 2018: 113). In other words, the high range and ultra-speed of the cyber domain enable operations to be conducted across the globe in a matter of seconds. Thus, the striking power in terms of volume and range is also substantial. There is no clear explanation of what the cyber domain is, nor where militaries should be operating within cyberspace – as there is no clear concept on the exact missions they should be doing.

Some authors argue that the military must limit its activities within cyberspace (Crowther, 2017: 63). This is not meant as to restrict military action within the cyber domain, but rather to limit what

functions should the military cyber units execute. For instance, the same author argues that in the United States around 90% of all cyber activity is private, meaning that it is managed by private citizens or corporations (Crowther and Ghori, 2015: 81). Thus, the military should not be operating within this 90% unless it pertains to one of the missions appropriate for military participation. According to the DoD, there are three main cyber missions: (1) Defend DoD networks, systems, and information; (2) Defend the US homeland and US national interests against cyberattacks; (3) Provide support to military operational and contingency plans (Department of Defence, 2018: 3-4). As an example of boundaries, Crowther (2018: 64) suggests that the military cyber units should not be involved with say, interactions between private corporations like Pay-Pal and Amazon unless the person initiating the payments are involved in activities that would make them the target of intelligence operations. In this respect, the military should not be operating within the private sector, but the question remains as to their role in the cyber domain. According to McGuffin and Mitchell (2014: 401-402), this role is explained in the four sets of activities that relate to the military; intelligence, information, crime, and military operations. All these activities can be carried out in the cyber domain, since militaries contribute to intelligence operations, conduct information operations, and sustain both, special and conventional military activities. Collectively, these four areas compose the military cyber domain, as shown in Figure 1 of appendices (Crowther, 2017: 65).

Regarding conventional and special military operations within the cyber domain, an instance of cyber-supported military operation could be the 2008 Russian actions against Georgia. Although one year earlier, Russia conducted operations entirely within the cyber domain against Estonia, the situation in Georgia was quite different. In this sense, the Russians conducted military cyber operations against targets in Georgia to damage their command and control systems, in combination with conventional military operations on the ground and air (AFCEA, 2012). This also serves to prove the argument that the cyber domain can connect the other four conventional military domains.

The cyber domain is not restricted to the tactical and operational levels only. It covers the strategic framework as well. Deterrence is a strategic concept that inevitably exists within all four conventional domains of warfare. It is, however, much harder to set a clear framework of deterrence concepts that are feasible for the cyber domain, due to its fast-paced technological

development. Generally, cyber technologies are offence devoted, as it is often easier, as well as significantly cheaper to deploy an attack on network infrastructure, rather than defending it, assuming the higher costs of defence and the limited efficiency (Siroli, 2018: 114). In this respect, the above-studied deterrence concepts can be grouped into two main categories according to their functionality – deterrence ‘by denial’ and deterrence ‘by punishment’. Classical concepts are mostly clustered in the ‘by denial’ group. It has been debated whether the classical deterrence concepts of the nuclear age apply to cyber warfare or a new equivalent is needed (Richet, 2015: 112). Most of the classical concepts are impracticable, like absolute deterrence, which states that it must not fail in any way, to preserve the peace. On the other hand, the technological dominance of the offensive function could also re-establish the strike first conceptual approach of classical deterrence. Clearly, due to the rationality and affordability of cyber-attacks, concepts like pre-emptive strikes in the cyber domain are going to be the only viable option for the deterrence ‘by punishment’ cluster. In principle, the core concept of deterrence by retaliation is crucial for this group, however, it is complicated by the problem of attribution, which will be discussed further in the second chapter. In any case, the key nuclear-age classical deterrence concept of mutual assured destruction seems irrelevant to the cyber domain, even with respect to attacks on critical infrastructures that cause physical damage on industrial control systems. Still, other classical deterrence concepts might fit just in place for the cyber domain. For instance, the idea that less force may also possess significant deterrent value might be relevant for the ‘by denial’ group. This is because establishing cyber defence systems typically requires little effort, but it may provide some deterrence value in return. Another concept that could be considered relevant to the cyber domain, is the classical concept that forces which are clearly inferior to their rivals might have some deterrent value. Since the nature of cyber-attacks is relatively open-source, it means that anyone with enough technical knowledge might be able to deploy a simple attack with deterrence goals in cyberspace, including state-sponsored attacks by small but technically developed countries. An appropriate example for this is Estonia, which is one of these nations that are comparatively small both, geo-politically and by population, but also very active within the cyber domain. Lastly, the classical idea of deterrence based on fear of consequences might not only be a relevant concept but even a functional group on its own in cyberspace. This is because the cyber domain serves to connect all other conventional warfare domains. If a defender-nation possesses a very broad spectrum of cyber weapons and other interconnected capabilities, it guarantees at

least some deterrence value, since adversary states might not be so keen on attacking based on fear of such capabilities.

As for contemporary deterrence concepts, they can also find a place in the ‘by denial’ and ‘by punishment’ groups. Most of them are applicable within the cyber domain since cyber-attacks have been deployed together with conventional military operations after the Cold War. For example, the ‘by punishment’ group can be considered relevant since the cyber domain provides a way to punish without raising too much international attention. The cyber domain is undoubtedly the least regulated domain of warfare, both because it is the latest domain to occur, and also due to distinctive difficulties that further complicate the approach. Moreover, the concept of international collaboration in deterrence should also apply to cyberspace, since allied vital interests and security could be threatened there. On the other hand, the idea of minimal deterrence policy could be viewed both ways – indeed, the cyber domain ensures less need for deterrence in the other conventional domains, however, it provides yet another unregulated and potentially destructive battlefield. From a certain perspective, it might seem like there is a global arms race for cyber capabilities going on between both state and non-state actors (Buchanan, 2017: 110). In this respect, any legislative and regulative activities regarding the cyber domain appear to be very complicated. Additionally, the pace of modification in this field is very high and often critical. This is due to the fast-paced technological development, resulting in the frequent manufacturing and deployment of new cyber tools. Overall, the cyber domain is very dynamic, difficult to handle, and perhaps in need of an adaptive and resilient approach, especially in terms of national strategy, which will be examined in the next part.

1.4: Deterrence and National Cybersecurity Strategies.

Different countries all over the world are currently attempting to shape the process of digital transformation to obtain the benefits of this global change in their societies. However, the rapid development of digital technologies involves some risks as well. The digital infrastructure worldwide is still largely insecure due to technical and other factors, which makes this transformation prone to exploitation. It is therefore imperative to strategically deal with cybersecurity challenges if the digital transformation is to be successful. Consequently, most

technologically advanced states are constantly reviewing their national security strategies to ensure that they are always improved and prepared for the risks which are continuously emerging in a more closely networked and politicized world. This part examines the Western model, which will include examples from the European Union and the United States, although some states in the East like Russia and China are actively pursuing strategic cybersecurity measures as well.

The European Union (EU), for instance, drafted a combined cybersecurity strategy in 2013 and upgraded it to a Network and Information Security directive in 2016, requiring all member states to develop their national cybersecurity strategies (Lord, 2016). As a result, Baezner and Cordey (2019) identify six common elements that have emerged from this directive through most of the member states. Firstly, the EU states have developed a detailed approach to cybersecurity, which consists of technical capabilities. Secondly, cybersecurity strategies are separate doctrines that are aligned with broader national security strategies. Third, most strategies are focusing on building defensive cyber capabilities, except the Netherlands, which is the only state that explicitly discloses the development of its offensive capabilities to rely on deterrence by punishment. In that sense, it does not mean that other EU states are not to developing such capabilities, however, they would rather not reveal such information. Fourth, all EU cybersecurity strategies emphasize the significance of international cooperation within the framework of regional and international organizations to improve collaboration in the cyber domain. Fifth, all member states underline the need for cooperation with the private sector in their strategies. For example, the Netherlands and Italy have adopted an approach that involves a distinct public-private partnership for cybersecurity, while Germany has only established a partnership with the operators of critical infrastructures. Other EU member states prefer to provide funding to industries involved in cybersecurity (Baezner and Cordey, 2019: 8). Lastly, all member states highlight the significance of raising cybersecurity awareness regarding issues at all levels of society, as well as the need for better education. As it comes to the military – each state has a cyber body, which is often directed by the commander-in-chief of the armed forces of the member state (Baezner and Cordey, 2019: 7). This hierarchical method shows that member states are increasingly more aware of the importance of cybersecurity regarding all parts of the armed forces. The situation is similar further west in the United States, although their national cybersecurity strategy has evolved and transformed many times from 1988 to contemporary days, especially after 9/11.

The George W. Bush administration proposed some new doctrines and passed legislation that shaped US policies in cyberspace (Soesanto, 2019: 9). Some of these include; (1) the Patriot Act, which extended the authority of the National Security Agency (US Congress, 2001); (2) the Homeland Security Act, which established the Department of Homeland Security (US Department of Homeland Security, 2002); (3) and perhaps most relevantly, the announcement of the National Strategy to Secure Cyberspace, which enabled defence and security agencies to strengthen their efforts, improve their capabilities, and proclaim that the US “reserves the right to respond in an appropriate manner” to state and non-state actors (The White House, 2003). Indeed, these legislative efforts provided additional power to the US security agencies, however, the strategic aspect was still lacking. This is evident since the Department of Defence announced its primary cybersecurity strategy three years after the National Strategy to Secure Cyberspace. The DoD strategy clearly stated the Pentagon’s intention to obtain “military strategic superiority in cyberspace” and to ensure that “adversaries are deterred from establishing or employing offensive capabilities against US interests in cyberspace” (Chairman of the Joint Chiefs of Staff, 2006: 13). The strategy also states that the DoD will:

“[...] deter malicious adversary use of cyberspace while promoting freedom of action and trust and confidence in US cyberspace operations. Through deterrence, DoD seeks to influence the adversary's decision-making processes by imposing political, economic, or military costs” (Chairman of the Joint Chiefs of Staff, 2006: 14).

This strategy undoubtedly illustrates the reality of the cyber domain. Eventually, it underlines that deterrence in cyberspace is not impossible, but on the contrary, it is an essential element to ensure stability and security. On a strategic level, the cybersecurity strategy continued to evolve during Obama’s presidency, which builds upon the efforts of the previous administration. Obama strived to develop a US cybersecurity strategy that is “designed to shape the international environment and bring like-minded nations together on a host of issues, including acceptable norms regarding territorial jurisdiction, sovereign responsibility, and use of force” (The President of the United States, 2009: 20, cited in Soesanto, 2019: 13). Obama also established a sort of hierarchy in his strategy through “anchoring and elevating leadership for cybersecurity-related policies” by appointing a cybersecurity policy coordinator at the White House, who was previously involved with the military (Soesanto, 2019: 14). President Obama signed five executive orders to realize the objectives of his strategy. Their main purpose was to authorize offensive and defensive actions in cyberspace. The most important of them was Presidential Policy Directive 20, which went into

effect in October 2012. The classified document entered the public sphere in 2013 when it was leaked by Edward Snowden and published by The Guardian (Greenwald and MacAskill, 2013). The directive basically provides a framework for the US offensive and defensive cyber operations. On its policy side, some authors like Segal (2016: 28-29) argue that this directive has slowed down US offensive operations in the cyber domain compared to previous operations like Stuxnet, which will be examined in the next chapter. This hampering was transpired by characterizing some comprehensive standards that would guide future cyber operations within its inter-agency planning process. This included norms on impact, risks, methods, geography and identity, transparency, authorities, and civil liberties - while ultimately placing final say in the hands of the President. In the context of deterrence, the Presidential Policy Directive 20 modified in response to the extensive criticism of other offensive cyber operations, which were carried out without adequately assessing their implications. These actions of President Obama emphasized on his idea to enforce deterrence by denial and deterrence by de-legitimization. Another vital policy that illustrates the US cyber deterrence strategy relevant for the previous decade is the Department of Defence Strategy for Operating in Cyberspace. It recognizes that the DoD is predominantly concerned with three main areas of potential enemy activities. These are as quoted:

“(1) theft or exploitation of data; (2) disruption or denial of access or service that affects the availability of networks, information, or network-enabled resources; and (3) destructive action including corruption, manipulation, or direct activity that threatens to destroy or degrade networks or connected systems” (Department of Defence, 2011: 3).

The Department also highlights that the US will consider cyberspace as a warfare domain, maintaining capabilities to effectively operate in it. Such operations require establishing, training, and preparing military and civilian forces to conduct both offensive and defensive operations in the cyber domain. Consequently, maintaining an offensive cyber capability automatically becomes a priority. Their use as a potential penalty measures in effective deterrence strategy in response to, or in the prevention of, a cyber-attack must be credible. Such capabilities may include cyber weapons, which are defined as “digital objects that can be used to achieve military objectives by disabling key functions of computer systems and networks.” (Yannakogeorgos and Lowther, 2013: 116). Corresponding to the changing policies in the White House and the DoD, the NSA also utilized and united their cyber operational efforts within the newly created US Cyber Command, with the mission is to:

“[...] direct the operations and defence of specified DoD information networks and; conduct full-spectrum military cyberspace operations to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries” (Department of Defence, 2010).

When President Trump was inaugurated at the beginning of 2017, his new administration faced great public pressure to deal with the alleged cyber interference in the 2016 elections by the Russian Federation. The President wobbled between agreeing with the intelligence community that Russia is, in fact, responsible, and at the same time arguing it “[...] could have been other people and other countries, nobody really knows for sure,” (Krishnadev, 2018). In this respect, any kind of retaliation within the cyber domain remains unknown, at least to the publicly available sources. On the other hand, the political debates in favour of a more aggressive cyber deterrence approach took more initiative in all three branches of political power in the face of the DoD, Congress, as well as the White House. This is evident from the DoD’s report on task force cyber deterrence (DoD - Defence Science Board, 2017). This report predicts that the concept of deterrence by denial could become inefficient in cyberspace, since “the unfortunate reality is that, for at least the coming five to ten years, the offensive cyber capabilities of our most capable potential adversaries are likely to far exceed the United States’ ability to defend and adequately strengthen the resilience of its critical infrastructures” (DoD – Defence Science Board, 2017: 4). Generally, the report proposes eight deterrence concepts to implement in favour of setting internationally recognized norms and rules of the cyber domain (DoD DSB, 2017: 7-8). Another interesting strategic concept was the idea that “responding to adversary cyber-attacks and costly cyber intrusions carry a risk of escalation, but not responding carries near certainty of suffering otherwise deterrable attacks in the future” (DoD DSB, 2017: 7). Indeed, it becomes clear from this report that the intentions of the US under the Trump administration are to advance and develop cyber deterrence concepts by relying on ideas, such as norms and rules, together with more aggressive approaches like deterrence based on fear of consequences. From a theoretical perspective, such an approach differs from the past US deterrence ‘by denial’ logic moving it into the more offensive area of ‘deterrence by punishment’ and ‘by fear of consequence’. Since the ‘by denial’ concept is shaped by past events, the expectation of future cyber actions between the US and other actors may require ‘proof’ of the US cyber capabilities to renew the desired deterrence strategy.

In 2018-19, President Trump advanced the concepts of the task force report by adopting a national cyber strategy. The Strategy envisioned the US cyber capabilities, as well as an initiative for cyber deterrence, through which the US will:

“[...]work with like-minded states to coordinate and support each other’s responses to significant malicious cyber incidents, including through intelligence sharing, buttressing of attribution claims, public statements of support for responsive actions taken, and the joint imposition of consequences against malign actors” (The White House, 2018: 21).

In this respect, the more diplomatic approach would be a deterrence strategy based on internationally accepted norms and regulations. This possibility will be examined in the next part of the thesis, along with some of the challenges regarding deterrence in the cyber domain.

Chapter 2: Challenges to Cyber Deterrence.

This chapter will be more practically oriented, providing an insight into some of the challenges to cyber deterrence. It will also demonstrate attempts to implement norms and regulations, determining if they were successful and if not - investigating where and why they failed. The part will offer a thorough case study examination of cyber-attacks to perceive the practical side of the already established deterrence concepts in the previous part. Other challenges, such as attribution in cyberspace and non-state actors will also be examined.

Overall, cyber deterrence is not an easy strategy to achieve. Some authors argue that difficulties, such as those listed above, together with diminishing capability to retaliate, unnecessary escalation, as well as potential legal difficulties, make cyber deterrence an impracticable strategy (Lee, 2015: 14). The problem with such statements, although correct in defining the issues of cyber deterrence, is that they are pursuing the absolute classical deterrence concept, which anticipates that deterrence must not fail in any way. In the cyber domain, this concept is not applicable, as it has been already established by the previous chapter. The circumstances involved in the cyber domain are such that it has not been easy to apply all concepts of classical deterrence to cyberspace. As such, cyber deterrence may imply complexity, as well as actions in a contemporary world, whose outcomes and purposes are much less absolute and more pragmatic than those of the nuclear age. The thesis supports the argument that views cyber deterrence as a separate branch in deterrence theory, which has been developing ever since the actions in Estonia (2007) and Georgia (2008) (Stevens, 2012:

148-149). This idea has largely failed to translate into concrete military doctrines and strategies, that are separate from the national security strategies of most states. Meanwhile, it is evident that cyber deterrence has yet to play a greater role in international security. The US, as it has been apparent from the last part, is developing another branch of cyber military strategy through policies, which strive to achieve preventive effects. The attempts to develop norms and rules has remained a focal point in the American geopolitical initiatives, despite the ‘America first’ approach of the current US administration and its ambition to develop more offensive cyber capabilities.

These capabilities can be demonstrated by nation-state actions in cyberspace. Such actions might be defensive as well, although this part will emphasize on the offensive actions conducted by both, state and non-state actors. Such actions have been continuously deployed for sabotage and espionage purposes since 2003. Well-known examples that will be discussed in this chapter include the Russian attacks against Estonia (2007) and Georgia (2008), and perhaps most notably, operation Olympic games, also known as ‘Stuxnet’ (2006-2012). More recently, a wave of cyber-attacks has been revealed to range from continuous Russian aggression against Ukraine power grids, (Zetter, 2016) to infiltration of US federal offices, (Lipton, et.al., 2016). This trend is very likely to continue, due to the relatively low cost of cyber-attacks and the higher chances of them being successful. Consequently, this ensures that countries will not only keep deploying cyber-attacks but also that they will improve and develop them in the future. Artificial Intelligence (AI), for example, may drastically enhance cyber capabilities. Many authors support this statement claiming that introducing AI and Machine Learning systems will become an integral part of both cyber offence and defence, which indicates an escalation in frequency, impact, and sophistication (Yang et al., 2018).

As it comes to non-state actors, they will be recognized as another challenge in cyberspace. They represent a form of interference and acknowledge that attacks and counterattacks may also come from third parties that are not state-related. This part will emphasize on the different groups that may include non-state actors in cyberspace (Sigholm, 2013). It will also assess their role, together with the benefits and drawbacks regarding deterrence. Nevertheless, this challenge further highlights that there is a wide ‘grey zone’ in the cyber domain, especially regarding disruptive activities by non-state actors. This draws the line between disturbance and real damage that could

eventually lead to the use of force, which could escalate and initiate a cyberwar without any state to state involvement.

Lastly, the attribution challenge is often the most cited one regarding the practical unavailability of cyber deterrence as a strategy. This problem will be thoroughly examined in the last part aiming to establish how sure should a state be to attribute a cyber-attack. With attribution, the anonymity provided by cyberspace grants an opportunity for adversaries to commit attacks that exploit vulnerabilities without revealing their identity. Consequently, a state can deny responsibility even if the victim can pinpoint the origin of this attack to the accused state by employing forensic techniques. This denial is possible due to the infrastructure of cyberspace, and technology allowing attackers to mask their identity, thus making the recognition of any involved actor very difficult. This could be avoided if states manage to establish a set of internationally recognized rules and norms for cyberspace, which will be examined in the following part.

2.1: International cyber deterrence initiatives.

Going back to the Western model, there are some noticeable examples of international cyber deterrence initiatives. It was around the time of President Bush's administration that the issue of internationally accepted rules and norms in cyberspace began to attract more attention. An appropriate example is provided by the Commission for the cybersecurity of the 44th President of the US. The report stated that:

“The US willingness to cooperate with other governments on cybersecurity will be an important component of US advocacy. That cooperation should focus on establishing norms, which are expectations or models for behaviour... A normative approach to international cybersecurity focuses on how countries should behave” (Center for Strategic and International Studies, 2008: 20-21).

In the contemporary discourse of US cyber strategy, norms are considered as a strategic objective and are clearly understood as regulations for the international community in cyberspace. Still, this quote also indicates the ambitions of the US to play a leadership role in this field. It suggests that

the idea was combined with deterrence as a joint component of international strategy, involving advocacy, cooperation, and rules. The report even goes so far as to portray the US as an alternative to the United Nations (UN), which was deemed “politically incapable of enforcing a global cybersecurity treaty” (Center for Strategic and International Studies, 2008: 21). This proposed setup would let the US be the primary viable authority that deals with international agreements and promote rules and norms in cyberspace. Such an idea would not be easily accepted by nations, like China and Russia, and thus the US idea of internationally accepted rules and norms for the cyber domain remains unrealized. This leaves cyberspace as the least regulated warfare domain, allowing state-actors to launch attacks without any fear of sanctions and violating international laws.

Nevertheless, the American efforts did not halt and in 2011, the US International Strategy for Cyberspace was signed by Barack Obama. It is the first US policy document to provide, “an approach that unifies our engagement with international partners on the full range of cyber issues” (The White House, 2011). Norms and rules are endorsed in the context of administering the broader prospects of peaceful and just interaction within the cyber domain. The document underlines the collaboration and cooperation, as well as confirming the right to self-defence under the UN Charter. The rules and norms in this policy cover technical issues of network functionality, as well as fundamental freedoms, like free speech and the right for privacy. A notable statement of this document is that “... adherence to such norms brings predictability to state conduct, helping prevent the misunderstandings that could lead to conflict’ (The White House, 2011: 9). This quote indicates the relation between norms and rules for the cyber domain and deterrence. Other similar connections, like in 2010, the US Deputy Secretary of Defence highlighted the problems inherent to cyber deterrence, concluding that deterrence by denial would be most beneficial to the United States, suggesting that if “there are to be international norms of behaviour in cyberspace, they may have to follow a different model that is not derived from nuclear deterrence” (Lynn, 2010: 100). Although this statement corresponds with the argument of the thesis, it is evident from the last chapter that President Trump’s administration is slowly replacing the concept of deterrence by denial with deterrence by punishment. Nonetheless, the primary role of authority in crafting internationally accepted rules and norms for the cyber domain remains an objective to the current US administration, as it has been established from the national cyber strategy of the United States (2018). Consequently, it may be concluded that the US anticipates some deterrent effect from the

creation of international cyberspace norms if they are aligned with their national interests. Cyber deterrence might not be guaranteed by rules and norms alone due to challenges, such as non-state actors who ignore international law. While it is a hard task to achieve, internationally accepted regulative norms could act as a deterrence approach that will certainly help regulate and keep track of actions in the cyber domain. Such initiatives are still in their earlier stages and no global or US-supported framework of legislative norms and rules has been established and globally accepted, nor has a separate military doctrine or national strategy for cyber deterrence.

Despite the US efforts to portray itself as a global leader in cyberspace, other world powers and organizations have also tried to initiate internationally accepted norms and rules for cyberspace. A global agreement is hard to achieve, mainly because different states have different interests, thus making it difficult for everyone to settle on a certain set of norms and rules. The UN is one of the organizations that attempts to prevent this challenge by hosting many initiatives and international groups working on the broad issues of cyberspace. One such international body is the UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security. They came up with a report, which repeatedly refers to the establishment of “norms pertaining to State use of ICTs, to reduce collective risk and protect critical national and international ICT infrastructure” (United Nations, 2010: 7). On a military level, NATO is also an appropriate example for an organization advocating that globally accepted norms and rules for cyberspace will reduce the risks in this domain. (Stevens, 2012: 161). All NATO members have supported this initiative, going as far as the secretary-general making frequent reference to the deterrence potentials of collective action, by enforcing article 5 of NATO’s commitment clause to mutual defence against aggressive actions (Corera, 2019). These examples clearly illustrate the international efforts for norms and rules regarding the cyber domain. However, as it has been previously noted, it is not easy to attain global agreements, due to the difference in national interests.

By contrast to international organizations, it could be argued that Russia views ‘cyber’ as a substance of internal security rather than foreign affairs. Their participation in global treaties has been based upon their desire to self-manage the risks within their own sovereign borders (Stevens, 2012: 162). This indicates that the concept of normative based cyber deterrence, as proposed by the West, is largely unpopular in the East. Such a statement could be supported by the Shanghai

Cooperation Organization (SCO), where Russia together with China, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan adopted their own accord which defined “information war” as “dissemination of information harmful to social and political, social and economic systems, as well as spiritual, moral and cultural spheres of other States” (Kanuck, 2012: 17). The interpretation itself demonstrates the difference between the eastern and the western models. The east defines the information spectre of the cyber domain, whereas the west defines the cyber aspect, which includes cyber-attacks that aim to disrupt or destroy systems or critical information infrastructure. Disregarding any difference, the main goal of the negotiations should be concentrated on creating an internationally accepted posture on global treaties, concentrated on endorsing norms and rules that can clarify jurisdictional responsibilities, and establish international institutions that strive to enable the exchange of information between countries and their security communities around the world.

Perhaps the European Union best fits in these criteria through the Council of Europe. Going back to the beginning of the 21st century, the Council of Europe established the convention on cybercrime, which is the primary transnational treaty that seeks to focus on crimes in cyberspace, by adjusting national laws, improving investigative techniques, and increasing cooperation among nations (Convention on Cybercrime, 2001). More recently, the Council proposed another global internet treaty that would execute the abovementioned functions as well as aim at protecting the free use of cyberspace. In particular, the proposition consists of establishing an Organization for Security and Cooperation in Europe (OSCE), with the main purpose of sharing information on cyber deployments during military conflicts (Galbreath, 2008: 23). This initiative was supported by the main world powers, such as the US, Russia, and others, however, the actual executive power of this organization remains limited.

Another attempt for establishing rules in the cyber domain is the Tallinn Manual. This is a theoretical, non-binding effort on establishing the proper way for international laws to be applied regarding warfare actions in cyberspace. It was supported by NATO and written by a group of international experts in the field. The Tallinn Manual was the first such attempt to comprehensively analyse the topic of rules and norms for cyberspace, bringing some degree of clarity regarding legal issues. The focal point of the manual is concentrated on those cyber actions that are comparable to ‘armed attacks’ in conventional military domains. Such cyber-attacks could

authorize states to self-defend, similarly to attacks transpiring during military conflicts. The better part of the Tallinn Manual has emphasized on solving these problems (Schmitt, 2017). The second version of the manual studies the international legal agenda that applies to such disruptive and destructive cyber actions. The applicable legalities include a law determining state responsibility, a law of the seas, international telecommunications, space, and diplomacy, with emphasis on individual human rights law. This second attempt also examines other general values of international law, such as sovereignty, jurisdiction, due diligence, and the prohibition of intervention, apply in the cyber domain. (Schmitt, 2017).

Despite all international initiatives to regulate cyberspace, the effectiveness of the norms-based deterrence approach remains questionable, mainly because no global agreement has been reached yet. In fact, from the many unsuccessful initiatives, one may conclude that even if it was possible to get all nations to obey a set of rules and norms, established through negotiations and diplomatic efforts, there are no guarantees that all states would fully adhere to such rules. Although the norms-based approach might not provide absolute deterrence to the cyber domain, it still needs to be regulated to avoid cyber actions that aim to exploit this lack of rules. This makes the norms and rules deterrence concept viable for a deterrence strategy in cyberspace if it is combined with the continued attempt to find other deterrence methods that provide solid effects in a domain that is unsuitable for applying conventional models.

Overall, even if cyber deterrence could be made to fully function between states through normative agreements, there is a way more disturbing side on a non-state level, mainly because in contrast to traditional military domains, the tools and weapons deployed within the cyber domain are widely accessible to both, state and non-state actors who do not operate under similar normative values.

2.2: Case studies of nation-state actions in the cyber domain.

As it became clear in the first chapter, the concepts of deterrence by punishment and by denial are designed to alter the cost-benefit calculations of enemies. Most importantly, they need to be credible to function properly. Consequently, if a country wishes to deter or attack it must provide demonstrable signals for its cyber capabilities and that it can execute the threatened attack. These concepts are applicable in cyberspace, in the same way as they are relevant to the other four

conventional domains. This is because cyberspace spans three-domain layers, which are visualized by the US Strategic Cyberspace operation guide as physical, logical, and cyber-persona. The physical one consists of the physical network components. The logical layer is the digital connection between the physical layer and the cyber-persona. The last layer consists of the people that are operating behind the network (Leitzel and Allard, 2016: 7). Evidently, deterrence strategies can find their way in all these layers. This is essentially different from the deterrence concepts in the conventional domains since none of them spans through all layers.

Consequently, to establish a relevant deterrence model in the cyber domain, it must be clear which actions need to be deterred. This constitutes the greatest difference between deterrence in the physical realms and the cyber domain. In conventional domains, deterrence is concentrated against physical attacks on individual resources or material targets that when attacked are not hard to attribute. On the other hand, deterrence in the cyber domain is focused on manipulating the elements within the domain, as well as the environment itself. This can be examined in three main approaches by grouping operations in the cyber domain into three categories - cyber-attacks, cyber espionage, and cyber theft. Cyber-attacks are clearly defined by their degrading, denying, and destructive acts. Espionage in cyberspace is what is known as stealing valuable information for intelligence gain. Lastly, theft is also a form of stealing valuable information, but mainly for financial purposes, sometimes without direct state participation. Attacks and espionage are mainly used by state actors, whereas theft is typically used by non-state actors.

Today, cyber-attacks are very common, and they can include the denial, degradation, or even destruction of both military and civilian communications systems. The most widely used and accessible example of is distributed denial of service attacks (DDoS). While DDoS attacks are usually treated as one of the less harmful types of cyber-attacks, they remain dangerous and can still challenge less developed governments. Such attacks have already been used against state actors like the US and its government ICT infrastructure, Estonia in 2007 and Georgia in 2008 (Klimburg, 2011: 49). So far, these attacks to the US or their critical digital infrastructure are not drawing enough debates on deterrence in the cyber domain. On the other hand, a grand jury in New York charged several Iranian hackers in absent for their alleged participation in DDoS attacks against US interests in the financial sector (Federal Bureau of Investigations, 2016). These indictments could not be considered as threats that needed to be denied by a deterrence strategy,

but more appropriately by relevant criminology policies. Since the Iranians were absent when they attacked, they cannot signal the attack or receiving deterrence signals. Such indictments enforce no real costs on Iran or the individuals who executed the attack since they are safe outside the US borders. These issues will be discussed further in the last part of the chapter, which will examine attribution in cyberspace.

Beyond DDoS attacks, actions in the cyber domain get more serious. An appropriate example is the Russian attacks against Ukrainian electric infrastructure. The attack is often viewed as the first effective cyber-attack on an electrical power grid that was able to jeopardize the command and control systems of several power distribution companies and briefly interrupt their supply to the Ukrainian citizens. (Zetter, 2016). In this case, the fusion between layers and domains is evident, since the alleged state-actors involved used the cyber domain to deploy their actions and the result was present in one of the conventional domains – land since these actions had physical or material consequences. This supposedly Russian actions resulted in a weak response that offered no indication for deterrence in cyberspace (Rid, 2016).

Another example involving non-material, but strategic consequences is the US 2016 elections, which again was blamed on the Russian Federation and defined as a mass-influence operation. The attack is largely considered as an information operation of the involved Internet Research Agency (Lapowsky, 2017). This agency created many social media accounts in different platforms claiming to be Americans that support radical political organizations, ultimately creating echo-chambers. Furthermore, general disinformation was spread by government-controlled media in Russia, while also being advertised in different social media platforms. Additionally, non-state actors affiliated with Russian military intelligence service (GRU) allegedly infiltrated the information systems of the Democratic National Committee (DNC), the Democratic Congressional Campaign Committee (DCCC), and campaign managers, publicly releasing stolen files and emails through WikiLeaks during the election campaign (Shear and Sanger, 2017). On the Russian side, several government representatives have repeatedly denied any participation in this operation. In response to these massive influence campaign supposedly committed by the Russian Federation against one of the major political candidates of the 2016 US Presidential election, the White House expelled several suspected intelligence agents and placed sanctions on

Russia's major intelligence agencies, the FSB and the GRU (Sanger, 2016). However, the costs imposed by the US were insignificant compared to the results accomplished by Russia.

These examples of nation-state actions provide case studies, regarding the difficulty to achieve deterrence in the cyber domain. Although there were signals of Russian disinformation actions, identified by the FBI as early as, a year before the election no significant preventive measures were taken on the US side (Lipton, et.al., 2016). In this case, the alleged Russian interference should be classified not as an attack, but rather an espionage act or theft, which does not fit in the conventional deterrence frameworks. Still, the effect of this disinformation campaign was significant, which is highlighted as a declassified report by the Office of the Director of National Intelligence. It concludes that these actions were information warfare in the form of an espionage campaign, which considerably hampered the DNC and partially damaged the reliability of the US electoral system (Office of the Director of National Intelligence, 2017). This underlines that cyber deterrence has been fundamentally challenged by the fact that sensitive information can be turned into a cyber weapon and used against the defender. Even in examples where specific malicious code is executed to achieve physical damage, there are is no legitimate strategy to signal threats within the cyber domain other than referring responses to physical actions. Consequently, it is safe to assume that deterrence concepts are still unclear, due to the lack of coherent and separate national strategy for cyber deterrence. Efforts through the abovementioned international initiatives from the first part, as well as the Tallinn Manuals by NATO, have outlined the framework in which cyber deterrence could fit in its legal aspects, yet there is still no evident application at present.

Operation Olympic Games is perhaps the most important case study in this part. This crown jewel of cyber-attacks, also known as Stuxnet, has demonstrated that a meticulous and well-designed cyber-attack can cause physical damage and circumvent a variety of protections, utilizing a precisely targeted point of interest and attack. Stuxnet is essentially a malicious worm, that can be separated into 3 distinct modules. The worm was responsible for executing the core commands of the attack, a file that is responsible for the spread of the malware, and a rootkit charged with avoiding detection by hiding any files and processes related to the malware (Veluz, 2010). It is designed very differently than other worms and malware in general. This is because it looks for a specific type of configuration boxes to be ticked to execute its primary function. If, however, this requirement is not met, it remains dormant in the system of the infected hardware and does not act

in any way. The primary target and condition of activating the malware is the presence of Siemens Step7 software used by Programmable logic controllers (PLCs). If that condition is met the worm executes the routines. The layered design that attacks multiple systems is also complex in another key element. It sends false sensor readings and imitates normal working conditions so to prevent any sort of termination due to the system detecting unusual readings suggesting a problem or abnormality (Broad, Markoff and Sanger, 2011). Stuxnet has allegedly been developed by the US and Israel and has been used to target Iranian facilities in order to prevent their nuclear program. It is revolutionary in the sense that it is the first and only known instance to date of a cyber-attack causing physical damages in the real world and arguably, achieving its goal. However successful in its purpose and widely believed to be revolutionary to what it means to cyberwarfare, J.R. Lindsay (2013: 392) argues that even though it was effective, it did not cause a severe effect and delay on Iran's nuclear program. Furthermore, he argues that contrary to initial beliefs, such well-designed and articulate cyber-attacks involve a substantial financial commitment that does not necessarily translate to the same amount of damages. He also suggests that the defender state may have to spend and develop significantly less in order to achieve deterrence by denial, which would result in substantial advantages for them in the event of cyberwar.

Overall, the concept of deterrence within the cyber domain is indeed difficult to achieve. That does not mean cyber-attacks are undeterrable. Most of them can function anonymously, which is another challenge for cyber deterrence (Brantly, 2016: 86). This anonymity hampers attribution and is often associated with the success of an attack, ensuring it bypasses deterrence by denial systems embedded in network infrastructures. On the other hand, deterrence by punishment could impact the cyber-persona layer as well, however, the next part will establish that other significant challenges are exceptional to cyberspace, which are coming from anonymity.

2.3: Non-state actors in the Cyber Domain.

Although nation-states seem to be the most logical actor to take cyberwarfare actions, recent accidents demonstrate that non-state actors may also play an important role, especially in low-intensive cyber conflicts. There are several variations of non-state actors, and this part will focus on explaining their role and their impact on the cyber domain. The previously mentioned state-

sponsored DDoS attacks in Estonia, were in fact partially conducted by non-state actors, since volunteers and mercenaries actively took part in the conflict. They represent a type of non-state actors for hire, that can act as a united cyber force, by joining efforts to purposely overload various network systems, including Estonian government services and commercial platforms (Ottis, 2010: 100-101). A more appropriate example could be ‘Anonymous’, which is another type, often called hackers, that claimed accountability for a few widely publicized cyber-attacks, including, DDoS, sensitive information leaks, and other similar activities associated with international security (Deibert et al., 2011: 129).

There are non-state actors that are primarily motivated by large economic gains. They can include malware writers and organized criminals in cyberspace, who have been relatively dynamic in recent years, according to Verizon (2012). Cyber-crimes, for example, can be various, including online harassment, identity theft, blackmailing, and extortion. Most of these crimes share the common goal of quick money advances and at least 80% of them are projected to originate in some sort of organized activity (Eshel, 2012). According to the same statistics, these organizations are mostly small in size, involving not more than 5 to 10 people, which are not structured strictly, as it is the case with organized crime gangs in the real world that are involved in illegal drugs for instance.

There is also a type of non-state actors in cyberspace, which have nationalistic tendencies and are also known as patriot hackers. They often aim their actions against foreign countries that are adversaries to their home country in support of domestic governments. Such groups have been active lately in numerous instances throughout the continuous conflicts in Kosovo. An appropriate example can be an organization of Serbian patriots, known as Black Hand, who attacked a Kosovo-Albanian website, threatening to jeopardize military computers of the involved NATO members (Denning, 2001: 241). The Kosovo conflict is categorized by Denning (2001:244), as the “the first Internet war”, although other conflicts have been categorized in the same way as well. Explicitly in the case of Kosovo, the label “Internet war” can be credited to the non-state actors involved in the conflict, given recognition to the wider role that is played by them.

Terrorism is also another type of non-state activity in cyberspace, which consists of terrorist organizations that use computers to execute cyber-attacks that can spread public fear in the pursuit of their political or religious goals. This topic has been debated during the last few years, especially

concerning the rise of Islamic fundamentalism in the Middle East. It could also be considered a rather emotionally charged subject, in which academic points of view have been alienated. Some counter-terrorism specialists claim that terrorism in the cyber domain is one of the most disturbing dangers in the 21st century (Thibodeau, 2014) (Morrison, 2012). Others suggest that such statements are mostly overstated, at the expense of more relevant cyber issues (Schneier, 2010).

All these types can be related in some way to what is generally known as hackers. Overall, non-state actors in the cyber domain can be summarized as people or groups with deep knowledge about computer technology willing to use it in their own interests. They are also usually looking to exploit delicate vulnerabilities of network infrastructures, and operating-system configurations. These malicious groups may be driven by different interests, like simple curiosity, quick financial gains, politics, or even simple boredom. The current classification of hacker groups is often done by their motivations, which is usually done by hat colour. According to their motives, they are categorized into black, white, and grey hats.

Black hats are the malicious category of people. They are the actors behind the exploitation of computer networks for their own advantage. These hackers are normally perceived as the most destructive non-state actors in the cyber domain, who act without any respect for the law or international regulations (Sigholm, 2013: 16). Such malicious individuals or groups may also act as mercenaries for states by carrying cyber-attacks on their behalf. This could further complicate the attribution problem for cyber deterrence since the victim state can easily attribute the attack to the non-state actor who conducted it, but it is almost impossible to attribute it to the state that ordered it.

White hats, on the other hand, are also known as ‘ethical’ hackers. They must possess high moral values, relative to commonly accepted norms. Often, their specialization is concentrated in ensuring the security of commercial ICT infrastructures and systems. People in this category are also commonly employed by government security agencies or by information security private companies. It is common for them to warn or consult big corporations about the vulnerabilities that they discover so that they could be patched.

Grey hats are people who often follow the narrative of their white hat colleagues. However, most of them may divert and occasionally break some of the rules. For instance, if people in this category

are targeted by a malicious cyber-attack, they might try to take the issue into their own hands, rather than report it to the relevant law-enforcing government bodies.

Overall, non-state actors in the cyber domain can play an important role, but also hardly ever cause more damage than state actors. Moreover, they could be employed as mercenaries in conducting offensive cyber actions in the name of an attacking state against another country. However, if non-state actors work on their own without government support, they could be easily identified and attributed guilt for their actions. Nonetheless, the next part will provide more clarity on the attribution process when it comes to state-actors in the cyber domain.

2.4: Attribution - How sure should a state be to attribute a cyber-attack?

Attribution is the act of identifying the source or cause of something. In other words, it is supposed to answer the questions of who did what. However, these questions present a huge problem, especially in the cyber domain. While anonymity has been one of the defining marks of the Internet, it is also the source of the issue with attribution in cyberspace. When attributing cyber-attacks, this anonymity grants an opportunity for adversaries to commit attacks without revealing their identity. Consequently, a state can deny responsibility to any cyber-attack, even if the victim state can point out the origin of the attack to the accused state. This is often referred to as plausible deniability, which makes the recognition of any involved actor very difficult.

Technology can aid victim states in attributing hostile cyber-attacks however, it is not enough to rely exclusively on it for credible attribution. This will be proven by examining the complex nature of the attribution process, by arguing that the threshold for attribution in cyberspace should involve not only the technology but also strategic and operational concepts.

In the context of International law, there are conventional frameworks related to attributing crime to the responsible actor. However, they are hardly applicable to cyberspace, due to its nature. The question of responsibility in the cyber domain is rarely decided by a single form of evidence. Lawful decisions are often based on accumulating direct or circumstantial evidence that can prove the responsibility of the malicious actor behind such conduct (Tran, 2018: 380). However, as it has been established in the first part of this chapter, the current state of international rules does not

offer appropriate regulation regarding cyberspace. The international community continues to work towards applying existing international laws and principles to cyberspace. This is because there are modern terms related to cyber-attacks that need appropriate definitions. One such term is the attribution threshold required for retaliation. For instance, according to Hill, the current DoD definition for 'cyber-attack' does not meet the threshold of an armed attack, which corresponds to International law, although it recognizes the malicious nature cyber-attacks (Hill, 2019: 4). In other words, this does not allow states the right to self-defence in cyberspace. Defining cyber operations as serious attacks is crucial because of the threshold required to meet such a definition. Seemingly similar in their intrusive nature, espionage, and attacks in the cyber domain are unique in definition, as it has been already established. Due to definition gaps and the irrelevancy of International laws regarding the cyber domain, adopting a universally accepted threshold for attribution remains difficult. This keeps the plausible deniability factor effective for adversary operations in cyberspace. Even if an attack could be attributed to a certain computer or network, through employing all aspects of the attribution process, a state can still deny any involvement or knowledge of the incident (Rid and Buchanan, 2014: 5). This is mainly because there is no specific binding international law or common understanding that determines how sure should a state be to attribute a cyber-attack to an adversary.

As the first part of this chapter concluded, International laws operate in cyberspace under previously established norms and principles, which are hardly transferable to the cyber domain. This alone hampers the process of attribution in many ways, especially in establishing a threshold. It also highlights the issue of applying the armed attack threshold principle in cyberspace when their definitions are ambiguous. For example, a cyber-attack that targets a certain power grid and manages to shut it down without causing any physical damage would not necessarily meet the established threshold for attribution. However, a bomb that accomplished the same would meet that threshold and provide the victim state with the ability to defend itself under International law (Hill, 2019: 13). Furthermore, the existing International laws do not address the non-physical effects that cyber-attacks may have and do not provide solutions to the effects that they may have over time (Dev, 2015: 386).

Another limitation is associated with technology and its use regarding the attribution of responsibility. The technical aspect of attribution is mainly limited by the structure of cyberspace.

Because of this structure, actors committing cyber-attacks can conceal the original source of the attack, as well as their identity (Margulies, 2015: 495). Still, the use of cyber forensics technology may allow victim states to attribute. However, there are circumstances in which technical aspects alone are not enough to identify the responsible actor. Provided that the Internet infrastructure allows malicious actors to mask their identity and evade responsibility for their actions, it is reasonable to assume that all aspects of the attribution process are necessary in order to attribute a malicious cyber-attack.

The attribution process embodies a distinct analytical challenge. Since there is a gap when relying solely on the technical aspects of attribution in cyberspace, it would be more plausible to rely on specific input data and expertise from not one, but three main fields – technological, strategic, and operational. Each of these analytical aspects needs to be communicated and approved by the other. There is no single methodology, since the operational and strategic teams may alarm the technical team, or vice-versa. The Stuxnet case is appropriate to showcase the amount of work required in such processes. This cyber-attack was so complex that several different companies were required to focus all their analytical teams on different aspects of the attack, such as the propagation mechanism, the command-and-control setup, or the payload targeting, to analyse the whole content of Stuxnet (Lindsay, 2013: 377). Moreover, analysing these aspects required different skills, which further complicated the process. Its goal often depends on the incurred damage. If a cyber-attack failed to cause any obvious damage, the victim state may choose to ignore it, or only partially investigate it, thus limiting the attribution process before it even begins.

Nevertheless, in the case of serious cyber-attacks, there are three main goals in the attribution process. The technical goal is to comprehend the incident in its technological aspects. The operational goal is to understand the architecture behind the attack, as well as the profile of the attacker. Finally, the strategic goal is to determine who is responsible for the attack, assessing aspects such as, motives, political significance, and deciding if a counter-attack response is necessary. This three-goal framework is proposed by Rid and Buchanan (2014: 12) and supports the argument that attribution is possible by involving all three aspects of the process. In this respect, the technical aspect generates digital evidence by cyber forensic investigation techniques. Furthermore, the operational aspect processes this data and figure out the scale of the attack. Lastly, the strategic aspect finalizes attribution, determining the aim of the attack and the responsible actor.

To put it in another way, the quality of this process is likely to grow as the amount of resources increases. An appropriate example could be found in one of the first recorded series of cyber-attacks called ‘Moonlight maze’ (Elkus, 2013: 152-163). The targets included several US governmental bodies. In response, the Joint Task Force Computer Network Defence (JTF-CND) was assigned to deal with the cyber-attack. The result of going beyond technical forensics was imminent. It allowed for the proper attribution of the cyber-attack to the Russian government with a high level of certainty. This example serves to indicate that effective attribution in the cyber domain is indeed possible. All three aspects of the attribution process – technical, operational, and strategic – should be utilized to a full extent, in order to achieve the desired assurance that meets the attribution threshold.

Overall, attribution is fundamental when it comes to identifying responsible actors in the cyber domain. Regarding cyber deterrence, several obstructions are present for taking the next steps to more secure cyberspace. From the lack of laws and definitions to network infrastructures, nations need to solve such problems in their own way, since they mainly emerge from the lack of international cooperation. A purely technical routine is unable to carefully identify and validate attribution. It is clear that attribution cannot be limited solely to technical operations nor it can rely on international law. On the contrary, the larger the pool of resources and skills implemented within the attribution process, the better the chances of uncovering adversaries. All this makes attribution a very complex, multi-layered process, rather than a simple problem. Although the attribution process was characterized as possible, it remains difficult to achieve, which is crucial for the conceptual framework, which will be proposed in the next chapter.

Chapter 3: Cyber Deterrence Strategy framework.

The following parts of this final chapter will aim at establishing a framework for cyber deterrence strategies. This framework will consist of deterrence concepts suitable for the cyber domain, which were derived from the research. The framework will highlight these concepts by explaining why they are included and how they could prevent warfare actions in cyberspace.

In order to draft such a framework, it is important to define what actions in the cyber domain could be considered as an act of war. Generally, cyberwarfare is defined as: “the use of technology to attack a nation, causing comparable harm to actual warfare” (Collier and Friedman, 2014: 65). However, there is a substantial discussion between academics and experts concerning this definition, where some scholars even claim that the term does not exist (Gartzke, 2013: 43). One way of interpretation is that this definition is inaccurate because there have been no offensive cyber actions yet to be labelled as ‘war’. Alternatively, it is argued that 'cyberwarfare' is an appropriate definition for attacks, which can cause physical damage objects in the real world, like Stuxnet. Since there are no publicly known examples of actions in cyberspace that have led to full-scale war, there is no single definition of cyber warfare. However, certain cyber-attacks could be considered an act of war by some states. Thus, it is up to those states crafting their cyber deterrence strategies to define in their own way, which cyber actions could be viewed as an act of war.

Offensive cyber actions, such as those mentioned in the previous chapter have taken place in the context of IR, resulting in hesitant criticism and reciprocal plausible deniability by the involved malicious actor. This brings back the challenge of cyber attribution, which has been established as solvable. It is certain that while states rely on using cyber actions and combined conventional capabilities, the probability of escalation to physical confrontation occurring in the real world as a result of cyber actions is increasing. Still, reaching causing conventional war through cyberspace is unlikely, because of its lengthy nature, thus ambiguity remains (Green, 2016: 89).

Considering more recent examples, the first example of conventional military forces deployed in retaliation to an offensive cyber action was observed in 2019, when the Israel Defence Forces responded to a cyber-attack from the terrorist organization Hamas (Liptak, 2019). The airstrike was directed towards destroying a building, which was related to a successful cyber-attack by Hamas. More importantly, the Israeli retaliation resulted in the loss of human life. Although Hamas is a non-state actor, which made attribution easier for the Israeli, it is clear how such offensive actions in cyberspace could escalate to a potential war. This example also provides some ground on what actions could be considered an act of war in cyberspace, since hypothetically if Hamas was a state actor in this case, there would almost certainly be a full-scale war between Israel and the ‘state’ of Hamas. Unfortunately, it is unclear what type of cyber-attack they used, as the Israel Defence Forces have not provided any further details about the nature of the alleged attack.

The first part of this chapter will focus on deterrence by denial concepts that can be implemented within the cyber domain. It will look at how states can use their military capabilities to deter warfare actions in cyberspace by acknowledging concepts from both, classical and contemporary deterrence theories.

Strategies and concepts involving signalling to adversary state that the costs of successfully conducting a cyber-attack are high and the likelihood of success are low will be examined in this part. This will demonstrate how states can rely on preventive measures that can deny potential adversaries. This part will also claim that deterrence by denial is favourable and unique for the cyber domain. It will contrast denial opportunities in the other conventional military domains, where the ability to manipulate their natural aspects is evident, while the same is not true regarding cyberspace.

The second part will look at concepts related to deterrence by threats and punishment, that are suitable for the cyber domain. It will examine how states use their assets to punish or threaten potential adversaries that are determined to conduct cyber warfare actions. This part will draw parallels between the classical concept of nuclear deterrence and contemporary concepts of deterrence by punishment to determine how they apply to cyberspace. This part will also claim that deterrence by punishment in the cyber domain is indeed possible, however, it is often not credible enough without having enough sustainable intelligence. It will also demonstrate how distinguishing the different types of cyber actions is difficult and regularly leads to miscalculations.

If the 'by punishment' and 'by denial' conceptual clusters are incapable of solving the problem of cyber deterrence, there must be other relevant answers. Although the principal discussion remains and there is no simple resolution, the third part will go beyond traditional cyber deterrence concepts seeking to provide further clarity to the conceptual framework. It will propose a cumulative deterrence approach that will combine offensive and defensive deterrence aspects from the previous two parts, aiming to improve the proposed framework. This approach will claim that deterrence is not a simple tool to be used by states to deter adversary behaviour whenever they want to. Rather, deterrence has always been a combined complex of efforts that encompasses conventional concepts of deterrence and progresses beyond them. This might consist of various

global agreements and technical practices, such as rules and norm development, new policies and laws, liability structures for software and hardware, and more.

The fourth part synthesizes the findings of the previous three parts, forming the conceptual framework for national cyber deterrence strategies. This will be the culmination part of the whole research, where the proposed framework will take its final shape. It will aim to implement the established concepts from the first chapter, considering the challenges from the second chapter and summarizing the results from the first three parts of the third chapter. It will indulge in each concept and explain how this framework would help to prevent warfare actions in the cyber domain. The final part of this chapter will provide limitations to this proposition.

3.1: Cyber Deterrence - By Denial.

Both deterrence concept groups established in the first chapter - by denial and by punishment - demand pre-attack costs by the defending state. The distribution of assets for deterrence by denial differs in direct proportion with the efficiency with which it can deter adversaries. As Riggs (2004: 126) argues, the establishment of good and reliable deterrence by denial systems in cyberspace ultimately begins with the distribution of finances. This translates into purchasing technical and human resources that are enough to periodically update, enhance, audit, and manage complex network infrastructures. Such systems can be network or host-based defences. They can include intrusion detection and prevention systems, anti-virus products, and other parallel mechanisms. These are some of the overlapping measures that could be taken to gradually make the intrusion of adversaries into state networks more challenging. In the cyber domain, these costs are generally overlooked, however, they are deterrent in nature. Although they are not as sophisticated as other deterrence methods, they substantially increase the level of protection and decrease the probability of penetration to government networks. These measures are comparable to the physical world since the same kind of deterrence tactics can be employed by retail stores that place tracking chips on their products and detectors at doors. This denial strategy is designed to warn adversaries that the costs of a successful attack are high, and the probability of success is low, whether it refers to the cyber or the physical world. This highlights how the already established deterrence by denial concepts are, already as applicable in cyberspace as they are in the real world.

This is noticeable, especially since most cyber-attacks are in fact, unsuccessful due to the effective denial systems in place. The US Department of Defence absorbs millions of attack attempts per day, even though nearly 99.99% of them are unsuccessful (Howard and Cruz, 2017). Moreover, since the quantity of cyber-attacks is increasing exponentially, the United States has restructured and upgraded the better part of its network infrastructure to imply more sophisticated denial systems. This often allows the initial point of contact between the defending state and the adversaries to be chosen by the defending state. In military terms, it allows defenders to choose the terrain of battle. While this does not prevent the need for other deterrence concepts, it signals the increased cost imposition on adversaries and it allows for more efficient resource allocation and defence.

Unlike in any other conventional military domain, the opportunities for deterrence by denial in the cyber domain can be described as substantial and exceptional. While denial in land, sea, air, and even space is based on the control of a certain geo-dimensions, states relying on deterrence by denial can only partially alter the nature of the domains themselves. However, this cannot be true within the cyber domain. This is because every aspect of cyberspace can be manipulated by both, the defending and the attacking state. Everything from the network structure, to the hardware, firmware, and software, as well as access control of individuals, can be attacked and defended at any time. Typically, at all stages of cyber-attacks, the adversary is always trying to control the defender's network, over which it has limited perceptibility (Brantly, 2018: 48). This perfectly illustrates how cyberspace is indeed a battlefield with every aspect of the attacking and defending phases, which should be a subject of deterrence, no matter how complex it might be.

For 'by denial' strategies, some of the classical concepts of deterrence theory remains relevant. Generally, the two stages emphasizing on rational game theory and cognitive modelling are foundational. While in contemporary deterrence concepts the focus is pointed towards deterrence by punishment strategies, some of the modelling methods find their place in the deterrence by denial group. Though the theories may be similar, there are differences, such as the payoffs in cyberspace, which can be manipulated and often favour the defender. In fact, there are only a few other applications of deterrence by denial strategies, where the payoff conditions are that favourable to the defender. However, the capability to manipulate the potential payoff for attackers remains difficult. Although it is evident that using deterrence by denial strategies in cyberspace

can decrease the likelihood of successful attacks, the possible consequences can remain large, depending on their scale.

In this respect, some cyber-attacks are simply too costly and cannot be prevented by deterrence by denial strategies. For example, minimizing consequences from attacks on data sources entails the assimilation of this data. This kind of denial instruments introduces effectiveness for a large financial price. Consequently, although denial strategies offer a substantial capability for credible deterrence in the cyber domain, it does not solve the cyber deterrence problem singlehandedly. Denial systems can, in fact, reduce the prospect of successful attacks and are more likely to deal with low-class cyber-attacks by non-state or small state actors. Despite efforts to signal deterrence credibility through purchasing and implementing different denial systems, together with restructuring of network infrastructures, the cyber deterrence problem is still evident.

Perhaps the strategy of deterrence by denial might be a way for smaller, less developed countries that are eager to defend themselves and deter attacks within the cyber domain. Although it might be a quite big investment to make for a smaller country, implementing denial systems within the most crucial government networks is a convenient option to deter at least some cyber-attacks. It could be argued that if Estonia in 2007 and Georgia in 2008 have implemented such systems, they would have been less vulnerable to cyber-attacks, especially less sophisticated ones, like DDoS. Then again, this deterrence by denial strategy would only deter the low-level cyber-attacks. For more complex attacks in the cyber domain, such as those sponsored or directly conducted by advanced state actors, like Stuxnet, this strategy is only the first layer of protection and does not guarantee deterrence.

In this respect, it is evident how some of the classical deterrence concepts relevant to nuclear deterrence cannot be functional due to the nature of the cyber domain. One such unsuitable concept is that deterrence must not fail in any way in order to preserve peace. This can be observed in the Estonia case, where deterrence failed to prevent the allegedly Russian cyber-attacks, though these actions did not lead to a full-scale war between Russia and Estonia. Furthermore, other key classical deterrence concepts, like Mutual Assured Destruction also appear to be irrelevant to the cyber domain. This can be confirmed by the Stuxnet example, where deterrence by denial failed, and the attack on critical nuclear infrastructure did not lead to a devastating war between Iran and the United States, despite the physical damage that was caused. However, other classical concepts

can fit into a conceptual cyber deterrence framework. One example is the notion that less force may possess deterrent value. This is indeed relevant, since denial strategies, although expensive, typically require little effort. In return, they may provide enough deterrence value, especially against low-level threats, as it has been established in this part. Additionally, this also verifies another similar classical deterrence concept, which states that inferior forces to their rivals might have some deterrent value. This supports the argument that denial strategies in cyberspace may work on their own for smaller countries, having some deterrence value, although it might be limited to deal only with low-level cyber-attacks that are not hard to attribute.

As it comes to contemporary deterrence, there are also some applicable concepts with the potential to fit in a potential cyber deterrence framework. Notions, such as minimal deterrence are reciprocal to deterrence by denial strategies that concentrate on defensive systems. It could also be argued that relying on the concept of minimal deterrence ensures less need for deterrence in the other four military warfare domains of land, air, water, and space. However, it also reinforces the cyber domain, which is the most unregulated and potentially dangerous of all military domains, thus mutual deterrence could only be effective based on international cooperation.

Since cyberspace can serve to connect all other conventional domains of warfare, as it is man-made and can play a role in all other types of military operations, it is safe to assume that some contemporary deterrence concepts have a place in the conceptual framework. Partial deterrence in cyberspace can be achieved not only in defensive ways, like denial strategies but also in offensive ways, such as deterrence by punishment or fear of consequences. An appropriate example might be if a defending nation holds an extensive range of cyber weapons and other interconnected capabilities. This can guarantee at least some deterrence value, since other adversary nations that want to attack might not be so keen on advancing, based on their fear of punishment from these capabilities. These strategies will be further examined in the following part.

3.2: Cyber Deterrence – By Punishment

Another way of potentially achieving deterrence in cyberspace can be by punishing an adversary action in a way that ensures the attack will not re-occur in the future. This notion was examined in

the first chapter, where it was demonstrated how contemporary deterrence strategies can rely on punishment. The second chapter established the challenges of how cyber-attacks work and how they could be used as punishment in examples of damage done to physical infrastructure as a result of a cyber-attack. If deterrence by punishment strategy is applied to the nuclear age deterrence, retaliating a nuclear attack on a major city, for example, the only proportional response would be a nuclear counterattack on an adversary city. In this case, both cities are physically static and immobile. The same type of punishment strategy through retaliation has mostly transferred to contemporary deterrence practices in the other four conventional warfare domains. This is because it is indeed plausible and technically achievable to apply deterrence by punishment using ballistic missiles or airstrikes, instead of nuclear weapons. However, the same logic does not hold in cyberspace. This sort of deterrence based on retaliation or other forms of punishment is not as simple when applied to the cyber domain, as when it is applied to land, sea, air, water, and even space, due to several reasons.

Firstly, the state seeking to deter through punishment needs to have a solid proof that identifies the one who committed an adversary cyber action. The potential for deterrence by retaliation or other punishment always depends on credible attribution, as it was established in the second chapter. Although it was defined as achievable, retaliation that does not possess strong and attributing proofs is likely to misidentify the target and provoke redundant escalation.

Secondly, if a state wants to apply deterrence by punishment strategy, it must retaliate within a proximate time-based frame. In case that the attacked state cannot rely on comprehensive intelligence on the assets it wishes to retaliate against, developing it, together with a cyber weapon deployable against the adversary, increases the timeframe of the punishment. This delay might be in several days, weeks, months, or even years away from the initial attack for which the attacked state wishes to retaliate. Due to this chronological disconnection, the threat of punishment in response to an adversary cyber action falls into a category of what Brantly (2018: 45) refers to as 'hyperbolic discounting'. This means the risk of applying punishment for a cyber-attack can be so chronologically distant, that the retaliation is reduced to the point of irrelevance. In such cases, the retaliation can be considered as a separate attack from the original one by the adversary who stroked first.

Thirdly, deterrence by punishment requires proportionality, which is one of the fundamental concepts of deterrence, examined in the first chapter. It is essential to have equivalent assets to punish in order to prevent unnecessary escalation or violation of international law, as per the Tallinn Manual (Schmitt, 2017), noted in the second chapter. Comparable assets are not inclined within the cyber domain and are often difficult to identify (Libicki, 2016: 262). To apply deterrence by punishment against an adversary asset within the cyber domain, a state would need pre-established access or further information that goes beyond its geographical location. It is incomparable with deterrence by punishment in conventional military domains because a city, for example, cannot be moved and it is likely to be as vulnerable to conventional military attacks now, as it will be in the foreseeable future. As it comes to the cyber domain, however, a computer system that is recently compromised might be patched, upgraded, or taken offline in seconds, which would prevent accurate retaliation.

Finally, the state wishing to rely on deterrence by punishment must have a cyber weapon, often personalized to retaliate against a specific target. If the attacked state warns its adversary that will strike to punish an attack or the same retaliator directly deploys a cyber weapon repeatedly to attack the adversary state's systems, the whole operation could be ineffective. This is because deterrence by denial strategies of the adversary state might be credible enough to prevent the retaliator's cyber-attacks. The longer the state wishing to punish deploys cyber-attacks, the more likely it is that the adversary state updates its denial defence systems. Hence, if the attacked state wishes to punish the adversary state successfully, it must have a prior deep understanding of its characteristics and intelligence of the assets it wishes to retaliate against. The retaliator state needs also to find new exploits in order to accomplish their desired outcome or be assured that the adversary has not updated or patched their previously known vulnerabilities.

Altogether, some of the challenges regarding deterrence by punishment strategies in the cyber domain are related to signalling, whether the battle is limited within the domain or crosses over the other four conventional domains. Quick attribution is of foremost importance to credible punishment against an adversary, assuming the availability of proportional assets, as well as reliable intelligence about their features. As it was established in the second chapter, attribution in cyberspace is typically not a simple, fast-paced process, especially regarding state-actor cyber-attacks. Moreover, this challenge does not refer only to retaliation in cyberspace. Since

proportional target selection might be slightly easier in cross-domain retaliation, the first three reasons addressed above are still applicable.

As it seems that bot, deterrence by punishment, and by denial operate within the same time-based frames. Yet, attribution is only crucial for deterrence by punishment strategies, while on the other hand, it is generally not important for ‘by denial’ strategies. In their initial phases, both denial and punishment strategies emphasize on pre-attack means of deterrence, yet deterrence by punishment strategies essentially requires an after-attack attribution process as well. Based on the technical realities of the cyber domain and IR, deterrence by punishment is arguably more complex and harder to successfully achieve, than deterrence by denial.

Furthermore, in the case of deterrence by punishment, it could be argued that it illustrates the classical concept of pre-emptive strike. Undeniably, the cyber domain remains under the technological dominance of its offensive aspects, which could also lead to reinstalling the strike first conceptual approach of classical deterrence. Evidently, due to the rationality and affordability of cyber-attacks, concepts like pre-emptive strikes in the cyber domain are the only feasible option for deterrence by punishment. It has been debated in the first chapter whether the classical deterrence concepts are appropriate for the cyber domain or a new equivalent is needed. In principle, the core classical concept of deterrence by retaliation is complicated by the problem of attribution, as it has been established. On the other hand, other classical deterrence by punishment concepts, like pre-emptive strike, given that it is supported by reliable intelligence, might as well work in cyberspace.

Alternatively, the previously mentioned classical deterrence concept of ‘strike first’, which is self-explanatory, could also be viable for the cyber domain. Of course, this concept hardly ever achieves any efficiency, although it could cause another form of deterrence strategy, which relies on the fear of further consequences. This strategy is fully dependable on offensive means and without appropriate reasons, it could violate international law. It mostly refers to cyber operations, when the state wishing to impose deterrence by fear of consequences strikes first against its adversary to showcase its cyber capabilities and that it would be unwise to retaliate against their power in the cyber domain. This strategy is highly dangerous because it could cause unnecessary escalations and breaking of international regulations. Stuxnet is a prime example of such kind of operations, where the cyber-attack was not retaliation against the previous attack, but an

undercover ‘strike first’ attempt to stop Iran from acquiring a nuclear weapon. As it was established in the second chapter, the attack failed to accomplish its purpose, no matter that it managed to cause physical damage. On the other hand, this will remain in history as the first recorded cyber-attack that managed to inflict direct damage from the cyber domain to the real world. It might have some deterrence value since it could be considered as a showcase of cyber capabilities to the rest of the world with the intention to achieve deterrence by fear of consequences. The fact that cyber-attacks against the main actors behind Stuxnet is increasing (Abdollah, 2019), indicates that deterrence by fear of consequences credibility remains debatable.

Overall, using deterrence by punishment concepts in the cyber domain is indeed possible. However, it cannot be relied solely on this kind of deterrence strategy, since it is not a consistent or credible option under most circumstances, especially if states cannot rely on credible intelligence. This assessment is derived from analysing classical and contemporary deterrence concepts in the first chapter. It is also supported by many scholars, such as Valeriano and Maness (2015: 57-60), who argue that deterrence by punishment is mostly unproductive and often causes additional danger if used alone than other means of deterrence. Furthermore, having reliable intelligence about adversary systems can create its own separate issues, such as cyber espionage, which includes a security dilemma (Buchanan, 2017: 124). The more states engage in such highly offensive practices through the cyber domain, the more their actions are likely to be misunderstood and thus, cause unnecessary escalation and deterrence failures. The same refers to the deterrence by fear of consequences, since both are founded on the offensive nature of cyberspace.

3.3: Cyber Deterrence: Cumulative.

The cumulative approach to cyber deterrence can be considered a combination of deterrence by denial and punishment, with emphasis on fear of consequence. In other words, this strategy aims to combine concepts from the above-studied clusters, by underlining the offensive nature of the cyber domain. As it has been established in the first chapter, the western model of deterrence theory was created through methodical efforts by strategic scholars, which rendered strategy into a practical decision-making tool. The cumulative approach, however, is based on Israel’s view of deterrence, which has not been systematically developed as a theoretical framework. Instead, Israel

developed a deterrence posture that could be defined as “strategic common practice” (Bar-Joseph, 1998: 147-148). These common practices of deterrence oppose the widely accepted Western model of absolute deterrence, by advocating that building deterrence concept that can limit and shape the behaviour of adversaries is more efficient than to prevent all attacks.

The Israeli context of deterrence is obviously offensive, based on their common practice from large-scale conventional wars in the 20th century, that prevented coordinated invasion from neighbouring countries, as well as a continuous risk posed by non-state actors (Tor, 2015: 102). Nevertheless, in the past two decades, the Israeli view of deterrence evolved to a clearer and more extensive theoretical foundation. One of the conceptual groups that could fit in the proposed framework was established in this context, namely the cumulative deterrence. According to Almog (2004), Israel achieved deterrence in the conventional military domains using threats and military force over an extended period of conflict. In his view, cumulative deterrence seeks to achieve its goal in two main ways. The first way is to rely on establishing military supremacy in cyberspace, and the second is to rely on high-class military retaliation assets against foreign threats. Following the logic of the cumulative deterrence, it needs to be recharged every now and again, in order to preserve the image of supremacy it aims to create. This could be achieved through a sequence of small triumphs, achieved over extended periods of conflict, which should provoke a more restrained behaviour of the adversary, hence achieving the goal of the strategy.

This could be an appropriate concept to add to the cyber deterrence framework if it could be properly applied to cyberspace. For instance, the concept of replacing the classical deterrence perspective of absolute deterrence with the concept of cumulative deterrence is suitable, since it offers an alternative approach to the cyber deterrence problem. What is more, this approach often engages in brief showcases of power, in order to control the scope of a conflict, which according to Tor (2015) is more appropriate for cyberspace, due to its offensive nature. This corresponds with the aim of cumulative deterrence to limit and control the behaviour of adversaries, rather than relying on absolute deterrence that prevents all attacks, which makes the cumulative concept a suitable approach for deterrence in the cyber domain.

Other concepts of the cumulative deterrence strategy could indeed be adapted to the conceptual framework for cyber deterrence if they are applied properly. For example, this strategy can help establish a clear and coherent strategic message regarding what is unacceptable behaviour in the

cyber domain. Due to its offensive approach, cumulative deterrence can be useful to create norms for the strategic environment of cyberspace. This would require a thorough consideration of the adversary's strategic narrative, along with other factors, but if successful, it would provide a distinct way of sending deterrence signals and determining the 'red lines' in cyberspace. This alone could solve the 'rules and norms' problem in the cyber domain, which was established in the previous chapters.

Another principle of cumulative deterrence suitable for cyberspace is the capability and willingness to carry out small-scale cyber-attacks against opponents, intending to establish a position that asserts the deterring nation's national interests in the cyber domain. For this to be effective, these interests must be clearly defined and consistent. Other measures outside cyberspace, such as economic or diplomatic sanctions are also relevant. This would re-affirm deterrence credibility and demonstrate the deterring nation's willingness to act over an extended period.

Having established a credible posture through a cumulative deterrence strategy, the next step would be to achieve overwhelming supremacy in the cyber domain. One of the most important aspects of this strategy is to make the adversary believe that even if they try to carry out a cyber-attack, winning is not a genuine option due to the overwhelming capabilities of the deterring state in the cyber domain. Attaining supremacy should always include maintaining credible intelligence, together with possessing cutting edge offensive cyber capabilities. By achieving such status, it would not be hard to realize the aim of cumulative deterrence to accumulate multiple victories, which should progressively produce more restrained behaviour of the adversary. On the other hand, although this concept is suitable for asymmetrical conflict against most state and non-state actors, it is unclear how efficient it would be against other supremacy states, such as Russia or China.

Finally, making the attack difficult and more costly for the adversary is deterrence by denial concept, which is also a key part of the cumulative strategy. It defines building robust and well-protected network infrastructure as essential for cyber deterrence. This should take place through monitoring the continuous advancements in technology and applying vanguard defence systems to achieve a successful cumulative deterrence. This concept unites punishment, and fear of

consequence strategies with denial components, making it seem like an appropriate combination for the cyber deterrence framework.

As it comes to challenges, some of these studied in chapter 2 also apply to cumulative deterrence. In the case of deterrence by punishment and by denial, which are substantial parts of the cumulative strategy, most studies critique these concepts and some even claim that they are unsuitable for the cyber domain. They often point out the problem of attribution (Morgan, 2010: 65). Studies also suggest that cyber deterrence has limited value since the domain is unable to rely solely on deterrence by denial (Morgan, 2010: 67). The analysis of this research demonstrated how these two claims are not sustained, since although hard to achieve, the problem of attribution was established as solvable in the second chapter. What is more, cyber deterrence by denial is also considered possible, especially for smaller states and against non-state actors, as it has been shown in the second part of this chapter.

Firm critics of the ‘by denial’ strategy go as far as claiming that deterrence by denial is not well established and does not, in fact, differentiate from simple defence measures. Contrary, scholars like Paul, Morgan, and Wirtz (2009: 2) provide a proper definition of deterrence by denial, which usually refers to denying the enemy the benefits of a certain aggressive act or strategy. At any rate, regardless of the provided solid definition of this deterrence concept, publications are claiming that the deterrence by denial in cyberspace remains limited. They point out that this is due to the fast-paced progress of weapons in the cyber domain, as well as the rapid expansion of operational knowledge through the open-source dimensions of the domain (Liff, 2012). Despite their logical appeal, these statements are often not maintained by credible empirical evidence and only serve to exaggerate the case against cyber deterrence in general and deterrence by denial in particular. This is accurate especially regarding the current context of high-value strategic targets. This is because they are limited in number and are also typically air-gapped or rely on highly encrypted digital gateways, which makes defence easier, more cost-effective, and thus more promising (Lindsay, 2013: 373). Consequently, any deterrence strategy in the cyber domain is expected to benefit from integrating improved and robust denial systems, especially in combination with concepts from the deterrence by denial and by fear of consequence clusters.

Overall, cumulative deterrence offers a unique approach that adds valuable concepts to the framework for cyber deterrence strategies. Undeniably, this chapter claimed that there is a strategic

insufficiency in the cyber domain, particularly regarding deterrence. It was established that cyber deterrence as a strategic instrument evolves slowly in theoretical and practical terms, mostly due to an outdated theoretical framework that has borrowed its basics from the classical concept of absolute deterrence, which was relevant for the nuclear age, but fails to suffice in the 21st century. The next part will propose a framework for national cyber deterrence strategies, based on classical, contemporary, and cumulative deterrence concepts, as well as the findings of the research, considering the above-studied challenges.

3.4: Conceptual Framework for National Cyber Deterrence Strategies.

Deterrence in its Cold War form was developed with the main purpose of regulating a type of international relations that has now been set aside and is irrelevant for the 21st century. In that respect, some of the key classical deterrence concepts, such as absolute deterrence, have little significance today. At present, the cyber deterrence issue is rather different, both in scale and in nature. Hence, most concepts from the nuclear age can only serve as negative lessons on why it cannot be applied or why it should be avoided. However, there is one crucial lesson from that period that must be implemented in future cyber deterrence strategies. That is the concept of cooperative security, which should be applied to an even greater extent today in pursuing internationally accepted rules and norms since the interdependence embodied in the cyber domain is much greater. Cyber-attacks do not represent the threat of overthrowing world order in a massively destructive war. They are rather a representation of advanced technology development to some central features of that order. Thus, they are a less obscure, and more penetrating danger. In order to prevent such threats from occurring, states must develop separate national cyber deterrence strategies that eventually consists of the following compulsory concepts:

- **Deterrence by denial: For detection and immediate response to cyber-intrusions.**

The thesis has already established that even a short delay in detecting an attack in the cyber domain can be fatal regarding an appropriate response to it. Hence, every cyber deterrence strategy must begin with acquiring denial defence systems that can immediately deliver detection, prevention, and possibly mitigation services on the damage done. This can be provided by Intrusion detection and prevention software (IDPS), security information and event management systems (SIEM), and

other measures studied in detail above. Such systems can be programmed with specific security policies and sets of rules, that must be crafted by the state wishing to implement them. Ensuring a credible defence system can deter an adversary by totally denying the possibility or at least increasing the cost of a successful cyber-attacking. Thus, deterrence by denial is a vital concept in this framework, since there are billions of attacks in the cyber domain happening every day. Most of these cyber-attacks are not much sophisticated and often originate from motivations of non-state actors or states with low cyber capabilities, hence making them deniable by these systems.

- **Advanced denial systems: For robust defence and network infrastructure.**

Such systems on an advanced level are required if states want to improve their cyber deterrence strategies to undertake persistent cyber threats coming from state-actors with credible cyber capabilities. Such threats can be more serious, more intrusive, and more elaborately crafted cyber-attacks, that could potentially cause physical damages to critical infrastructures. Such defences are vital for meaningful deterrence by denial against adversaries because they serve as the first point of contact between the defending state and the adversary. The main issue often resides in the fact that network infrastructures are outdated, which allows the attackers to keep on looking for vulnerabilities. This is often not costly, since morally old network infrastructures, do not provide major backup when a defence system is penetrated. Hence, restructuring and updating the state network infrastructure should solve this problem, or at least minimize the potential damage from cyber-attacks. Moreover, advanced denial systems should be applied to the new infrastructure further fortifying the state defences. Although this whole process is very expensive and hard to achieve by all states, it signals credibility to adversaries and often serves to deter even higher-class cyber-attacks from state-actors. While this does not prevent the need for other deterrence measures, it takes place as another necessary concept for states wishing to craft their national cyber deterrence strategy.

- **Offensive cyber capacities: For credible deterrence by punishment.**

Moving on from the defensive narrative, if states want to retaliate against an adversarial cyber-attack, aiming to ensure that adversaries would not dare to attack again, they should include deterrence by punishment concepts in their cyber deterrence strategy. Such retaliation might include cross-domain operations that inflict several forms of damage in the cyber domain, as well as the other four conventional military domains. Moreover, economic, political, and diplomatic

sanctions might also be part of the retaliatory efforts, together with moves to provide public evidence that identifies the attackers, seeking international assistance and media pressure on them. Possessing evidence of who is behind the cyber-attack is a crucial characteristic of the deterrence by punishment concept. The credibility of this deterrence concept mostly depends on reliable attribution, which clarifies why the attack has occurred, who is behind it, and what type it is. Although attribution was defined as difficult but possible to achieve, retaliation that cannot rely on strong attribution is likely to cause a perplex and redundant escalation, possibly against the wrong target. Credible deterrence by punishment also requires states to have comprehensive intelligence, as well as proportionate cyber capabilities to retaliate against the adversary. Overall, retaliation should inflict as much damage as needed to deter another similar attack from reoccurring, which forces states that wish to implement this concept to their cyber deterrence strategy to depend on solid credibility for successful deterrence by punishment.

- **Advanced offensive cyber capabilities: For credible deterrence by fear of consequence.**

This concept is completely offensive in nature, as it aims to deter by aggression, relying on advanced cyber capabilities. States that wish to use this concept in their national cyber deterrence strategy should ensure their ability to execute high-end cyber-attacks that are similar to or better than Stuxnet in sophistication and level of competence. This concept typically requires the deterring state to strike first against its enemies, with the main purpose of demonstrating its powerful cyber capabilities. This aims to signal that it would be inappropriate for the attacked state or any other state-actor to retaliate against the deterring state's cyber assets. This deterrence concept is highly dangerous, as it could cause unnecessary escalations, as well as the breaking of international rules. Hence, it can only be credible on its own if the state that wishes to implement it in its cyber deterrence strategy can afford the risk of suffering international sanctions and has the benefit of advanced offensive cyber capabilities.

- **Cumulative deterrence: For combining the above concepts, seeking cyber supremacy.**

This set of cumulative concepts should be perceived as a combination of relevant deterrence by denial and punishment conceptions, that emphasize on fear of consequence. Particularly, it aims to make use of concepts from the examined clusters by embracing the offensive nature of cyberspace. Any state that wishes to rely on the cumulative deterrence concept must know that it shapes the behaviour of adversaries by demonstrating advanced offensive capabilities.

Nevertheless, it also recognizes the significance of deterrence by denial systems, which are necessary for ensuring a credible cyber deterrence strategy. In other words, states that employ cumulative deterrence to their cyber deterrence strategies could achieve control over adversary behaviour through retaliatory cyber-attacks, only if they are always supported by credible denial capabilities. The next step of this concept resembles deterrence by fear of consequence. It is based on achieving cyber supremacy, since, cumulative deterrence aims to make the adversary believe that the deterring state is untouchable in the cyber domain. Following the offensive concepts, reaching the state of supremacy should include reliable intelligence, as well as high-end offensive and defensive cyber capabilities. By achieving the status of cyber supremacy, adversary behaviour towards the deterring state should become more moderate. As it seems, this concept can deal with asymmetrical cyberwarfare actions coming from both, state and non-state actors. Nevertheless, it is uncertain how effective it would be against other cyber supremacy states, such as Russia, China, or the US. Overall, cumulative deterrence unites most of the appropriate concepts of punishment and fear of consequence, with denial components, making it highly functional for national cyber deterrence strategies.

• **Active international collaboration: For establishing rules and norms in the cyber domain.**

This concept is the most difficult one to achieve since it depends mostly on international collaboration. It aims to establish internationally accepted rules and norms for the cyber domain, which would require long and hard work by the whole international community. Still, the universality of the cyber deterrence issue and its growing international significance must be addressed in future strategies. Establishing rules and norms would require global combined efforts to considerably reorder the cyber domain. These could include agreeing on regulations that work in favour of preserving the peace, as well as creating new international organizations and networks to oversee, manage, and supervise cyberspace. Having in mind the few failed attempts to draft globally accepted rules, national deterrence strategies should call for more cooperation, but also more control and less freedom of action, as well as less tolerance for reckless behaviour that could lead to an escalation of tension in the cyber domain.

Clearly, the proposed framework for national cyber deterrence strategies consists of the most important classical and contemporary deterrence concepts established in the main body. Having a more abstract overview is also possible in the content tables, located in the appendices. It is evident

that fractions of both, classical and contemporary deterrence concepts found their way to remain relevant for the cyber deterrence conceptual framework.

For deterrence by denial, these are predominantly concepts that emphasize on rational game-theoretic and cognitive modelling, as noted in the first chapter, since deterrence by denial, requires little effort to implement. Furthermore, denial in cyberspace resembles the strategy of containment, as well as the concept that inferior forces to their rivals are also able to deter some attacks. The contemporary concept of minimal deterrence would also be feasible for the cyber domain, given that internationally accepted norms and rules are achieved. The same is also valid for concepts of deterrence by punishment and by fear of consequence in cyberspace. The framework can provide only guidelines for the establishment of a national cyber deterrence strategy and acknowledges that it is not universally applicable. This will be further demonstrated in the next part, which will provide limitations to the proposed conceptual framework.

3.5: Limitations.

The proposed framework for national cyber deterrence strategies is far from perfect, and it should be examined more broadly to further determine its applicability in the domain. This is because deterrence in cyberspace is inevitably incomplete, although success in limiting hostile adversary behaviour is achievable. In the projected form, the conceptual framework remains only one of the several alternatives for cyber deterrence solutions, which should be further developed as a model by the states that wish to craft their own national cyber deterrence strategies. Morgan (2010: 51) describes this seamlessly, stating that: “essentially, all models are wrong, but some are useful”. This relates to the proposed framework since it could not solve the cyber deterrence problem on its own, but it could help prevent warfare actions in the cyber domain.

One way it could be useful is that the combined concepts can be applied together or separately, depending on the needs of the country that wants to use them. Ideally, the conceptual framework should work in the best way if it is applied as a whole, but in some cases, this could not be possible. For example, some less developed states could find it difficult to rely on advanced deterrence by denial systems, since developing the required defensive cyber capabilities could be very expensive. On the other hand, building offensive capabilities to rely on deterrence by punishment in

cyberspace could be technically challenging for some states to accomplish. What is more, cumulative deterrence is only relevant for advanced states, since it could be difficult to implement, provided it maintains aspects from both, deterrence by denial and by punishment.

One other limitation of the proposed framework is that it does not deal with the dilemma of how to handle relations with rivals, as it focuses on deterring adversaries. In other words, it could be argued that the US, for example, will have a different approach to dealing with Iran's undesirable behaviour in cyberspace, compared to unwanted actions conducted by China.

Another important element that limits the proposed framework is that it does not consider how to behave towards attacks on the private sector. It proposes certain solutions and indulges in deterrence theory, acknowledging what is relevant for states. However, it does not reflect on the fact that it is possible to retaliate against an attack on critical national infrastructure, but it is very difficult for key private companies, such as banks, high-tech companies, or media corporations to defend themselves against attacks, due to their limited capabilities.

This thesis offers an opening basis for a future discussion of these limitations. Without a doubt, the conceptual framework and the solid basis of how states should deter attacks in the cyber domain could be useful. For instance, it could be beneficial for forthcoming discussions on how to deter attacks on the private sector, or how to deal with unwanted rival behaviour in cyberspace. What is more, the proposed framework in this form could serve as a cornerstone for other, more advanced and detailed, conceptual frameworks for national cyber deterrence strategies. Overall, this part acknowledged some of the possible limitations of the thesis and proposed topics for some further discussion.

Conclusion.

The massive leap in technology marking the 21st century led not only to a revolution in everyday life and all aspects of public service but also created an entirely new military domain. With that emergence also comes the challenge of cyber deterrence and the role this domain will play regarding itself and the other conventional military domains. The role of cyberspace is crucial, not only for its individual narrative but also because of how interconnected it is with the rest of the

conventional domains. It is also challenging because of the constant innovation and advancements in the field of technology. This thesis offered a conceptual framework for national cyber deterrence strategies, to prevent warfare actions in cyberspace.

In the first part, classical and contemporary deterrence concepts were examined and grouped by how they function. Furthermore, there was a focus on how they have changed from the nuclear age to their contemporary state. It was also established how those concepts differ from current ones and how they can be applied to the cyber domain. The efficiency of classical deterrence concepts, when incorporated into the conceptual framework for national cyber deterrence strategies, was proven to be limited, but possible. It was vital to draw a line between deterrence in general and cyber deterrence, as the cyber domain has substantial specifics that are unique and have no parallel in the other conventional domains. This is partly the reason Cold War deterrence concepts have failed to fully transition to the cyber domain.

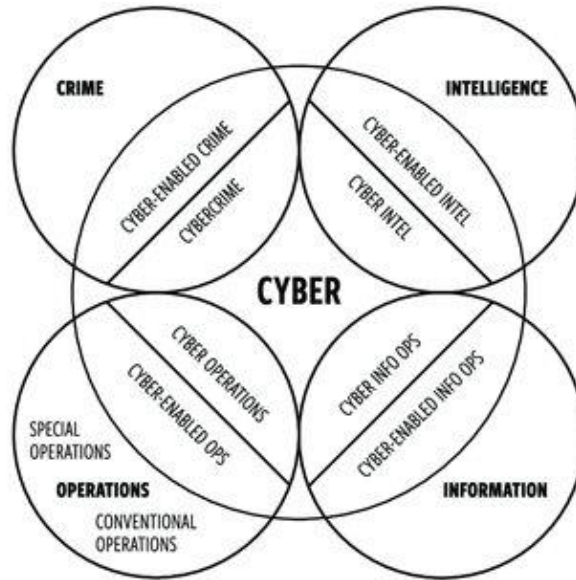
Cyber deterrence faces distinct challenges that are studied in the second chapter. Non-state actors are one such hurdle, as they do not abide by international laws. However, they are not seen as a significant threat, since they have fewer capabilities and larger budgetary restrictions, which in turn makes them easier to deter. Another important characteristic is that they are less challenging to identify, however, attribution in the cyber domain is generally more difficult, because of the anonymity embedded into cyberspace. Thus, very advanced and capable state-actors are very difficult to pinpoint and attribute guilt for their actions. Creating international initiatives has been a challenge on its own, since none so far have been successfully accepted by the international community, thus making these initiatives not valuable. The Tallinn manual is the only substantial international resource, which provides lawful guidelines on how to deal with cyber-attacks, but it is non-binding and so its efficiency cannot be fully estimated, nor does it serve as an international regulation. Another challenge examined in the second chapter is offensive cyber operations such as Stuxnet, which is the only known attack so far to cause physical damages, as well as the cyber-attacks on the Ukrainian power grids, which destabilized the electrical network. This highlighted the necessity for a cyber deterrence national strategy to be developed since the threat from similar or even more advanced attacks that can cause cyber warfare in the future is growing. The goal of the thesis was establishing a conceptual framework, purposed with serving to formulate national cyber deterrence strategies. It has done so by determining which concepts, derived from both

classical and contemporary deterrence strategies that have been proven, and effective, are suitable for the cyber domain. The deterrence by denial cluster, consisting of both classical and contemporary concepts has been evaluated substantially and deemed applicable to the cyber domain, which is illustrated in the proposed conceptual framework. The deterrence by threats and punishment cluster has also been assessed and formed correspondingly and was assimilated into the framework where a viable link has been established. Consequently, classical deterrence concepts, like massive retaliation, pre-emptive war, strike first, and the threat of war found their way to the framework. Additionally, the contemporary deterrence concepts of cross-domain operations and the threat of credible punishment are also a significant part of the framework. Furthermore, the proposed framework incorporates cumulative deterrence concepts, which combine both offensive and defensive capabilities in order to achieve supremacy. It also eliminates irrelevant conceptions, such as absolute deterrence and preventive war. Altogether, the proposed conceptual framework offers a competent approach to the problem of cyber deterrence, by guiding and formulating national cyber deterrence strategies through already established and relevant deterrence concepts from the classical and contemporary theories. This could contribute towards preventing warfare actions in the cyber domain, only if states concentrate their efforts in creating such strategies, which are focused on preserving the peace, rather than indulging in reckless behavior in an unregulated military domain. The framework could only serve as guidance for creating cyber deterrence strategies, and this thesis recognizes that it may not apply to every country. Furthermore, there are certain limitations that the framework encounters, such as its lack of consideration towards the private sector. Moreover, the implementation of the entire conceptual framework might not be possible for some states. Although partial adoption will also be beneficial, it would be less effective than the complete implementation of the proposed framework for the national cyber deterrence strategy.

The conceptual framework can be a great tool to guide states on how to initiate or further develop their own strategy in the cyber domain. Deploying and keeping up to date such a strategy has been established as crucial in this thesis. Therefore, implementing some, if not all, of the conceptual framework, is essential for states that wish to not only be more secure in the cyber domain but also have a way to fully utilize their cyber capabilities.

Appendices.

Figure 1:



Content tables:

Deterrence Strategy	Summary	Suitable Situations	Target Actors
Defensive Deterrence	Acquiring and developing denial defence systems in the form of IDPS, SIEM, as well as various other measures, is crucial in establishing a well-protected ecosystem that would be able to deny attacks. The level of advancements and investment is dependent on the state-actor and proportionately will measure the level of threat it can counter.	<ul style="list-style-type: none"> • Cyber-attacks aiming to penetrate and damage network infrastructure • Ones that are purposed in causing physical damages. • Malware designed to disrupt services 	Highly efficient against non-state actors, but it might be less efficient if used on its own versus sophisticated state-sponsored cyber-attacks

Deterrence Strategy	Summary	Suitable Situations	Target Actors
Offensive Deterrence	Deterrence by punishment and by fear of consequence both fall under the offensive deterrence strategy umbrella. Punishment requires retaliation actions that might involve the other military domains as well as sanctions and international assistance, with a stress on the importance of reliable attribution. 'By fear' relies on advanced cyber-attacking capabilities and the ability to strike first in an effective way and thus mark superiority that will deter retaliation as well as potential attack attempts.	<ul style="list-style-type: none"> • Involvement of the other four military domains might be utilized • Reliant on a strong retaliation cyber capability • Sanctions on an economic and diplomatic level 	Effective when used against state-actors, however, might have a lesser effect and not deteriorate cyber-attacks deployed by non-state individuals or organizations.

Deterrence Strategy	Summary	Suitable Situations	Target Actors
Cumulative Deterrence	The cumulative strategy combines defensive and offensive concepts aiming to achieve domain dominance. This is achieved by the development of advanced cyber weapons as well as establishing highly advanced denial systems. This combination creates the perception of total superiority that will result in relentless retaliation if tested.	<ul style="list-style-type: none"> • Achieving cyber supremacy • Reliable against most cyber-attacks as it deploys a combination of offensive and defensive capabilities • Discourage attack attempts by creating a dominant personification 	Well-rounded and effective against both state and non-state adversaries.

Deterrence Strategy	Summary	Suitable Situations	Target Actors
Rules and Norms	This concept requires the creation and establishment of rules and norms drafted and developed in an international agreement. The purpose of these regulations upon the cyber domain will be aimed at peace preservation on a global scale. It will also mean the establishment of international organizations as well as networks to monitor and manage the cyberspace	<ul style="list-style-type: none"> • Internationally accepted rules and norms • Reliant upon the monitoring and supervision conducted by international organizations • Expects all parties to have a national cyber deterrence strategy. 	Limiting the threat of hostile actions by participating states and utilizes international organizations to manage breaches in established regulation.

Bibliography:

1. Abdollah, T. (2019) 'Iran Increases Cyber Attacks On U.S. Government', available at: <<https://www.insurancejournal.com/news/national/2019/06/24/530257.htm>>, accessed on 17th May 2020.
2. AFCEA, (2012) *The Russo-Georgian War 2008: The Role of The Cyber Attacks In The Conflict*, Fairfax, V.A., p.1-27, available at: <<https://www.afcea.org/committees/cyber/documents/TheRusso-GeorgianWar2008.pdf>>, accessed on 13th May 2020.
3. Almog, D. (2004) 'Cumulative Deterrence and the War on Terrorism', *Parameters*, Volume 34, Number 4, p. 4-19, available at: <<https://www.hsdl.org/?abstract&did=453973>>, accessed on 18th July 2020.
4. Baezner, M. and Cordey, S. (2019) *National Cybersecurity Strategies in Comparison – Challenges for Switzerland*, Zürich, Switzerland: Center for Security Studies (CSS), ETH Zürich, p.1-34, available at: <<https://css.ethz.ch/en/center/CSS-news/2019/07/nationale-cybersicherheitsstrategien-im-vergleich--herausforderungen-fuer-die-schweiz-.html>>, accessed on 18th May 2020.
5. Bar-Joseph, U. (1998) 'Variations on a theme: The conceptualization of deterrence in Israeli strategic thinking', *Security Studies*, Volume 7 Number 3, p. 145-181, available at: <https://www.academia.edu/38714078/Uri_Bar-Joseph_Variations_on_a_Theme_The_Conceptualization_of_Deterrence_in_Israeli_Strategic_Thinking_Security_Studies_Vol.7_No.3_1998_pp._149-184>, accessed on 18th June 2020.
6. Brantly, A. (2016) *The Decision to Attack: Military And Intelligence Cyber Decision-Making*, Athens, Georgia: University of Georgia Press, p.133.
7. Brantly, A. (2018) 'The Cyber Deterrence Problem', in: T. Min rik, R. Jakschis and L. Lindstr m, (ed.) *10th International Conference on Cyber Conflict CyCon X: Maximising Effects*, Tallinn, Estonia: NATO CCD COE, p. 31-55, available at: <https://ccdcoe.org/uploads/2018/10/CyCon_2018_Full_Book.pdf>, accessed on 30th May 2020.

8. Broad, W., Markoff, J. and Sanger, D. (2011) 'Israeli Test On Worm Called Crucial In Iran Nuclear Delay', available at: <https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html>, accessed 22 June 2020.
9. Buchanan, B. (2017) *Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*, Oxford, UK.: Oxford University Press, p.110.
10. Center for Strategic and International Studies, (2008) *Securing Cyberspace For The 44Th Presidency*, Washington D.C: Center for Strategic and International Studies, p.20-21, available at: https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/081208_securingcyberspace_44.pdf, accessed 24th May 2020.
11. Chairman of the Joint Chiefs of Staff, (2006) *The National Military Strategy For Cyberspace Operations*, Washington D.C.
12. Clausewitz, C., Paret, P. and Howard, M. (1989) (ed.) *On War*, Princeton, N.J.: Princeton University Press, p.602.
13. Cohen, M. (2011) 'Peace In The Post-Cold War World', available at: <https://www.theatlantic.com/international/archive/2011/12/peace-in-the-post-cold-war-world/249863/>, accessed on 2nd May 2020.
14. Collier, P. and Friedman, A. (2014) *Cybersecurity And Cyberwar*. New York: Oxford University Press, p.65.
15. *Convention on Cybercrime*. 185.
16. Corera, G. (2019) 'NATO: Cyber-Attack On One Nation Is Attack On All', available at: <https://www.bbc.com/news/technology-49488614>, accessed on 26th May 2020.
17. Crowther, A. and Ghori, S. (2015) 'Detangling the Web: A Screenshot of U.S. Government Cyber Activity', *Joint Force Quarterly*, Volume 78, Number 3, p. 75-83, available at: <https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-78/Article/607658/detangling-the-web-a-screenshot-of-us-government-cyber-activity/>, accessed on 13th May 2020].
18. Crowther, G. (2017) 'The Cyber Domain', *The Cyber Defense Review*, Volume 2, Number 3, p. 63-78, available at: <https://www.jstor.org/stable/10.2307/26267386>, accessed on 12th May 2020].

19. Deibert, R., Palfrey, J., Rohozinski, R., Zittrain, J. and Thien, V. (2011) Access Contested, Cambridge, MA: MIT Press, p. 129.
20. Denning, D. (2001) 'Activism, Hacktivism, and Cyberterrorism: The Internet As a Tool for Influencing Foreign Policy', in: Networks and Netwars The Future of Terror, Crime, and Militancy (ed.), Santa Monica, CA: RAND, p. 241, available at: https://www.rand.org/pubs/monograph_reports/MR1382.html, accessed on 12th June 2020.
21. Department of Defense (2010) *U.S. Cyber Command Fact Sheet*, Washington D.C.: U.S. Department of Defense, p.1.
22. Department of Defense (2011) *Department Of Defense Strategy For Operating In Cyberspace*, Washington D.C: U.S. Department of Defense, p. 3.
23. Department of Defense (2017) *Dictionary Of Military And Associated Terms*, available at http://www.dtic.mil/doctrine/new_pubs/dictionary.pdf, Washington D.C.
24. Department of Defense (2018) *Cyber Strategy*, Washington D.C.: Department of Defense, pp.1-10.
25. Dev, P. (2015) 'Use Of Force" And Armed Attack Thresholds In Cyber Conflict: The Looming Definitional Gaps And The Growing Need For Formal U.N. Response.', Texas International Law Journal, Volume 50, Number 2, p. 386, available at: <https://texashistory.unt.edu/ark:/67531/metapth838918/>, accessed on 30th May 2020].
26. DoD Defense Science Board (2017) *Task Force on Cyber Deterrence*, Washington D.C.: Department of Defence, p.4, available at: <https://apps.dtic.mil/dtic/tr/fulltext/u2/1028516.pdf>, accessed on 22nd May 2020.
27. Dulles, J. (1954) 'Policy for Security and Peace.', p. 353-364, available at: <https://www.foreignaffairs.com/articles/united-states/1954-04-01/policy-security-and-peace>, accessed on 28th April 2020.
28. Elkus, A. (2013) 'Moonlight Maze', in: J. Healey, (ed.) A Fierce Domain: Conflict in Cyberspace, 1986 To 2012, Vienna, VA: Cyber Conflict Studies Association, pp.152-163.
29. Eshel, T. (2012) 'Organized Crime In The Digital Age', available at: https://defense-update.com/20120328_organized_cyber_crime.html, accessed on 12th June 2020.

30. Federal Bureau of Investigations (2016). 'Iranian Ddos Attacks', available at: <https://www.fbi.gov/wanted/cyber/iranian-ddos-attacks/irancybercollage.pdf>, accessed on 29th May 2020.
31. Federation of American Scientists & Natural Resources Defense Council (2009) *A New Nuclear Policy On The Path Toward Eliminating Nuclear Weapons*, Washington D.C.: Federation of American Scientists, pp.21-22.
32. Finkle, J. (2014) 'Exclusive: Iran Hackers May Target U.S. Energy, Defense Firms, FBI Warns', available at: <https://www.reuters.com/article/us-cybersecurity-iran-fbi/exclusive-iran-hackers-may-target-u-s-energy-defense-firms-fbi-warns-idUSKBN0JQ28Z20141213>, accessed on 29th May 2020]
33. Galbreath, D. (2008) The Organization For Security And Co-Operation In Europe, London: Routledge.
34. Gartzke, E. (2013) 'The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth', International Security, Volume 38, Number 2, p. 41-73.
35. George, A. (1991) Forceful Persuasion: Coercive Diplomacy As An Alternative To War, Washington D.C.: United States Institute of peace Press, pp.3-14.
36. Gergorin, J. (1991) 'Deterrence in the post-cold war era', The Adelphi Papers, Volume 32, Number 266, p. 3-13.
37. Green, J. (2016) Cyber Warfare, London: Routledge, Taylor & Francis Group, p.89.
38. Greenwald, G. and MacAskill, E. (2013) 'Obama Orders US To Draw Up Overseas Target List For Cyber-Attacks', available at: <https://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas>, accessed on 20th May 2020.
39. Hill, A. (2019) The Ultimate Challenge: Attribution For Cyber Operations, Montgomery, Alabama: Air University Press, p.4.
40. Howard, T. and Cruz, J. (2017) 'The Cyber Vulnerabilities Of The U.S. Navy', available at: <https://maritime-executive.com/editorials/the-cyber-vulnerability-of-the-us-navy>, accessed on 12th July 2020.
41. Huth, P. (1999) 'Deterrence and International conflict: Empirical Findings and Theoretical Debates', Annual Review of Political Science, Volume 2, Number 1, pp.25-48.

42. Jentleson, B. and Whytock, C. (2006) 'Who "Won" Libya? The Force-Diplomacy Debate and Its Implications for Theory and Policy', International Security, Volume 30, Number 33, pp.47-86.
43. Jervis, R. (1982) 'Deterrence and Perception', International Security, Volume 7, Number 3, p.17.
44. Kanuck, S. (2012) 'Sovereign Discourse on Cyber Conflict Under International Law', Texas Law Review, Volume 88, Number 7, p.17, available at: <https://www.law.upenn.edu/live/files/1345-sean-kanuck-reading-keynote>, accessed 26th May 2020.
45. Klimburg, A. (2011) 'Mobilising Cyber Power', Survival, Volume 53, Number 1, pp.41-60.
46. Kolodkin, B. (2012) 'Understanding Arms Control', available at: <https://www.thoughtco.com/what-is-arms-control-3310297>, accessed on 1st May 2020.
47. Krishnadev, C. (2018) 'Some Of The People Trump Has Blamed For Russia's 2016 Election Hack', available at: <https://www.theatlantic.com/international/archive/2018/07/trump-russia-hack/565445/>, accessed on 22nd May 2020.
48. Lapowsky, I. (2017) 'Facebook May Have More Russian Troll Farms To Worry About', available at: <https://www.wired.com/story/facebook-may-have-more-russian-troll-farms-to-worry-about/>, accessed on 29th May 2020.
49. Lee, H. (2015) 'The Challenges of Cyber Deterrence', Pointer, Journal of the Singapore armed forces, Volume 41, Number 1, p. 12-22, available at: [https://www.mindef.gov.sg/oms/content/dam/imindef_media_library/graphics/pointer/PDF/2015/Vol.41%20No.1/3\)%20V41N1_The%20Challenges%20of%20Cyber%20Deterrence.pdf](https://www.mindef.gov.sg/oms/content/dam/imindef_media_library/graphics/pointer/PDF/2015/Vol.41%20No.1/3)%20V41N1_The%20Challenges%20of%20Cyber%20Deterrence.pdf), accessed on 23rd May 2020.
50. Leitzel, B. and Allard, A. (2016) Strategic Cyberspace Operations Guide, Philadelphia, PA: Center for Strategic Leadership, p.7.
51. Libicki, M. (2016) Cyberspace In Peace And War, Annapolis, Maryland: Naval Institute Press, p.262.

52. Liff, A. (2012) 'Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War', Journal of Strategic Studies, Volume 35, Number 3, p. 401-428.
53. Lightbody, B. (2004) The Second World War, London: Routledge, p. 55.
54. Lindsay, J. (2013) 'Stuxnet and the Limits of Cyber Warfare', Security Studies, Volume 22, Number 3, p. 365-404.
55. Liptak, A., 2019. 'Israel Launched An Airstrike In Response To A Hamas Cyberattack', available at: <<https://www.theverge.com/2019/5/5/18530412/israel-defense-force-hamas-cyber-attack-air-strike>>, accessed on 11th July 2020.
56. Lipton, E., Sanger, D. and Shane, S. (2016) 'The Perfect Weapon: How Russian Cyberpower Invaded The U.S', available at: <https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?_r=0>, accessed on 23rd May 2020.
57. Lord, N. (2016) 'What Is The NIS Directive? Definition, Requirements, Penalties, Best Practices For Compliance, And More', available at: <<https://digitalguardian.com/blog/what-nis-directive-definition-requirements-penalties-best-practices-compliance-and-more>>, accessed on 19th May 2020.
58. Lynn, W. (2010) 'Defending a New Domain: The Pentagon's Cyberstrategy'. Foreign Affairs, Volume 89, Number 5, p. 100. Available at: <<https://www.jstor.org/stable/20788647>>, accessed on 25th May 2020.
59. Margulies, P. (2015) 'Sovereignty And Cyber Attacks: Technology's Challenge To The Law Of State Responsibility', Melbourne Journal Of International Law, Volume 14, Number 1, p. 495, available at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2557517>, accessed on 30th May 2020.
60. McGuffin, C. and Mitchell, P. (2014) 'On domains: Cyber and the practice of warfare', International Journal: Canada's Journal of Global Policy Analysis, Volume 69, Number 3, p. 394-412.
61. McKenzie, T. (2017) Is Cyber Deterrence Possible, Montgomery, AL: Air University.
62. Merriam-webster dictionary website, available at: <<https://www.merriam-webster.com/dictionary/domain>>, accessed on 12th May 2020.

63. Min rik, T., Jakschis, R. and Lindstr m, L. (2018) 10Th International Conference On Cyber Conflict, Tallinn, Estonia: NATO CCD COE, pp.31-55.
64. Morgan, P. (2010) ‘Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm’, in: National Research Council, (ed.) Proceedings of a workshop on deterring cyberattacks, Washington D.C.: National Academies Press, p. 67, available at: <https://www.nap.edu/catalog/12997/proceedings-of-a-workshop-on-deterring-cyberattacks-informing-strategies-and#toc>>, accessed on 21st June 2020.
65. Morrison, J. (2012) ‘US Readies Cyber-Attack Forces’, available at: <https://www.bbc.co.uk/news/technology-19922421>>, accessed on 12 June 2020.
66. Nalebuff, B. (1988) ‘Minimal Nuclear Deterrence’, Journal of Conflict Resolution, Volume 32, Number 3, p. 411-425.
67. National Research Council (1997), Post-Cold War Conflict Deterrence, Washington DC: The National Academies Press.
68. Office of the Director of National Intelligence, 2017. *Background To “Assessing Russian Activities and Intentions In Recent US Elections”*: *The Analytic Process And Cyber Incident Attribution*, Washington D.C: ODNI, p. 6-7, available at: https://www.dni.gov/files/documents/ICA_2017_01.pdf>, accessed on 29th May 2020.
69. O'Smith, D. (1955) U. S. Military Doctrine, New York City: Sloan & Pearce, p.68.
70. Ottis, R. (2010) ‘From Pitchforks to Laptops: Volunteers in Cyber Conflicts’, in: C. Czosseck and K. Podins (ed.) Conference on Cyber Conflict, Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence, p. 97-109, available at: https://ccdcoe.org/uploads/2018/10/1_Proceedings2010FullBook.pdf>, accessed 12 June 2020.
71. Paul, T., Morgan, P. and Wirtz, J. (2009) Complex Deterrence, Chicago: University of Chicago Press, p.2.
72. Richet, J. (2015) Cybersecurity Policies And Strategies For Cyberwarfare Prevention, Hershey, PA: Information Science Reference, p.112.
73. Rid, T. and Buchanan, B. (2014) ‘Attributing Cyber Attacks’, Journal of Strategic Studies, Volume 38, Number 2, p. 4-37.

74. Rid, T. (2016) 'How Russia Pulled Off The Biggest Election Hack In U.S. History', available at: <<https://www.esquire.com/news-politics/a49791/russian-dnc-emails-hacked/>>, accessed on 29th May 2020.
75. Riggs, C. (2004) Network Perimeter Security. Boca Raton: Auerbach Publications, p.126.
76. Sanger, D. (2016) 'Obama Strikes Back At Russia For Election Hacking, available at: <<https://www.nytimes.com/2016/12/29/us/politics/russia-election-hacking-sanctions.html>>, accessed on 29th May 2020.
77. Schmitt, M. (2017) Tallinn Manual 2.0 On The International Law Applicable To Cyber Operations, (ed.) Cambridge: Cambridge University press.
78. Schneier, B. (2010) 'Threat Of 'Cyberwar' Has Been Hugely Hyped', available at: <<https://edition.cnn.com/2010/OPINION/07/07/schneier.cyberwar.hyped/>>, accessed on 12th June 2020.
79. Segal, A. (2016) The Hacked World Order: How Nations Fight, Trade, Maneuver, And Manipulate In The Digital Age, New York: Public Affairs, p. 28-29.
80. Shear, M. and Sanger, D. (2017) 'Putin Led A Complex Cyberattack Scheme To Aid Trump, Report Finds', available at: <https://www.nytimes.com/2017/01/06/us/politics/donald-trump-wall-hack-russia.html?_r=0>, accessed on 29th May 2020.
81. Sigholm, J. (2013) 'Non-State Actors in Cyberspace Operations'. Journal of Military Studies, Volume 4, Number 1, p. 1-37.
82. Siroli, G. (2018) 'Considerations on the Cyber Domain as the New Worldwide Battlefield' The International Spectator, Volume 53, Number 2, p. 111-123.
83. Soesanto, S. (2019) *Trend Analysis: The Evolution Of US Deterrence Strategy In Cyberspace*. Zürich, Switzerland: Center for Security Studies, pp.1-40, available at: <https://css.ethz.ch/content/specialinterest/gess/cis/center-for-security-studies/en/publications/risk-and-resilience-reports/details.html?id=/t/h/e/e/the_evolution_of_us_defense_strategy_in>, accessed on 19th May 2020.
84. Stein, J. (1992) 'Deterrence and Compellence in the Gulf, 1990-91: A Failed or Impossible Task', International Security, Volume 17, Number 2, p. 147-179.

85. Stevens, T. (2012) 'A Cyberwar of Ideas? Deterrence and Norms in Cyberspace', Contemporary Security Policy, Volume 33, Number 1, p. 148-170.
86. The White House (2003) *The National Strategy To Secure Cyberspace..* Washington D.C.
87. The White House (2011) *International Strategy For Cyberspace.* Washington D.C.
88. The White House (2018) *National Cyber Strategy Of The United States Of America.* Washington D.C. p. 21.
89. Thibodeau, P. (2014) 'Cyberattacks An 'Existential Threat' To U.S., FBI Says', available at: <<https://www.computerworld.com/article/2516690/cyberattacks-an--existential-threat-to-u-s---fbi-says.html>>, accessed on 12th June 2020.
90. Tor, U. (2015) 'Cumulative Deterrence as a New Paradigm for Cyber Deterrence', Journal of Strategic Studies, Volume 40, Number 1-2, pp. 92-117.
91. Tran, D. (2018) 'The Law Of Attribution: Rules For Attributing The Source Of A Cyber-Attack', Yale Journal Of Law And Technology, Volume 20, Number 3, p.376-441, available at:
<https://law.yale.edu/sites/default/files/area/center/global/document/2017.05.10_-_law_of_attribution.pdf>, accessed 30 May 2020.
92. U.S. Congress (2001) *Uniting And Strengthening America By Providing Appropriate Tools Required To Intercept And Obstruct Terrorism (USA Patriot Act) Act Of 2001.* Washington D.C.: US Congress.
93. U.S. Department of Homeland Security (2002) *Creation Of The Department Of Homeland Security.*
94. United Nations (2010) *Group Of Governmental Experts On Developments In The Field Of Information And Telecommunications In The Context Of International Security.* A/65/150, New York: General Assembly, p.7. Available at:
<<https://undocs.org/A/65/201>>, accessed on 26th May 2020.
95. Valeriano, B. and Maness, R. (2015) Cyber War Versus Cyber Realities, New York: Oxford University Press, p. 57-60.
96. Veluz, D. (2010) 'Stuxnet Malware Targets SCADA Systems', available at:
<<https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/54/stuxnet-malware-targets-scada-systems>>, accessed on 26th July 2020.

97. Verizon, (2012) '2012 Data Breach Investigations Report', available at: https://www.wired.com/images_blogs/threatlevel/2012/03/Verizon-Data-Breach-Report-2012.pdf>, accessed on 12th June 2020.
98. Yang, G., Bellingham, J., Dupont, P., Fischer, P., Floridi, L., Full, R., Jacobstein, N., Kumar, V., McNutt, M., Merrifield, R., Nelson, B., Scassellati, B., Taddeo, M., Taylor, R., Veloso, M., Wang, Z. and Wood, R. (2018) 'The grand challenges of Science Robotics', Science Robotics, Volume 3, Number 14.
99. Yannakogeorgos, P. and Lowther, A. (2013) Conflict Conflict And Cooperation In Cyberspace The Challenge To National Security and Cooperation In Cyberspace, Boca Raton, Florida: CRC Press, p. 116.
100. Zetter, K. (2016) 'Inside The Cunning, Unprecedented Hack Of Ukraine's Power Grid' available at: <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>>, accessed on 23rd May 2020.