UNIVERSITY OF TARTU

Faculty of Social Sciences

Johan Skytte Institute of Political Studies

David Aljoscha Hoffmann

# OFFENSE-DEFENSE THEORY, STATE SIZE AND POSTURING IN THE CYBER DOMAIN: THE CASE OF THE UNITED KINGDOM AND THE REPUBLIC OF ESTONIA

MA thesis

Supervisor: Thomas Linsenmaier

Tartu 2019

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

.....

*/ signature of author /*

The defence will take place on ..... */ date /* at ..... */ time /*

..... */ address /* in auditorium number ..... */ number /*

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

..... */ position /*

I, David Aljoscha Hoffmann (personal code 39109260068)

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

OFFENSE-DEFENSE THEORY, STATE SIZE AND POSTURING IN THE CYBER DOMAIN: THE CASE OF THE UNITED KINGDOM AND THE REPUBLIC OF ESTONIA

supervised by Thomas Linsenmaier.

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

3. I am aware of the fact that the author retains the rights specified in p. 1 and 2.
4. I certify that granting the non-exclusive licence does not infringe other persons' intellectual property rights or rights arising from the personal data protection legislation.

Tartu, 07.01.2019

_____ (signature)

**Abstract**

The increasing relevance of the cyber domain has an impact on the national security of states. At current stage, states are in a phase of introducing the cyber approach that best coincides with their security needs. While all states share the same threat of becoming victim to devastating cyber-attacks, they need to consider whether they take an offensive or defensive cyber posture in order to increase security in the virtual domain. This thesis addresses the question of whether state size have an effect on the cyber posture of state. First, in an attempt to theorize cyber posturing, the study modifies traditional assumptions of the offense-defense balance theory and applies the logic of the balance to the cyber domain. In addition, this thesis elaborates state size as a specific element that could explain an offensive or defensive cyber posture. It analysis whether cyber posture of small and large states differs and examines the sensitivity of small and large states to the offense-defense balance. In an empirical analysis of the cyber posture of Estonia and the United Kingdom, the research examines theoretical assumptions in a comparative analysis. The thesis demonstrates that state size has an impact on the cyber posture of states. While the UK adopts an offensive cyber posture, Estonia's strategic documents do not indicate the development of offensive cyber capabilities at present the time. Finally, the thesis points out that small states are more sensitive to the offense-defense balance in cyberspace and adjust their cyber posture according to the offensive or defensive advantage.

**Table of Contents**

**List of abbreviations**

| | | |
|---|---|---|
| ACD | - | Active Cyber Defense |
| CERT | - | Computer Emergency Readiness Team |
| DoS attack | - | Denial of Service attack |
| EGDI | - | e-Government Development Index |
| EU | - | European Union |
| GCI | - | Global Cybersecurity Index |
| GCHQ | - | Government Communications Headquarters |
| GDP | - | Gross Domestic Product |
| G7 | - | Great seven – the seven largest economies in the world |
| ICT | - | Information and Communication Technology |
| IT | - | Information technology |
| ITU | - | International Telecommunications Union |
| NATO | - | North Atlantic Treaty Organization |
| NCSS | - | National Cyber Security Strategy |
| NOCP | - | National Offensive Cyber Program |
| OT | - | Operational technology |
| UK | - | United Kingdom |

## 1 Introduction

Cyberspace has become a matter of national security. The use of information and communication technologies makes societies increasingly dependent on the cyber domain and pushes states to take action in order to preserve prosperity and security. States are currently in a phase of introducing the cyber approach that best coincides with their security needs. A growing number of governments have declared the cyber domain as one of the state's security priorities and formulated cyber security strategies to strengthen resilience, combat attacks and distribute tasks and responsibilities.[1] All states share the same threat of becoming victims to devastating cyber-attacks. The 2018 Global Risk Report of the World Economic Forum identifies cyber-attacks as one of the most likely occurring risks in the next year.[2] Cybersecurity is of high relevance for every society, regardless of their stage of development.

As a result, states are increasingly diverting considerable recourses into the security of national networks and servers. While the emphasis is on defensive capabilities, some states develop offensive cyber capabilities for increasing their security.[3] This raises the question of which are the factors that influence a state's decision to develop offensive cyber tools and adopt an offensive posture in cyberspace.

In the literature, various authors elaborate the benefits and risks of offensive cyber capabilities and scrutinize how these tools alter national security approaches.[4] Whereas conventional theories have been applied to the cyber domain, the question of cyber posturing has been still undermined. In an attempt to theorize cyber posturing, this study addresses this gap and contributes to the growing literature of cyber security in two ways. First, it modifies various concepts in order to make traditional International Relations (IR) theory applicable to the cyber environment. Cyber posturing and factors behind the development of offensive or defensive cyber capabilities could be explained by various

[1] For a list of national cyber security strategies see: NATO Cooperative Cyber Defence Centre of Excellence, 'Cyber Security Strategy Documents'
[2] World Economic Forum, *The Global Risks Report 2018*
[3] The World Street Journal currently lists 29 states that include offensive components in their military strategy. See: The Wallstreet Journal, 'Cataloging the World's Cyberforces'
[4] See for example: Kello, *The virtual weapon and international order*; Choucri, *Cyberpolitics in international relations*; Lewis, *Rethinking cybersecurity*; Lin, 'Offensive Cyber Operations and the Use of Force'; Peterson, 'Offensive Cyber Weapons'; Lewis, *Rethinking cybersecurity*

well-established theories.[5] This research utilizes offense-defense balance theory to explore state posturing and applies this logic in the cyber domain. In line with neorealist thinkers, the thesis assumes that the offense-defense balance determines a state's cyber posture.[6]

Second, in addition to the more general concern of applying IR theory in cyberspace, this study seeks to highlight state size as a specific element that has been so far neglected in studies of offense-defense theory. The few existing studies, which apply conventional offense-defense theory to the cyber domain, make no distinction between small and large states.[7] This thesis addresses this gap by examining how size is linked to a certain cyber posture. Contributing to small states literature, this research explores how small states deal with the cyber domain from their specific position and presents new findings regarding their cyber posturing.

The aim of the thesis is to explore how state size matters for which offensive or defensive cyber posture a state adopts. It analysis whether cyber posture of small and large states differs and examines the sensitivity of small and large states to the offense-defense balance. Accordingly, the research question of this thesis is the following: what effect does state size have on the cyber posture of state? Derived from offense-defense theory and small state literature, the thesis hypothesizes that small states adopt a cyber posture, which closely corresponds to the offense-defense balance, whereas cyber posturing of large states might deviate from the balance. Depending on whether offense or defense has the advantage in cyberspace, small states rather opt for an offensive or defensive cyber posture, whereas large states have more leeway to choose. Moreover, the thesis assumes that there is no difference in cyber posture of small and large states, as the offense-defense balance effects both states in a similar way.

Methodologically, this study makes use of a comparative analysis, comparing the cyber posture of the United Kingdom and the Estonian Republic. The UK represents a large and

[5] For instance, deterrence theory distinguishes between deterrence by retaliation (offensive) and deterrence by resilience (defensive), which could be an explanatory approach to cyber posture. See Freedman, *Deterrence*

[6] For attempts to theorize offense-defense in the cyber domain, see Saltzman, 'Cyber Posturing and the Offense-Defense Balance'.

[7] See for example: Locatelli, 'The Offense/Defense Balance in Cyberspace'; Shaheen, 'Offense-Defense Balance in Cyber Warfare' and Locatelli, 'The Offense/Defense Balance in Cyberspace'

Estonia a small state. The empirical part focuses separately on cyber doctrine and cyber capabilities in order to identify an offensive or defensive cyber posture.

The theoretical part of this thesis (chapter 2) is structured as follows: First, it engages with offense-defense theory. The offense-defense theory is the independent variable to explain cyber posture of states. How does offense-defense theory may explain the choice for an offensive or defensive posture and which factors influence the offense-defense balance? Second, derived from conventional offense-defense theory, the thesis transfers the assumptions to the cyber domain and adjusts the main concepts accordingly. How does the logic of the offense-defense balance function in the cyber domain? In this discussion, the study does not aim to answer the question of whether offense or defense has the advantage in cyberspace, but rather discusses how the advantage of either offense or defense affects theoretical expectations of state posture in the cyber domain. Third, the thesis delves into the literature of small states in international security with the aim to establish how small states shape posturing. Additionally, these assumptions are theorized against the background of the cyber domain. How does state size shapes the decision to adopt an offensive or defensive posture in cyberspace? Do the adjusted factors of offense-defense balance theory have influence on small state's cyber posture in the same way they have on large states?

The theoretical considerations are followed by the methodology part (chapter 3), which defines the methodological parameters of this thesis. The empirical part (chapter 4) scrutinizes cyber posture of the UK and Estonia to test the hypothetical assumptions. The aim is to provide an illustration of the theoretical argument and discuss it in a comparative perspective. The conclusion (chapter 5) summarizes findings of this thesis.

## 2 Theorizing the offense-defense balance and state size in cyberspace

The following chapters frame the theoretical part of this research. First, it conceptualizes cyberspace and points out various characteristics that are necessary in order to understand the basic principles of the virtual domain and their relevance for national security. Second, the following part illustrates the traditional offense-defense balance and examines how the same logic can be applied to the cyber domain. Particular emphasis will be placed on the distinction of offensive and defensive cyber capabilities. Finally, the concluding chapter of the theoretical part focuses on small states and theorizes their posture in the virtual domain.

### 2.1 Cyberspace and national security

Cyberspace is often considered as the fifth domain beside land, sea, air and outer space.[8] Due to its fundamental difference from traditional domains, the cyber domain poses a challenge to strategists, military planners and analysts. This section conceptualizes the main elements of cyberspace and contrasts them to the three domains of land, sea, and air. The aim is to provide a brief overview of cyberspace's main characteristics and highlight challenges regarding the different environment from a national security perspective.

The concept of space is a crucial element in International Relations theory. In world politics, states attempt to use all types of space to exercise power and influence. Thereby, they use technologies to make space more accessible and usable. For a long time, states operated only on land and at sea. The technological advances of vehicles and ships were of high strategic importance. Since the beginning of the 20th century, the air space became a decisive domain in terms of warfare. Military planes were used to increase military power and react more quickly and precisely to military threats. The notion of space is thereby often linked to territoriality.[9]

[8] This thesis uses the terms cyberspace, cyber domain and virtual domain interchangeably. For information on cyberspace as the fifth domain, see for example: THE ECONOMIST, 'War in the fifth domain: Are the mouse and keyboard the new weapons of conflict?', 1 July 2010

[9] Choucri, *Cyberpolitics in international relations*, 5

In the literature, the concept of cyberspace is blurred.[10] The impact of the new domain is significant for political, economic and social life. Economic actors conduct money transactions, politicians increase their popularity, terrorists plan attacks and military forces increase their power and efficiency. Cyberspace is an "operational domain"[11] in the sense of being useful to communicate, store and exchange information. This thesis looks at cyberspace from a security perspective.

Libicki provides a useful three-layered conceptualization of cyberspace. Firstly, the physical layer contains computer hardware, routers and partially wires. These components are foundational and existential for cyberspace, making that the domain is entirely reliant on electronic devisces. Secondly, the syntactic layer consists of the code that enables hardware components to communicate with each other. The hardware components of the physical layer require software to function. Programmers and system designers use codes to instruct machines and give them tasks to complete. The syntactic layer is crucial when it comes to system hacking. As elaborated in the following chapters, intruders seek to alter codes in a way that they gain authority over the system and use the system for own purposes. Thirdly, the semantic layer is the information that is stored in cyberspace, i.e. on a server or computer device. The information is what users of cyberspace receive when they enter the domain. Libicki correctly indicates that attacks can take place on the semantic level due to the spread of false information.[12] Although these attacks certainly have influence on a state's national security, this thesis is based on a conceptualization of cyber-attacks that takes place on the syntactic level.

Each of the three layers depends on the former one and cannot function without it. Software must be installed to hardware and information can be only accessed when the software enables the hardware to display it. On the contrary, destroying the semantic layer has no effect on the former two, nor does destroying the syntactic layer affect the existence of the physical components themselves.[13] Clark extents the model with a fourth layer that can be placed above the semantic layer. The fourth layer consists of the people

[10] For a table of different definitions of cyberspace see Kuehl, 'From Cyberspace to Cyberpower: Defining the Problem', 26–7
[11] Ibid., 29
[12] Libicki, *Cyberdeterrence and Cyberwar*, 12–3
[13] See further elaboration on Libicki's Model in: Bryant, *International conflict and cyberspace superiority*, 53

who act in cyberspace. People contribute to the domain by adding content to the network and develop it further.[14] For the purposes of this study, it is useful to include people in the model. People are considered one of the greatest risks for network security. Especially for a state's most protected critical infrastructure that is controlled via a closed intranet system, people pose the greatest danger to penetrate the system by connecting infiltrated devices.[15]

Having characterized the main components of cyberspace, the following section highlights various aspects that make the cyber domain distinct from other domains. Pointing out these characteristics is a necessary step to take before applying the conventional offense-defense balance theory to the cyber domain. Moreover, it underlines the argument of a security dilemma in cyberspace and the analysis of states' cyber posture.

To begin with, cyberspace, in contrast to the conventional domains, is a virtual domain designed by humans and not existing in nature.[16] In the conventional domains, people use technology to make land, sea, air and outer space usable. While ships, planes, cars and railways were invented and developed to utilize air, land and sea, in cyberspace the technology itself constitutes the domain.[17] This aspect is central, as it outlines the consequences and limits of cyber-attacks. The more society is reliant on the virtual domain, the higher the damage of a cyber-attack. Due to a drastic increase in the dependency on the internet, the cyber domain gains increasing significance. However, in contrast to the conventional domains, states could theoretically decide to withdraw from the cyber domain and cut off internet access to their citizens.

Moreover, on the internet, the concept of borders does not apply to cyberspace in the same way as it does to the conventional domains. Border studies provide a wealth of literature that discusses how the traditional concept of borders changes with globalization

[14] Clark, 'Characterizing cyberspace: past, present and future', 4
[15] See for example: Jackson, William, 'The security singularity: When humans are the biggest problem'. *GCN,* 23 September 2011
[16] See for i.e. Kuehl, 'From Cyberspace to Cyberpower: Defining the Problem', 30. According to Kuehl, this view is only half true. He points out that the cyberspace is still based on physical characteristics (e.g. electromagnetic spectrum): ibid.
[17] Ibid., 29

and the global expansion of the internet.[18] Vinton Cerf, the "father of the internet", states that "the internet was designed without any contemplation of national boundaries" and is therefore "totally unbound with respect to geography"[19]. From the security perspective, it could be said that all states are neighbors to one other.[20] However, this does not mean that national borders have become obsolete.[21] States operate on the basis of a territorial logic and consider themselves responsible for the provision of security inside their territorial boundaries. States project this logic into the cyber domain when they, for instance, aim to secure their citizens, companies, digital infrastructure, etc. For the sake of security, states seek to gain control over actions in cyberspace.

From a legal perspective, cyber actions taking place inside state boundaries are matter of domestic jurisdiction. People acting in cyberspace are still located in a state with certain legal provisions. For instance, several states have introduced regulations that force companies to store information about their citizens on servers located within the state's territorial boundaries.[22] Others create firewalls that restrict access to information on the internet.[23]

When it comes to cyber-attacks, the geographic locations of attackers and victims do not play a role, as attacks can be launched independently from any device that has access to the internet. In addition, geographic characteristics such as mountains, rivers and oceans do not affect the attack as long as the malicious code has reached the targeted system.[24] As geography is a key variable in the traditional offense-defense balance theory, the following chapters provide a more detailed view on what can be seen as equivalent to geography in the cyber domain.

---

[18] See for example: Hare, 'Borders in Cybespace: Can Souvereignty Adapt to the Challanges of Cyber Security?' and ibid.
[19] Guernsay, Lisa, 'Welcome to the World Wide Web. Passport, Please?'. *New York Times,* 15 March 2001
[20] Buchanan, *The Cybersecurity Dilemma,* 106
[21] Goldsmith and Wu, for instance, illustrate the significance of geography in cyberspace. Their main argument relies on the heterogeneity of internet users and their demands (language, geographical identification technology etc.) See: Goldsmith and Wu, *Who controls the Internet?*, 58–63
[22] See for example: Cohen et al., 'Data Localization Laws And Their Impact on Privacy, Data Security And the Global Economy'
[23] For instance, the Great Firewall of China regulates the internet flow between China and the outside world. The firewall allows Chinese citizens to connect with foreign countries for economic purposes, but seeks to censor Western ideology. For an overview, see Sammarco, 'The Great Firewall and the Perils of Censorship in Modern China'
[24] Buchanan, *The Cybersecurity Dilemma,* 106

Furthermore, attributing cyber-attacks is an issue that challenges states to draw the correct conclusions and react appropriately to cyber-attacks.[25] Actors in the domain are more difficult to identify than in the physical domains. When using proxy servers, it is technologically possible for online actors to conceal their identities. Determining the origin of the threat requires time and financial resources and does not always lead to a certain result. Another example is the Great Firewall of China, which regulates the internet flow between China and the outside world. The firewall allows Chinese citizens to connect with foreign countries for economic purposes but seeks to censor Western ideology.[26]

Another characteristic worth considering is the wide range of actors that operate in cyberspace. The threat to a state's security may originate from individual hackers, organized crime or hostile governments. In principle, a single computer device connected to the internet is capable of entering the virtual domain and developing it further. No entity owns the internet and governments, companies and individuals all enter the cyberspace in the same way. Accordingly, all actors face the dangers that occur when operating in the cyber domain. In the same vein, all actors are potentially able to pose a danger. Even individual hackers may inflict high damage with relatively low costs. Thus, non-state actors can wield considerable power in the cyber domain. Consequently, in comparison to the physical domains, states enter into competition with a wide range of actors and do not have the same monopoly on the operational level.[27] These observations have implications for security studies and challenge International Relations theory in general. They undermine the state-centrism of the conventional offense-defense theory, as not only armed forces matter, but also professional hackers having the skills to penetrate networks and cause harm to societies.

However, an advanced cyber-attack that causes danger to a state's critical infrastructure requires advanced technological skills and financial support in order to bypass security systems. Lewis, for instance, argues that "the most dangerous and damaging attacks required resources and engineering knowledge that are beyond the capabilities of non-

[25] For a discussion on the attribution problem, see: Rid and Buchanan, 'Attributing Cyber Attacks', 5
[26] For a brief overview, see Sammarco, 'The Great Firewall and the Perils of Censorship in Modern China'
[27] Reveron, 'An Introduction to National Security and Cyberspace', 6

state actors, and those who possess such capabilities consider their use in the context of some larger strategy to achieve national goals".[28] Therefore, the number of actors behind sophisticated cyber-attacks can be reduced. This research narrows its focus to states and considers them the most powerful actors in cyberspace.[29] States possess sustainable financial resources to plan and conduct high-level cyber operations. Therefore, state-to-state interaction is a key consideration for national cyber security and the cyber security dilemma, even though attacks by non-state actors occur more often.

To summarize, this chapter first presented a definition of cyberspace that establishes the conceptual baseline for this thesis. In short, cyberspace is a virtual domain consisting of physical components, virtual software and stored information created and maintained by people. The opportunity to exploit the domain through cyber-attacks makes it a national security issue. The significance for a state's security is rising with the increasing dependence of people and machines on the internet, which is the backbone of cyberspace. The second part of this chapter underlined the main characteristics of the cyber domain. The projection of traditional theory onto the cyber domain requires a closer look at the role of borders, threat actors and the general construction of the virtual domain. Even though the elaborations in this chapter provide only a brief introduction into how cyberspace functions, it suffices to apply conventional theoretical assumptions to the cyber domain.

## 2.2 Offense-defense theory

### 2.2.1 Theoretical considerations

The offense-defense balance is a central variable of the security dilemma.[30] First, this section briefly illustrates the main arguments of the security dilemma in order to understand the logic behind the offense-defense balance. These theoretical considerations are necessary to understand why states opt for an offensive or defensive cyber posture.

[28] Lewis, *Rethinking cybersecurity*, 7
[29] States may act through a complex network of hacking groups. However, in such a setting, the state remains the actor in charge, even though it is often difficult to observe a clear link between hacking groups and the state.
[30] Jervis, 'Cooperation under the Security Dilemma', 186–7

Secondly, this section includes an illustration of the offense-defense balance and scrutinizes how the assumptions can be applied to the cyber domain. Thirdly, derived from offense-defense theory, this section seeks to formulate a conceptualization of state posture that is used as the dependent variable throughout this thesis.

The security dilemma is an essential lens through which International Relations scholars can explain a state's security behavior and the outbreak of conflicts.[31] The precondition of the dilemma is the anarchic character of the international system. Without a higher authority, states find themselves in a "self-help system", in which they take precautions in order not to become a victim of outside aggressors.[32] Consequently, states are trapped in the security dilemma when a state increases its security while decreasing the security of other states, which need to respond similarly even though they did not intend to do so.[33]

According to Booth and Wheeler, the security dilemma consists of two levels with different strategic predicaments: the dilemma of interpretation and the dilemma of response.[34] Firstly, states face the dilemma of interpretation "(…) when they are confronted, on matters affecting security, with a choice between two significant and usually (but not always) undesirable alternatives about the military policies and political postures of other entities."[35] Governments have to assess a perceived threat and take a decision regarding the intentions, motivations and capabilities of other actors under conditions of "unresolvable uncertainty". One dimension of unresolvable uncertainty is the "other minds problem", which stems from psychology. It is based on the assumption that foreign policy actors are hardly able to fully understand other state actors. Although states can scrutinize each other's behavior to a certain degree, they can never be confident about other states' intentions.[36] Another dimension that result from unresolvable uncertainty is the "ambiguous symbolism of weapons"[37]. Governments are challenged to discern whether a potential adversary is developing its military capabilities for defensive

[31] See for example: Booth and Wheeler, *The Security Dilemma*; Jervis, 'Cooperation under the Security Dilemma'; Glaser, 'The Security Dilemma Revisited' and Booth and Wheeler, *The Security Dilemma*
[32] Lynn-Jones, 'Offense-Defense Theory and Its Critics', 664
[33] Jervis, 'Cooperation under the Security Dilemma', 169
[34] The definition of the security dilemma sis taken from: Booth and Wheeler, *The Security Dilemma*, 4
[35] Ibid.
[36] Ibid.
[37] Ibid., 42

or offensive reasons. States develop defensive capabilities in order to guarantee their own security in a constantly competitive environment and offensive capabilities in order to alter the status quo for their own benefit.[38]

The second predicament, the dilemma of response, arises when decision makers believe they are certain about the intentions of the potential adversary. Consequently, they have to determine an appropriate response. The policy tool used to respond significantly influences the outcome of the dilemma. On one hand, misplaced trust towards another state may result in the state becoming a victim of an adversary that aimed to change the status quo. On the other hand, misinterpretation based on suspicion may result in an unintended military conflict. The phenomenon by which states escape the dilemma by using methods that result in enmity, although both originally have not intended to enter into confrontation, is defined as the security paradox.[39]

For this thesis, the dilemma of interpretation is more relevant. States adopt their force posture according to their security concerns, which is based on how they interpret the intentions of potential adversaries. Neorealist authors ascribe "security-seeking states"[40] two different force postures to increase their security: offensive and defensive.[41] The offense-defense balance, as a key variable of the security dilemma, sheds light on the question of why states adopt a certain posture. The central element of the balance is the "ambiguous symbolism of weapons", which includes the offensive-defensive distinction of weapons and the resulting question of whether the offense or the defense has the advantage. Assuming that defensive and offensive weapons are distinguishable and that defense has the advantage, states may increase their security without (or only to a small extent) causing a decrease in the security of other states. States are better off focusing on the protection of their territory and adopting a defensive force posture.[42] On the other hand, when offense has an advantage, "available technologies make it less expensive for

[38] Ibid., 42–5
[39] Ibid., 4–5
[40] Security dilemma theory categorizes states into security-seeking and greedy states, determined according to their motives. For further terms of this classification see Tang, *A Theory of Security Strategy for Our Time*, 24
[41] See for example Lynn-Jones, 'Offense-Defense Theory and Its Critics', 665
[42] Jervis, 'Cooperation under the Security Dilemma', 186–7

states to seek security by adopting offensive military postures and strategies."[43] Thus, the offense-defense can be defined as the "ratio of the cost of the forces the attacker requires to take territory to the cost of the forces defender has deployed"[44]. In this regard, the offense-defense balance could serve as an explanation of why states adopt an offensive or defensive posture. In a security environment where offensive weapons predominate, the theory suggests that states have more preferences to adopt an offensive posture. Contrary, a defensive advantage suggests that states opt for a defensive posture.[45]

Slayton applies the logic of the offense-defense balance to the cyber domain by using a utility-cost ratio conceptualization of offense to defense. According to her, the "utility advantage of cyber offense is the value of the offensive goal (e.g., taking territory, stealing secrets, or gaining control of a computer) less the minimum costs of achieving it"[46]. Accordingly, "the utility of the defense is the value of the defensive goal (e.g., holding territory, maintaining secrecy, keeping control of a computer) less the minimum costs of defense"[47]. Depending on whether offense or defense utility is higher, offense/defense has the advantage in the cyber domain and states are expected to favor either an offensive or defensive cyber posture.

The offense-defense balance is influenced by various factors, which determine whether offense or defense has the advantage. In the literature, there is a distinction between the "broad" and "narrow" approach to operationalizing the offense-defense balance. While the narrow approach includes only geography and technology, the broad approach adds variables such as force size, nationalism and cumulativity of resources to measure the balance.[48] The following examination is based on a narrow approach, which includes the factors of geography and technology and scrutinizes their applicability in the cyber domain. Furthermore, the section contains various considerations of what could determine state posture in cyberspace.

[43] Lynn-Jones, 'Offense-Defense Theory and Its Critics', 674–5
[44] Glaser and Kaufmann, 'What is the Offense-Defense Balance and Can We Measure it?', 55
[45] These assumptions count when states are equal in power. Even though the defense could have an advantage, the outcome may be distorted by powerful states that turn the balance to their advantage due to their superiority. See: ibid., 51
[46] Slayton, 'What Is the Cyber Offense-Defense Balance?', 80
[47] Ibid.
[48] Glaser and Kaufmann, 'What is the Offense-Defense Balance and Can We Measure it?', 60–1

To begin with, applying offense-defense balance theory to the conventional domains, geographic environment often provides advantages for the defender. An army needs to cross mountains, rivers, oceans or other territory-linked obstacles for which it is unlikely to be as well prepared as the defender.[49] In the cyber domain, these geographic obstacles are not present.[50] Malicious code can be send around the world with high speed and concrete targets. One could argue that the internet is based on the physical existence of wires connecting electronic machines and servers. As described in the previous chapter, the first layer is existential for the internet to work. Destroying the physical infrastructure of the internet would indeed have fundamental effects on accessing and using the cyber domain. In theory, these wires could be geographically located and attacked. However, firstly, it is practically impossible to endanger cyberspace by cutting the wire, as cyber networks consist of too many intertwined cable connections that can replace the interrupted wire.[51] Due to earthquakes and outdated materials, it is in fact common for internet wires to be interrupted and to require repair. Secondly, an attack on the Transatlantic Telecommunications Cable, for instance, which connects North America with Europe (TAT-14), would require financial resources and appropriate technology that would be disproportionate to the damage such an interruption would cause. Thus, the non-existence of a geographic factor in cyberspace suggests that offense has an advantage in the sense that aggressors do not need to overcome natural obstacles.[52]

However, there is another crucial aspect to add to this discussion. The geographic factor indicates the vulnerability of a state to outside threats. The offense-defense theory assumes that states with natural obstacles are less vulnerable to potential aggressors and better at defending their territory. Bringing in the small/large distinction, in the conventional domains a large territory is more difficult to attack than a small one. Therefore, large states are by definition better protected by the geographic factor than small states. However, state size and geographic factors do not help to understand the cyber postures of small and large states. In the cyber domain, the geographic environment is no obstacle to the placement of malicious code onto foreign networks. Instead,

[49] Jervis, 'Cooperation under the Security Dilemma', 194–5
[50] Buchanan, *The Cybersecurity Dilemma*, 106
[51] An insightful overview of all submarine cables see: TeleGeography, 'Submarine Cable Map'
[52] Various governments seek to gain control over their national networks by creating virtual obstacles (e.g. national firewalls). The next chapters discuss these issues in detail.

digitalization could be understood as the cyber equivalent, which may similarly affect cyber posture.

The degree of digitalization constantly increased during the last decades and will continue to rise. The International Telecommunications Union (ITU) predicts an increasing number of interconnected computer devices, up to 25 billion by 2020.[53] Most of them belong to the consumer realm, such as household appliances, medical technology, devices for private businesses and public authorities, etc. In addition, manufacturing, transportation and utility companies increasingly make use of technological devices to enhance productivity and improve operational processes. For offense-defense balance theory, digitalization of the critical infrastructure sector matters the most, as it has the greatest impact on a state's national security. The most vulnerable critical infrastructure in the cyber domain includes energy, healthcare, the financial industry, the military/defense industry and transportation.[54]

The degree of digitalization suggests that the greater a state is digitalized, the more dependent it is on cyber technologies and the greater the surface for attacks. In other words, an increasing degree of digitalization increases a state's vulnerability in cyberspace. The degree of digitalization is what states decide upon in order to gain economic and social advantages. In contrast to the traditional domains, it is not given by nature. It seems that the degree of digitalization does not play a considerable role when comparing small and large states. Large and small states could have the same degree of digitalization and are therefore in the same manner vulnerable to cyber-attacks. For this reason, digitalization does not necessarily correspond to a difference in the cyber posture of small or large states.

What impact does digitalization have on the offense-defense balance? Contrary to geography, digitalization seems to turn the balance towards the offense for the following reasons. First, a digitalized infrastructure provides intruders broader opportunities to cause damage and makes it harder to defend. Companies, organizations and state authorities make use of the same software. The WannaCry malware attack conducted in

[53] International Telecommunication Union, 'Getting ready for the digital economy', 4
[54] An executive order by former US-president Barack Obama lists 16 sectors of critical infrastructure and includes both physical and cyber-attacks in its strategy to defend these sectors: The White House, *Presidential Policy Directive - Critical Infrastructure Security and Resilience*

May 2017 serves as an appropriate example. The attacker exploited a security gap in the Windows operating system and blackmailed users to pay before unlocking their computer. The ransomware infected around 300,000 computers in 150 countries[55] and affected a wide range of sectors, such as transportation, telecommunication, energy, shipping and health care.[56] Even though WannaCry does not fall into the category of state-to-state attacks, it demonstrates the vulnerability of cyber infrastructure and the impact such attacks have on a state's security.

Second, information technology (IT) and operational technology (OT) are increasingly converging. While information technology includes the day-to-day use of software and hardware to communicate and transmit data, operational technology controls and monitors physical devices, such as power grids or dams. The general trend is that these physical devices, before operated by self-contained systems, increasingly use the same hardware and software as IT does. For example, power grids use information on people's consumption and adjust their energy production accordingly.[57]

To sum up, taking a specific dyad of states into consideration and keeping all other factors constant, the less digitalized state seems to have an advantage in cyberspace. In the offense-defense calculation, a more digitalized state must invest more into its cyber defense than a less digitalized state. Thus, digitalization seems to work opposite to territory. The more digitalized, the more offense gains the advantage. Less digitalized states reduce their margin of error as attackers have fewer opportunities to cause sophisticated damage to a state's infrastructure. The degree of digitalization is linked to the dependency on ICT infrastructure. Highly digitalized states are less likely to be able to withstand a blow, as the damage on the state's infrastructure would be high. Contrary, a less digitalized state is less dependent on the functioning of national networks that connect the servers of critical infrastructure. As digitalized states are more dependent on ICT's, it can be expected that they develop the cyber capabilities that detect or prevent attacks from hostile servers. Therefore, with an increasing degree of digitalization, states should opt for an offensive cyber posture.

[55] Coburn et al., 'Cyber Risk Outlook 2018', 15
[56] Ehrenfeld, 'WannaCry, Cybersecurity and Health Information Technology', 104
[57] This argument is brought up by Coden and Bartol, 'Our critical infrastructure is more vulnerable than ever. It doesn't have to be that way'

Moreover, the digitalization variable can be considered an amplifier of the offense/defense posture. Depending on whether offense or defense has the advantage, it can be expected that digitalized states make careful considerations of which posture to adopt in order to maximize national security. Whether states with a higher degree of digitalization invest more in offensive cyber capabilities would be a logical consequence of the aforementioned reasons. A detailed analysis on offense/defense advantage follows in the next chapters.

In addition to geography, technology is the second factor that determines the balance. Offense-defense theorists focus mainly on mobility and firepower when scrutinizing the impact of technology on the balance.[58] There is a general agreement among scholars that mobility is more advantageous for the offense than for the defense. The argument is that weapons, which move more quickly and are more agile are able to break through defensive formations and may overcome the geographic advantage of the defender.[59] In contrast, firepower tends to favor the defense for the opposite reasons. The argument is that defenders may stay camouflaged in secure positions while the attacker is more vulnerable due to troop movements.[60]

The concepts of mobility and firepower need adjustments in order to apply them to the cyber domain. Saltzman suggests applying the concept of "versatility" instead of mobility, which "relates to the capacity to technologically attack different types of ICT-based targets at the strategic, operational, and tactical levels."[61] The more system networks of critical infrastructure a state is able to penetrate, the more advantages it has in a cyber conflict. When cyber weapons, in the form of malicious code, are considered as equivalent to traditional weapons, the ability to intrude into a variety of foreign networks applies better than the conventional mobility concept. In this regard, versatility seems to strengthen the offense advantage in cyberspace.

Moreover, Saltzman suggests adjusting the concept of firepower to "byte power". According to her, byte power "relates to the degree of technological damage that can be inflicted on the enemy's ICT-based infrastructure at the strategic, operational, and tactical

[58] See Lieber, 'Grasping the Technological Peace', 78 ibid.
[59] See Glaser and Kaufmann, 'What is the Offense-Defense Balance and Can We Measure it?', 62
[60] Ibid., 64
[61] Saltzman, 'Cyber Posturing and the Offense-Defense Balance', 43

levels."[62] Intrusions alone do not influence the balance. To use malicious code effectively, states need to program it in such a way that it causes the desired damage. Byte power seems to be advantageous for the offense. Innovations in byte power, meaning the ability to exploit a vulnerability with high damage, by definition favor the offense. To use byte power for its own defense, the defending state must gain access to the attacker's network, for which it requires offensive cyber capabilities. A further examination of offensive and defensive capabilities proceeds in the following chapters.

The considerations of the offense-defense theory form the basis of the conceptualization of cyber posture that is used throughout this thesis. Cyber posture is composed of the two elements of capability and state doctrine. The thesis distinguishes between offensive and defensive cyber capabilities. Whereas defensive cyber capabilities refer to preemptive measures taken inside a state's territory on national networks, offensive cyber capabilities means possessing malicious code that could attack foreign networks. Both elements will be discussed in the following chapter.

While capabilities describe the means states possess in their arsenal, doctrine refers to how the state intends to use these means. In other words, capabilities mirror the resources that a state is able to convert into offensive or defensive military strength.[63] This thesis assumes that states are rational actors, developing the capabilities, which fit best to their goal of maximizing security.[64] Therefore, it can be assumed that states not only develop the capabilities that bring most use, but also adopt the posture that maximizes their security. The strategic advantage of capabilities is crucial for a state's cyber posture. Lynn-Jones states that "when there is an offensive advantage, it means that available technologies make it less expensive for states to seek security by adopting offensive military postures and strategies."[65] Accordingly, when defense has the advantage, states invest in defensive capabilities and adopt a defensive posture.

[62] Ibid., 44
[63] This argument is predominantly present in neorealist theories. See for example: Mearsheimer, 'Structural Realism', 78
[64] Keohane, *Neorealism and its critics*, 7
[65] Lynn-Jones, 'Offense-Defense Theory and Its Critics', 674–5

However, the offense-defense balance is merely an indicator that decision makers perceive.[66] States cannot be entirely confident about the advantage of offensive or defensive capabilities. At this point, a state's doctrine comes into play. States adopt their state posture according to how they perceive the offense-defense balance and formulate it in their doctrine.[67] According to the North Atlantic Treaty Organization (NATO), a doctrine is the "fundamental principles by which the military forces guide their actions in support of objectives."[68] Doctrines mirror the intentions on how states seek to use available capabilities and signal to others their military objectives. Accordingly, if the offense is believed to be in the advantage, states most likely adopt an offensive doctrine, whereas a defensive advantage suggests the adoption of a defensive doctrine.

To sum up, this chapter first presented the classical offense-defense balance theory. Second, it translated the logic of the theory into the cyber domain. As geography and technology are crucial for the classical offense-defense balance, the chapter adjusted these factors to the cyber environment. While digitalization was theorized as the cyber-equivalent to geography, byte power and versatility are used equivalent to technology. Accordingly, the offense-defense balance functions differently in the cyber domain. Whereas territorial size matters in the conventional domains, it does not play a role in cyberspace. Projected onto the variable of state size, small and large states are in the same manner vulnerable to cyber-attacks. Instead of territorial size, the degree of digitalization has a larger effect on the offense-defense balance in the virtual domain. Furthermore, whereas geography favors the defense in the conventional domains, digitalization favors the offense. Regarding technology, both byte power and versatility rather favor the offense in cyberspace equally to firepower and mobility in the conventional domains. These assumptions are summarized in the following table.

[66] Van Evera, for instance, underlines the difference between the actual and the perceived offense-defense balance. See van Evera, 'Offense, Defense, and the Causes of War'
[67] Lynn-Jones, 'Offense-Defense Theory and Its Critics', 671
[68] North Atlantic Treaty Organization, 'NATO Glossary of Terms and Definitions', 39

**Table 1: Traditional vs. cyber: factors determining the offense-defense balance and their expected advantage**

| Conventional domains | Advantage | Cyberspace | Advantage |
|---|---|---|---|
| Territory | defense | Digitalization | offense |
| Technology | | Technology | |
| Fire power | defense | Byte power | offense |
| Mobility | offense | Versatility | offense |

Before proceeding to a deeper literature-based discussion on the offense-defense advantage in cyberspace, the following two sub-chapters conceptualizes offensive and defensive cyber capabilities and elaborate their differences. Contrary to the conventional domain, where the distinction between offensive and defensive weapons is often blurred, the following illustrates that cyber weapons are clearer to differentiate than in the conventional domains. In theory, this makes the assessment easier and the security dilemma less acute. Furthermore, examining the technological opportunities in cyberspace helps to understand why a state opts for a certain cyber posture.

### 2.2.2 Offensive cyber capabilities

States with an offensive cyber posture actively develop cyber tools to intrude in a foreign network. To understand a state's offensive cyber posture, this section examines offensive cyber capabilities and scrutinizes how these could be advantageous for states. In this context, two concepts must be distinguished: cyber-attack and cyber exploitation. Lin defines a cyber-attack as " the use of deliberate actions and operations – perhaps over an extended period of time – to alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks or the information and (or) programs resident in or transiting these systems or networks."[69] Cyber-attacks are deployed for destructive purposes to damage another actor's computer system. By contrast, cyber exploitation is "the use of actions and operations – perhaps over an extended period of time – to obtain information that would otherwise be kept confidential and is resident on or transiting

[69] Lin, 'Offensive Cyber Operations and the Use of Force', 63

through an adversary's computer systems or networks."[70] Contrary to cyber-attacks, cyber exploitations do not pursue destruction as the main objective. The attacker attempts to intrude into a network with the smallest degree of intervention, but still enough to obtain useful information. Thereby, it is in the interests of the attacker to keep the intrusion unnoticed.[71]

Both actions require the penetration of another network. In addition, when attacking or exploiting a network the intruder makes use of the same vulnerability in the system.[72] Therefore, it is difficult for the defender to differentiate whether the intrusion takes place to exploit information on a network server or to prepare an attack with a more damaging dimension.

States have various options to intrude into foreign networks. To begin with, offensive cyber operations require vulnerabilities in the system of the adversary. Computer systems have weaknesses, which intruders exploit when penetrating a network. These weaknesses are valuable as long as the defender has not recognized and fixed it. After discovery of a vulnerability, the information is often made public and practitioners can update their systems and install patches to prevent an attack.[73]

The penetration of a foreign computer system requires access to the network. If the target network is connected to the internet, the intruder may reach remote access from his own internet access point. However, states protect their critical infrastructure by creating a network that has no link to the internet. In this case, the infiltration of the computer device takes place either in the programming process of the software, or the intruder gains physical access to the network.[74]

The intruder has different opportunities to penetrate a network and cause damage. Root attacks begin with an intrusion into a network by creating a normal user account. Attackers may additionally seek to gain authority over the network by exploiting system vulnerabilities.[75] Furthermore, probing attacks entail the scanning of particular devices in

[70] Ibid.
[71] Ibid., 82
[72] Ibid.
[73] Ibid., 65
[74] Ibid., 66
[75] Ayala, *Cybersecurity Lexicon*, 166

order to find system vulnerabilities. A common way to gain remote access to a network is to find zero-day exploits. Intruders seek to determine unknown weaknesses in the system software and penetrate the network using viruses, worms or related cyber capabilities.[76] Furthermore, in a denial of service attack (DoS-attack), the attacker sends an enormous number of requests with invalid return addresses. The server waits for authentication approval, which it never receives. The number of requests overstrains the server and leads to server breakdowns.[77]

Once the attacker places malicious code onto a foreign network, the intruder has the control of its activation. Either the intruder programmed the activation of the payload in advance or controls it from outside and activates it at any suitable time. The term payload describes the capacity malicious code can exert after placed in an adversary system. Depending on the infiltration code, the payload can be manifold in its damage. Intrusions may cause damage to data, cause the leak of confidential information or destroy a whole computer network. The objective is often not to destroy the network itself, but to influence the infrastructure that is connected and controlled by the network.[78] These attacks have an indirect effect and are in the most cases not reversible. For instance, a malicious code may cause overheating of a machine or other electronic devices and trigger serious damage. Indirect effects of cyber-attacks are in most cases the main objective of an attacker.[79]

Cyber-attacks reach their target in a short period. Malicious code may cause damage right after being send by the attacker. However, to deploy offensive cyber capabilities and intrude into networks of critical infrastructure, states need to start the operation a long time before it is needed. Launching offensive cyber operations requires preparation. States need time to develop new exploitation tools or discover zero-day vulnerabilities and develop tools that can exploit these vulnerabilities. Additionally, in many states the development and deployment of offensive cyber capabilities requires authorization from political and legal authorities. Therefore, despite the high speed at which an intrusion may take place, cyber operations still depend to a certain extent on human speed. People

[76] Ibid., 179
[77] Ibid., 54
[78] Lin, 'Operational Considerations in Cyber Attack and Cyber Exploitation', 41
[79] Ibid., 38

require time, patience, discipline and advanced technological knowledge to launch cyber operations. Consequently, in order to be prepared for potential conflicts, states must develop cyber capabilities already in peaceful times.[80]

### 2.2.3 Defensive cyber capabilities

This section focuses on defensive cyber capabilities and describes the competencies a state may develop in order to protect its critical infrastructure from outside threats. The section distinguishes between two types of measures that include a defensive cyber posture. The first group of measures are passive defensive. States develop capabilities with the primarily focused on finding vulnerabilities in their own network. The other measure is active defense, in which states develop capabilities to penetrate foreign networks with the purpose of defending their own networks.

In the literature, defensive cyber operations are often best practice guidelines for governments and organizations exploring what to do in order to make networks more secure. Therefore, this section provides an overview of passive defensive measures and dedicates more space to active defense, as it plays a greater role in the context of the offense-defense balance. To begin with, security practitioners share the view that an important component of cyber defense is knowing one's own network. Rob Joyce, head of NSA's Tailored Access Operations team, states that "if you really want to protect your network you have to know your network, including all the devices and technology in it."[81] In addition, security practitioners offer a whole range of preemptive measures that can be deployed in order to protect networks. States may block or blacklist certain entities from sending mail to network servers in order to prevent malicious code.[82] Moreover, keeping the software updated and installing regular patches to fix vulnerabilities in the system, ideally right after security companies release them, makes the system more secure. As is the case with the development of offensive cyber capabilities, defensive measures cost time and resources. Especially when the network connects critical infrastructure, updates must be proven in order not to reset important settings.[83] Furthermore, monitoring user

[80] See for example: Buchanan, *The Cybersecurity Dilemma*, 42
[81] Joyce, 'USENIX Enigma 2016—NSA TAO Chief on Disrupting Nation State Hackers'
[82] Ayala, *Cybersecurity Lexicon*, 41
[83] Buchanan, *The Cybersecurity Dilemma*, 54

accounts and deleting access and accounts of former employees reduces opportunities for intruders to penetrate a network.[84]

Moreover, defensive cyber measures include the deployment of intrusion prevention systems, which detect suspicious activities and hinder them from reaching their target. Network security monitoring is the "collection, analysis and escalation of indications and warnings to detect and respond to intrusions."[85] Monitoring does not prevent attackers from entering the network, but rather hinders them from achieving their objectives. It has a clear defensive character. Due to the constant development of innovations, system firewalls are never completely secure. Technological innovations offer intruders new opportunities to penetrate a network. Network security monitoring prevents intruders from completing their mission and achieving their goals.[86] It is often managed by computer security incident response teams (CSIRTs) or computer emergency readiness teams (CERTs). A CERT is a "group of individuals usually consisting of Security Analysts organized to develop, recommend, and coordinate immediate mitigation actions for containment, eradication, and recovery resulting from computer security incidents."[87] States invest in CERTs to be prepared for the moment when intruders attempt to penetrate their network. In recent years, collaboration between CERTs of different states has increased. Sharing information is of high value in the cyber domain. CERTs that identified a threat or system vulnerability share their knowledge with allied states to prevent damage or exploitation of their networks.[88] The earlier a state knows about a vulnerability in its system, the less likely hostile intruders can use this system error to execute an attack.

In contrast to passive defensive capabilities, active defense includes the intrusion into foreign networks in order to prevent the intruder from causing damage to the network. In the literature, there are different conceptualizations of the active defense concept, depending on whether it is applied to organizations and companies or to nation states.[89] According to Graham, "active defenses consist of electronic countermeasures that attack

[84] Ibid., 55
[85] Bejtlich, *The practice of network security monitoring*, 4
[86] Ibid., 5
[87] Ayala, *Cybersecurity Lexicon*, 36
[88] An overview of the role of CERTs see: Skierka et al., 'CSIRT Basics for Policy-Makers'
[89] For an organization-based approach to active defense see: Denning and Strawser, 'Active Cyber Defense: Applying Air Defense to the Cyber Domain'

an aggressive computer system, immobilizing that system and thus halting the cyber-attack."[90] Active defense is used as a pre-emptive measure to prevent destructive cyber-attacks. States attack hostile servers right after their networks have been penetrated. This concept plays a significant role in the discussion of offense-defense theory, as it blurs the distinction between offensive and defensive cyber posture. At this point, the dilemma of interpretation comes into play. States may develop offensive capabilities with defensive intentions. Defensive realism assumes that security-seeking states develop weapons for their own protection. However, how can a state know that a potential adversary is developing offensive weapons for active cyber defense and not for offensive attacks?[91] Active defense requires the same offensive capabilities that are necessary when intruding into foreign networks with offensive intentions. Thus, states possessing offensive capabilities are already potential aggressors.

Another aspect that deserves consideration is that "fully maximizing network security necessitates intrusion into the networks of other actors."[92] By intruding into foreign networks, states gather information they need to protect their own network and prevent potential attacks. These defensive-minded intrusions are only feasible because of the possibility to conduct operations that are covert and difficult to attribute. In the conventional domains, placing military forces on adversary's territory would obviously violate a state's sovereignty and causes conflict. Even an invasion for defensive purposes would most likely result in an escalation.[93]

Finally, active defense in the sense of "hacking back" could hit innocent actors whose device has been abused. Hostile states can launch their attack from devices that are located in a third country. An accurate investigation that guarantees reliable evidence would be time-consuming and expensive.[94] Therefore, Jeffrey Carr underlines that "technological limitations will place states in a position where a timely decision to use active defenses requires states to decide to use them with imperfect knowledge."[95]

---

[90] Graham, 'Cyber Threats and the Law of War', 92
[91] This question has been extensively debated in the security dilemma theory. See e.g.: Jervis, 'Cooperation under the Security Dilemma', 207.
[92] Buchanan, *The Cybersecurity Dilemma*, 64
[93] Ibid., 72–3
[94] Graham, 'Cyber Threats and the Law of War', 92
[95] Carr, *Inside Cyber Warfare*, 68

To sum up, a crucial part of the conceptualization of offense/defense cyber posture is whether states develop offensive or defensive cyber capabilities. The two sub-chapters examined the differences between offensive and defensive cyber capabilities. While cyber weapons are clearer distinguishable than conventional weapons in the traditional domains, the intentions of their use are blurred. Those states having the technical skills to conduct a cyber-attack can use them, whether for offensive or defensive purposes. Therefore, active defense defined as the ability to hack-back after becoming victim of an intrusion is considered as an offensive capability in the technical sense. However, the intentions of a state matter. Thus, the state's doctrine and cyber strategy, the second component of cyber posture, provides insight into how and under which circumstances offensive cyber capabilities can be deployed.

The previous two sub-chapters elaborated the question of the offense-defense theory, namely whether offensive and defensive weapons are distinguishable. The next chapter is devoted to the question of whether the offense or the defense has the advantage in cyberspace. A literature-based comparison of different assumptions illustrates that answering this question is by no means simple.

### 2.2.4 Discussing offense-defense cyber advantage

This thesis argues that the offense-defense balance variable is a crucial factor that may have great influence on a state's cyber posture. If offense or defense is in the advantage, states are likely to opt for it in order to maximize their security. Structural realists mainly use the offense-defense balance in order to understand the outbreak of wars and conflict.[96] The following section scrutinizes the advantages of offensive and defensive capabilities not with the aim to understand when conflict in cyberspace is more likely, but rather to understand the reasons behind a states offensive/defensive cyber posture. In other words, the cyber offense-defense balance is used as a variable to explain cyber posture rather than conflict. Whether an offensive cyber posture leads to conflict is a different question that is not elaborated in this research. Certainly, the offense-defense balance is not the only variable that explains posture. However, under the assumption that states act rationally, it can be expected that they mirror the offense-defense balance in their posture.

[96] See for example: van Evera, 'Offense, Defense, and the Causes of War'

In the literature, most of the scholars, journalists and security practitioners argue in favor of an offense advantage in cyberspace.[97] Many assessments focus on the technological component of cyberspace. Joseph Nye, for instance, highlights that "the internet was designed for ease of use rather than security, [and therefore] the offense currently has the advantage over the defense."[98] However, he adds that this advantage can change when cyber security systems become stronger.[99] Lieberthal and Singer argue in the same vein. To their mind, most systems and products were programmed to facilitate the flow of information rather than focusing on security issues. Additionally, they point out that in order to patch vulnerabilities and update systems, defenders rely on intruders who seek to penetrate their network. Only then can defenders investigate and fix system vulnerabilities.[100]

In line with the majority view, this thesis argues that offense has the advantage in cyberspace. This would suggest that states as rational actors rather invest in offensive cyber capabilities. However, to contrast this consideration, the following section delivers arguments for the opposite. The aim is to illustrate that the offense-defense balance in cyberspace faces the same problem of defining the offense/defense advantage as in the traditional domains.

A smaller group of authors challenges the assumption of an offense-dominated cyberspace.[101] Firstly, they criticize the absence of empirical evidence that proves the offensive advantage. Furthermore, when evaluating the offense-defense balance, adherents of the defensive advantage often include more than only the technological component into their assessment.

Their theoretical arguments are often based on a cost-benefit analysis and highlight the enormous cost of an offensive cyber operation. Monte, for instance, indicates that "breaking into a particular network may be cheap after the tools and infrastructure are in place," but "building and maintaining the infrastructure for a program of sustained operations requires targeting, research, hardware engineering, software development, and

[97] Aquilla, 'Cyberwar Is Already Upon Us'; ibid.
[98] Nye, *Cyber Power*, 5
[99] Ibid.
[100] Lieberthal and Singer, 'Cybersecurity and U.S.-China Relations', 14
[101] See for example: Lindsay, 'Stuxnet and the Limits of Cyber Warfare' and Rid, *Cyber war will not take place*.

training."[102] The costs occur in the preparation process. There is no empirical evidence that the cost-benefit ratio of financial resources and offensive capabilities is lower than the ratio of financial recourses and defensive capabilities.

Rid, for instance, highlights three reasons why the offense does not necessarily have the advantage in cyber conflict. Firstly, he points out that "the better the protective and defensive setup of complex systems, the more sophistication, the more resources, the more skills, the more specificity in design, and the more organization is required from the attacker."[103] Secondly, he notes that offensive cyber capabilities are often programmed for a specific vulnerability in target system. A repeated application of the same code is unlikely, as other system have different configurations. Moreover, once the defender patched the vulnerable entry point, the code seems to be useless.[104] Accordingly, Gartzke remarks that cyber-attacks are "use and lose" capabilities.[105] Thirdly, an increasing number of security companies attempt to find system vulnerabilities, which increases the difficulty to find entry points. During the last years, the public and private sector recognized the threat that endangers their digital infrastructure and hire security companies to secure their networks. The more security companies attempt to identify vulnerabilities, the more difficult it becomes for attackers to intrude a network.[106]

Additionally, Richard Clarke, a former National Coordinator for Security, Infrastructure Protection and Counter-terrorism for the United States, develops the argument to invest first in cyber defense before focusing in the offense. To his mind, a credible defense strategy is necessary to protect its critical infrastructure in the first place. Developing a strike-first strategy, which includes the immediate destruction of threats, is complicated in cyberspace, as the threat can come from every server in the world.[107] Moreover, Clarke highlights that defenders do not simply identify the vulnerability once they became victim of a cyber exploit. They also analyze the malicious code and program patches to become

[102] Monte, *Network attacks and Exploitation*, 56
[103] Rid, 'Cyber War Will Not Take Place', 28
[104] Ibid.
[105] Gartzke, 'The Myth of Cyberwar', 60
[106] Rid, *Cyber war will not take place*, 169
[107] Clarke and Knake, *Cyber war*, 78

resistant for future attacks. Although updating all systems is costly and burdensome, states at least patch their critical infrastructure, which defuses the potential of the threat.[108]

A comparison of different views on offense/defense cyber dominance demonstrates that even though most of the scholars assume an offense advantage, the debate is by no means settled. When it is difficult to determine whether offense or defense is advantageous in cyberspace, can the offense-defense balance serve as a suitable variable to explain cyber posture? This thesis argues that it can. States not only adopt an offensive/defensive cyber posture according to what the *actual* offense-defense balance indicates, but rather adjust their posture according to what they *perceive* as being advantageous. In other words, in the frame of the theory, when all states are similarly rational actors and perceive an offensive advantage in cyberspace, all states would deploy offensive capabilities and adopt an offensive cyber posture to maximize their security. On the contrary, when states perceive an advantage on the defense, they would accordingly focus on defensive capabilities and opt for a defensive posture in cyberspace. Admittedly, this radical theoretical conclusion does not necessarily reflect empirically observable behavior at all time, as states are not always rational actor and other factors could influence a state's cyber posture. However, in line with neorealist assumptions and following the majority view of an offensive advantage in cyberspace, it can be expected that states adopt an offensive cyber posture.

Furthermore, offense or defense cyber posture must be understood as a tendency rather than an either/or choice. To secure itself from cyber threats, every state needs defensive cyber capabilities. Without having network protection in place, states are exposed to a much larger number of threat actors. When network systems are not secure, even attackers with limited knowledge are able to intrude critical networks and cause danger to a state's infrastructure. On the other hand, every state possesses a certain amount of offensive cyber capabilities. As discussed above, offensive cyber capabilities involve merely possessing the knowledge to intrude into foreign network systems to place malicious code that could cause harm to a state's critical infrastructure. When deploying defensive measures (e.g. network monitoring), states gain knowledge of vulnerabilities, which could be used for their advantage to attack other systems, in which the entry point has not

[108] Ibid., 89

been patched. Therefore, cyber posture includes not only the offensive or defensive capabilities a state possesses in its arsenal, but also doctrine, namely the declaration in which it expresses the intention to make use of these capabilities. Consequently, states with an offensive cyber posture develop offensive cyber capabilities and formulate in their doctrine under which conditions they seek to use them. Contrary, states with a defensive posture invest their financial resources in defensive cyber capabilities and accordingly disclose it in their doctrine.

Moreover, the variation in posture raises the question of whether state size makes a difference in cyber posture. During the last years, journalists have extensively published incidents of state-to-state cyber-attacks, in which mostly powerful states, such as the USA, China and Russia are in focus.[109] Is the development of offensive capabilities a trend of great powers to increase their influence in world politics or are small states likewise involved in this trend? Is cyber offense-defense theory helpful to understand cyber posture of small states? Conventional offense-defense theory does not make distinction between small and large, but predominantly focuses on powerful states.

The following chapter scrutinizes small state's security characteristics and discusses them in light of the offense-defense theory. The identified factors that influence the cyber offense-defense balance, namely the degree of digitalization and technology characterized as versatility and byte power, form the basis of the analysis. The chapter scrutinizes how state size features matter for these factors and whether they make a difference in cyber posture.

### 2.3 Small states and the offense-defense balance in cyberspace

This chapter examines how features that determine the offense-defense balance effect small states in cyberspace. First, the chapter outlines the approach used for this thesis to differentiate between large and small states. Next, it discusses key characteristics of the

[109] The Center for Strategic and International Studies lists the major cyber incidents distinguishing between offender and victim state. See Center for Strategic and International Studies, 'Significant Cyber Incidents Since 2006'

security behaviour of small states in the traditional domains and theorizes them in cyberspace. The aim of this section is to outline a conceptual framework in order to explain small state's cyber posture and give answer to the main question of how state size shapes cyber posture of states.

International Relations literature provides wide range of approaches on how to group states according to their size. The variety of approaches, reaching from quantitative, qualitative, relational and self-perceptional attempts to categorize state size, points to the complexity of applying this concept and inferring sophisticated hypotheses. However, a deeper discussion on how to differentiate between small and large goes beyond the scope of this thesis. In accordance with neorealist theory, it is sufficient to focus on material characteristics and define smallness in absolute terms using quantitative criteria. Accordingly, and in line with the offense-defense theory, the conceptualization of state size used in this thesis rests on a structural realist approach.

To begin with, attempts at conceptualizing state size in absolute terms often include the following criteria: size of the territory, population size, economic activity, and the level of military capacity.[110] Even though these criteria seem clear and easy applicable, it remains a matter of debate to what extent a state needs to fulfill the criteria in order be regarded as small or large.[111] However, it seems reasonable that structural realists conceptualize state size in terms of power. The elusive concept of power encompasses the ability of states to shape the outcome of international events. While large states have a great influence on international decision-making, small states are rather objects of great power politics than active subjects reliant on great power politics. To operationalize power, the approach typically includes countable scales such as the number of weapons, soldiers or the total gross domestic product (GDP) to determine the economic strength of a state.[112]

[110] See for example: East, 'Size and Foreign Policy Behavior: A Test of Two Models', 557
[111] For a discussion on this matter, see Wivel et al., 'Setting the scene: small states and international security', 6
[112] Browning, 'Small, Smart and Salient?', 670

Following from the conceptual distinction between small and large states, the literature illustrates the challenges that small states face.[113] The following section points out these challenges and critically examines smallness against the background of the offense-defense theory. First, the primary goal of survival is more acute for small states than for larger powers. In an anarchic international system, small states constantly need to adjust their security strategy according to the decisions of larger powers.[114] Furthermore, small states have a smaller "margin of error" when organizing their national security strategy. While large states do not directly risk their survival when testing security strategies, wrong security decisions may have existence-threatening effects on small states.[115] Regarding state posturing, the small margin of error and financial constraints suggest that small states are more sensitive to the offense-defense balance. Small states need to take wise decisions on their posture, as mistakes can have a much higher impact. For posturing one could therefore expect that small states' postures correspond more closely to the offense-defense balance.

Second, small states react instead of shaping the structure of the international system. The asymmetric distribution of power reduces opportunities to gain security goals using military means. Entering into conflict with a powerful adversary may have existentially threatening consequences. In this vein, Mearsheimer theorizes that "the bigger the gap in power between any two states, the less likely it is that the weaker will attack the stronger".[116] Accordingly, Glaser and Kaufmann consider asymmetric power differences when outlining the offense-defense balance. On the one hand, small states may overcome the size disparity when the defensive advantage of the balance is large. The security of a state increases with the advantage of the defense. In other words, aggressors may need to invest multiple times more into the offense in order to overcome the defensive advantage. On the other hand, the power disparity of states can be so different that "even if defense has a large advantage, a much wealthier attacker might still be able to outspend a defender by a sufficient margin to gain an effective offensive capability."[117] To conclude, the

[113] Some authors oppose to draw a distinction between small and large state's security behavior, arguing that both pursue the same goal of survival and security. See e.g. Lamoreaux, 'Acting small in a large state's world'
[114] See for example: Thorhallsson and Steinsson, 'Small State Foreign Policy', 4–5
[115] Waltz, *Theory of International Politics*, 194–5
[116] Mearsheimer, *The Tragedy of Great Power Politics*, 33–4
[117] Glaser and Kaufmann, 'What is the Offense-Defense Balance and Can We Measure it?', 51

assumptions suggest that small states rather opt for a defensive security posture, especially when the advantage of offense/defense is not clearly visible.

Having said that, how do conventional offense-defense factors influence small states? Regarding geography and technology, both factors apply in the same way for small and large states. However, a brief illustration of how these factors affect small states is necessary in order to examine the same logic in the cyber domain. First, in conventional offense-defense theory, geography gives advantage to the defense. In the same way as large states, small states on islands or surrounded by mountains are more secure than others are. Thus, the geographic factor has the same defensive effect on both small and large states. Accordingly, when geographic obstacles give an advantage to their security, small states are expected to opt for a defensive posture.[118]

Second, as illustrated above, technology in terms of mobility and firepower gives advantage to both offense and defense. The development of military technology is an investment in capabilities. Small states lack the resources to invest in the newest military capabilities. Depending on whether offense or defense has the advantage, small states seek to maximize their security with the lowest costs and highest benefits and adopt their posture accordingly. In this regard, the technology variable has a similar effect on both small and large states.

The application of the offense-defense balance to small states must be considered with caution. The theoretical assumptions indicate that the variables can be applied to small states in the same manner as to large states. This raises the question of whether it is useful to distinguish between small and large when applying the offense-defense balance. Certainly, it makes sense when looking at the balance in general. Small states are more sensitive to the offense-defense balance and therefore have not much leeway when determining their posture. The reasons are not the factors of the offense-defense balance, but rather the size of the state itself.

Moreover, even though the advantage is on the offense, small states need to overcome the power asymmetry to their potential aggressors. Would a small state attack another state in order to increase its security? An explanation for a small state's offensive posture could

[118] Indeed, due to the small territorial size, small states are overall an easier target, as powerful states do not need much effort to take control over small state's territory.

be that small states attack in order to pre-empt or to deter potential invaders. However, using this mean of last resort would imply that the small state has already given up its primary goal of survival. These abstract considerations concern a state dyad with asymmetric power distribution. When the dyad consists of two states of the same size, the offense-defense balance seems to have a greater impact on state posture, as rather factors such as technology and geography play a role instead of unequal distribution of power. To conclude, the asymmetric distribution of power seems to supplant the offense-defense balance variable in terms of explaining state posture.

These conventional assumptions of the small state literature illustrate the general argument that small states act differently than large states.[119] The following section examines whether the unique characteristics of cyberspace makes small states behave like large states regarding their cyber posture, or in any case differently from what the conventional small state's literature assumes. Trying to establish the cyber posture of small states, the aim of this section is to connect the tendencies of small state security policy to offense-defense theory and question why states opt for an offensive/defensive posture. What kind of behavior is to be expected when thinking about the security of small states regarding their offensive and defensive capabilities?

Overall, the thesis argues that the logic of a cyber offense-defense balance applies in the same manner to small states. First, when it comes to the sensitivity of small states towards the offense-defense balance, it can be expected that small state's cyber posture mirror more closely the offense-defense balance, as they face the pressure of recourse constraints and margin of error similarly in the cyber and the traditional domain.

Second, as theorized in the previous sections, the factor of digitalization applies in the same manner to small and large states. In contrast to the traditional domain, where geography rather favours the defense, in the digital domain small and large states are in the same way vulnerable to cyber-attacks. Small and large states choose the degree of digitalization by themselves and can adjust their cyber posture accordingly. Therefore,

[119] Some authors oppose to draw a distinction between small and large state's security behavior, arguing that both pursue the same goal of survival and security. See e.g. Lamoreaux, 'Acting small in a large state's world'

the degree of digitalization does not seem to indicate a difference in small or large states cyber posture.

Third, it can be even expected that small states use the cyber domain to balance their structural disadvantage of being small. Areng, for instance, argues that small states may increase their influence in the international arena developing "cyber power". The development of information and communication technology requires qualitative personnel instead of quantitative military forces, which give advantage to small states and make warfare more equally. In this regard, Areng notes that "cyber means are planned and used as an effective force multiplier, an enhancement for traditional means or as a stand-alone capability that can give substantial asymmetric advantage to states that are considered weaker in terms of traditional combat power."[120]

When theorizing the offense-defense balance in cyberspace on small states, the illustrations above indicate that the factors determining the balance apply in the same manner to small and large states. Accordingly, when the majority suggests an offensive advantage in cyberspace, it can be expected that small states similarly adopt an offensive posture in cyberspace. However, these considerations are vague and reflect only the behaviour of small states in the offense-defense discussion. In the previous chapter, the debate on whether offense or defense has the advantage in cyberspace underlined that even though the majority of authors assume an offensive advantage, the issue is by far not clear.

In a small-large comparison, this research assumes that powerful states still mirror the offense-defense balance, but can afford to ignore it to a certain extent for the following reasons. First, they are by definition wealthier and can afford the development of offensive capabilities that may increase their security. Adopting an offensive cyber posture makes sure that they are on the safe side to protect their critical infrastructure. Consequently, possessing financial resources suggests that large states are less reliant on the offense-defense balance. Even without having a clear picture of what the offense-defense balance suggests to adopt, large states have the resources to invest in both capabilities.

[120] Areng, 'Lilliputian States in Digital Affairs and Cyber Security', 6

Second, large states pursue different aims and ambitions. While survival is still their primary goal, they also aim security through hegemony. States compete with each other in gaining ultimate power. Mearsheimer argues that "the desire for more power does not go away, unless a state achieves the ultimate goal of hegemony"[121]. To achieve this aim, large states require offensive cyber capabilities not only for the purpose of defending, but also for gaining superiority in the cyber domain. This underlines the expectation that powerful states rather opt for an offensive cyber posture.

Furthermore, in accordance with the majority of an offensive advantage in cyberspace, small states are expected to adopt an offensive cyber posture. The factors determining the balance apply to small states in the same manner as to larger powers. Small states might even become more active regarding the development of offensive cyber capabilities in order to decrease their asymmetric security advantage. These assumptions suggest that that the effect of state size is low. It is expected that small and large states act similarly in the cyber domain. The next chapters test these assumptions empirically.

[121] Mearsheimer, *The Tragedy of Great Power Politics*, 2

## 3 Methodology

The previous chapters theorized state posture in the traditional and cyber domain against the background of the offense-defense theory. In terms of method, the empirical part makes use of a comparative analysis of two cases, the United Kingdom and the Estonian Republic. The research employs a most similar systems design (MSSD) to scrutinize how state size influences the cyber posture of states.[122]

Cyber posture is the dependent variable of this thesis. The variable is dichotomous taking the value offensive or defensive. The offensive or defensive nature of a state's cyber posture is established by analyzing the character of (a) doctrine, and (b) capabilities. A posture is considered offensive, when the doctrine emphasizes the intentions to deploy offensive code to intrude into foreign networks and when the state possesses offensive capabilities to carry out such offensive operations. In contrast, a posture is considered defensive when the doctrine highlights only measures that focus on the security of national networks rather intruding into foreign systems.

To determine the offensive or defensive posture of a state regarding its doctrine, this research analysis cyber security strategies, annual security reviews, public speeches by security officials, and statements published by governmental institutions with the aim to identify terminology reflecting offensive or defensive thinking. For example, when "offensive capabilities" or "ability to attack first" is referred to with the intention to intrude into foreign networks, the thesis assumes that a state adopts an offensive posture. In contrast, the terms "network management", "updating systems" and "analyzing cyber threats", which refers to actions taking place only inside national networks, are presumed to suggest the cyber posture to be rather defensive. While it is difficult to quantify the precise degree of offensive and defensive posturing, the analysis of the cyber doctrines is sufficient to establish the overall character of a state's cyber posture.

In addition to doctrine, the thesis assesses the capabilities that a state is able to deploy. To complement doctrine, capabilities indicate what the state is actually capable of doing. An offensive doctrine alone is not yet an offensive posture. Doctrine needs to be underpinned with matching capabilities. In order to measure whether a state has offensive

[122] This thesis makes use of the MSSD as outlined by Gerring. See: Gerring, *Case study research*, 131–3

cyber capabilities, the thesis identifies (a) whether offensive measures are part of repertoire of state and (b) whether a state outlines scenarios for offensive deployment. Regarding sources, establishing the presence of offensive cyber capabilities represents a challenge. Most of the information is confidential and kept in secret for the public, this thesis relies on cyber security reviews, official statements and the budget that has been spend for cyber security purposes in order to identify the nature of capabilities a state develops. Even though the sources do not allow for precise measurement, they are sufficient for this thesis to establish the presence or absence of offensive capabilities.

The independent variable of this thesis is state size. Being aware of the conceptual challenge to differentiate between small and large states (see chapter 2.3) this thesis nevertheless defines state size as a dichotomous variable. Accordingly, states are classified as being small or large. In order to measure state size, the thesis relies on the neorealist approach, which takes the size of territory, population size, economic strength, and the level of military capacity into account.[123] This thesis operationalizes state size relying on the data of the World Bank country profiles[124] and the Military Expenditure Database created by the Stockholm Peace Research Institute.[125]

The UK is with a population of over 66 million the third biggest country in the European Union and belongs to the 25 population riches countries in the world.[126] Even though the UK is in a global comparison relatively small regarding its territorial size, it has political and economic influence all over the world due to its colonial legacy. In addition, the UK is a permanent member of the United Nations Security Council and in the group of the seven largest economies in the world (G7). With a nominal GDP of more than USD 2.6 trillion (nominal)[127], the UK belongs economically to the most powerful states in the world. Furthermore, the UK had an annual military expenditure of 47 billion dollar in 2017[128], which the second highest in the European Union after France. At least in a

[123] Browning, 'Small, Smart and Salient?', 670
[124] World Bank Country Profiles: https://data.worldbank.org/country
[125] Military expenditure taken from the SIPRI Military Expenditure Database from the year 2017: https://www.sipri.org/databases/milex.
[126] Population United Kingdom - World Bank Open Data (2017): https://data.worldbank.org/.
[127] Nominal GDP United Kingdom - World Bank Open Data (2017): https://data.worldbank.org/.
[128] Military expenditure taken from the SIPRI Military Expenditure Database from the year 2017: https://www.sipri.org/databases/milex.

regional scale, the figures illustrate that the United Kingdom can be considered as a large state.

In contrast, the Estonian Republic belongs to the group of the smallest states in the world. With a population of slightly above 1.3 million, Estonia is the fourth smallest country in the European Union after Malta, Luxembourg and Cyprus.[129] Estonia has a GDP of almost USD 26 billion (nominal), which is among the smallest economies in the European Union.[130] Finally, the military expenditure of Estonia was slightly above 536.3 million, which was more than 2 percent of the GDP, but still among the lowest in the European Union.[131] This qualifies Estonia being a small state.

As Gerring describes for MSSD, "the chosen pair of cases is similar in all respects except the variable(s) of interest"[132], in this case state size. Other potentially relevant factors are regime type, alliance membership, the degree of digitalization including e-infrastructure dependency, information and communication technology development and the level of cybersecurity. These factors are comparable in both cases. For example, regarding regime type, both are full democratic states[133], members of the European Union, and members of NATO.

Important with regard to cyber posturing, both states are on a similar level of digitalization. To operationalize the broad concept of digitalization and the level of e-infrastructure dependency, the thesis includes the e-Governance Index published by the Department of Economic and Social Affairs of the United Nations.[134] The index is composed of the Telecommunication and Infrastructure Index, the Human Capital Index and the Online-Service Index. It indicates the preparedness of government institutions to offer public services using ICTs. As theorized in the previous part, the thesis assumes that an increase in the degree of digitalization rises the dependency on ICTs and makes society more vulnerable to cyber-attacks.

[129] Population Estonia - World Bank Open Data (2017): https://data.worldbank.org/
[130] Nominal GDP Estonia - World Bank Open Data (2017): https://data.worldbank.org/
[131] Military expenditure taken from the SIPRI Military Expenditure Database from the year 2017: https://www.sipri.org/databases/milex.
[132] Gerring, *Case study research*, 131
[133] Democracy Index 2017 created by The Economist Intelligence Unit: https://infographics.economist.com/2018/DemocracyIndex/
[134] United Nations, 'E-Government Survey 2018'

Estonia offers a whole range of public services to its citizens, which include digital identification and signing of documents, electronic tax declaration, online medical prescriptions and internet voting. Ninety-nine percent of the public services are available online. The decentralized Estonian information system (X-Road), connecting government authorities and companies with each other, guarantees a secure and fast exchange of data saving labor and time and creates transparency in the relation between state and citizen.[135]

In the same way, the United Kingdom is among the leading countries delivering public online services to its citizens. Since 2012, the online platform gov.uk is the countries single point of access to online services and combines services from all government authorities. Currently, UK citizens can obtain 780 public services online.[136] The figures in table 2 illustrates that both states are very highly committed to offering public services using ICTs.

**Table 2: E-Government Development Index (EGDI) 2018[137]**

| | **EDGI** | **EGDI-rank** | **EGDI-level[138]** |
|---|---|---|---|
| United Kingdom | 0.8999 | 4 | Very high |
| Estonian Republic | 0.8486 | 16 | Very high |

The concept of information technology development describes the progress of a society in developing and adopting ICTs. Online public services increase dependency on e-government structures and the cyber domain in general. This thesis utilizes figures from the ICT Development Index[139] to demonstrate the similarity of the two cases. The index is composed of three indicators: ICT infrastructure and access, ICT usage and ICT skills and includes indicators such as the proportion of households with internet access, proportion of people using the internet and education parameters.[140] In various aspects, the indicators are similar to the e-Government Index. However, as the figures are merely

[135] For an overview of Estonia's digital ecosystem see on Vassil, 'Estonian e-Government Ecosystem: Foundation, Applications, Outcomes', 12
[136] For more information and statistics, see: https://www.gov.uk/performance/services.
[137] United Nations, 'E-Government Survey 2018', 86–9
[138] The index distinguishes between four categories: very high (greater than 0.75), high (between 0.50 and 0.75), middle (between 0.25 to 0.50) and low (less than 0.25).
[139] International Telecommunication Union, 'Measuring the Information Society Report 2017'
[140] For methodological procedure see: International Telecommunication Union, 'The ICT Development Index (IDI): conceptual framework and methodology'

considered to show similarities between the two cases regarding their advanced stage in adopting ICTs, there is no need for a more detailed analysis of the parameters.

Table 3 illustrates the advancement of the UK and Estonia in the field of ICT-development. Both belong to the group of the 15 most advanced states in the world, measured by fixed and mobile telephone subscriptions, international internet bandwidth and percentage of households with computer and internet access.[141]

**Table 3: ICT-Development Index (IDI) 2017**[142]

| | **IDI value** | **IDI rank** |
|---|---|---|
| United Kingdom | 8.65 | 5 |
| Estonian Republic | 8.14 | 14 |

Finally, the study includes the level of cyber security in order to examine the commitment to cybersecurity of both cases. By doing this, it includes the Global Cybersecurity Index (GCI)[143], which measures the engagement on cybersecurity in the following five pillars: legal, technical, organizational, capacity building and cooperation. Accordingly, it classifies states into three GCI tiers: initiating, maturing and leading. The index does not provide answers to the level of security of a specific state, but captures how well positioned states are regarding their cyber security.

Both the UK and Estonia are highly committed to improving their cyber security regarding organizational coordination and policy structure, technical security support, existence of legal structures, capacity building and cooperation and information sharing. In the ranking of all 192 UN member states, the UK and Estonia are ranked among the highest.

[141] Ibid.
[142] International Telecommunication Union, 'Measuring the Information Society Report 2017'
[143] International Telecommunication Union, 'Global Cybersecurity Index (GCI) 2017'

**Table 4: Global Cybersecurity Index (GCI) 2017[144]**

| | GCI score | GCI rank |
|---|---|---|
| United Kingdom | 0.783 | 12 |
| Estonian Republic | 0.846 | 5 |

To conclude, the illustrations above demonstrate that while the UK and Estonia are different in size, both are otherwise similar with regard to a range of potentially relevant features such e-government, ICT development and commitment to cyber security. The following section focuses on the cyber posture of both states separately before comparing both in a detail.

[144] Ibid.

## 4 Comparing the cyber posture of a large and a small state

The following part of this thesis assesses whether difference in state size is reflected in the cyber posture of state. First, the following sub-chapters scrutinize doctrine and capabilities of the United Kingdom and Estonia. The aim is to identify the overall cyber posture in order to assess whether the empirical evidence coincides with the theoretical assumptions stated in the previous part.

### 4.1 Cyber Posture of the United Kingdom

#### 4.1.1 Cyber doctrine

Every five years the British government publishes an updated National Cyber Security Strategy, in which they outline their approach to cyber security and how to tackle cyber-related risks.[145] These papers not only highlight priorities and values regarding UK's behavior in the cyber domain but also formulate the aims and ambitions to achieve the goal of securing individuals, companies and government institutions. The following section reflects the first two cyber security strategies by focusing on the UK's stance regarding the deployment of offensive and defensive cyber capabilities. Next, this section scrutinizes the most recent cyber security strategy in order to determine whether the offensive/defensive tendency of the previous strategies has been carried over to the most recent one and whether the UK cyber posture can therefore be considered offensive or defensive in terms of doctrine.

In June 2009, the United Kingdom published its first cyber security strategy. The government recognized the significance of the cyber domain for individuals, companies and government institutions and therefore published the Cyber Security Strategy as an addition to the existing National Security Strategy.[146] The paper provides a general overview of how UK understands cyberspace and identifies the threatening actors. Beside criminals and terrorists, states are regarded as "the most sophisticated threat in the cyber

[145] British Government, 'National Cyber Security Strategy 2016-2021', Cabinet Office, 'The UK Cyber Security Strategy' and British Government, 'National Cyber Security Strategy 2016-2021'
[146] Cabinet Office, 'Cyber Security Strategy of the United Kingdom 2009-2011', 14

domain"[147] due to their ability "to exploit computers and communications networks to gather intelligence on government, military, industrial and economic targets, and opponents of their regimes"[148]. Furthermore, the strategy points out UK's aims to use the cyber domain for their advantage in the fight against criminals, terrorists, and in military conflicts. Even though the strategy does not name the deployment of offensive cyber capabilities, taking the advantage entails to "cover the full range of possible actions that the UK might need to take (…) in order to support cyber security and wider national security policy aims."[149] In this regard, to "intervene against advisories"[150] is an explicit action that the strategy mentions.

In this sense, the UK acknowledges "the need to develop military and civil capabilities, both nationally and with allies, to ensure we [the British government] can defend against attack, and take steps against adversaries where necessary."[151] An indication of what entails these steps are not further elaborated. However, the strategy reveals that the UK seeks to become a powerful player in the cyber domain by using the advantages of cyber capabilities also for strategic warfare. Thus, cyber capabilities are not strictly for defensive purposes alone. The UK seems to reserve the right to use these tools to pursue its wider strategic aims.

Two years later, in November 2011, the UK published the second National Cyber Security Strategy (NCSS 2011), which entails a more detailed view on how the government seeks to secure the cyber domain.[152] The strategy determines a whole range of cyber threats and outlines how to approach these. The measures used in order to defend critical infrastructure are rather defensive. For instance, the government attempts to "improve (…) detection and analysis of sophisticated cyber threats"[153], "enhance (…) capability to defend against and deter high-end, state-sponsored threats"[154] and "exchange information with the private sector on the risks emerging from cyberspace"[155]. However, at one point

[147] Ibid., 13
[148] Ibid.
[149] Ibid., 15
[150] Ibid., 16
[151] Ibid., 14
[152] Cabinet Office, 'The UK Cyber Security Strategy'
[153] Ibid., 26
[154] Ibid.
[155] Ibid., 18

the government states to "take a more proactive approach to tackling cyber threats"[156]. Whether the proactive approach includes the deployment of offensive capabilities remains unclear. The strategy only indicates that the (Government Communications Headquarters (GCHQ) "(…) has some world-class skills at its disposal"[157], which relate to the espionage capabilities of the British agency rather than efforts to take an offensive stance in cyberspace.

Crucial for this thesis is the Cyber Security Strategy 2016-2021, which reflects the most recent plans and developments in how the UK copes with cyber threats. Overall, the strategy outlines a range of defensive measures in order to ensure the security of national networks, which suggest that the UK invests predominantly in defensive cyber capabilities. However, the strategy highlights the government's plans to adopt an Active Cyber Defense (ACD) program. According to the strategy, active defense is defined as the "principle of implementing security measures to strengthen a network or system to make it more robust against attack"[158]. The named security measures include "tackling phishing, blocking malicious domains and IP addresses, and other steps to disrupt malware attacks"[159]. As most of the UK critical infrastructure is owned by the private sector, the British government seeks to work close together with the industry and help them to protect machine software.[160]

Active cyber defense seems to include measures only within the boundaries of the UK's national networks. Thus, conceptualization of the term active defensive is not identical to what was theorized in the section of offensive cyber capabilities (chapter 2.2.2). In the academic debate, active defense refers to the intrusion into foreign networks in order to prevent the intruder from causing damage to one's own network infrastructure.[161] Looking at the conceptualization of the concept in the strategy, there is no indication that active defense involves the penetration of foreign networks. Ian Levy, Technical Director in the UK National Cyber Security Centre, even states that the ACD program "is not intended to imply retaliation (`hack back') by victims or militarisation of the internet

[156] Ibid., 26
[157] Ibid., 18
[158] British Government, 'National Cyber Security Strategy 2016-2021', 33
[159] Ibid., 34
[160] Ibid.
[161] See chapter: Defensive cyber posture

(…)"[162]. The program rather "aspires to protect the majority of people in the UK from the majority of the harm, caused by the majority of the attacks, for the majority of the time."[163] What does this mean for the UK's cyber posture? The ACD program underlines the UK's focus on the defense. Even though the term active defense may suggest actions that go beyond the protection of national networks, UK uses the concept for clearly defensive purposes.

Apart from the whole range of defensive cyber measures that the UK adopts within the Active Cyber Defense program, the NCSS 2016-2021 makes clear indications that the UK's defense includes offensive cyber elements.[164] While the British understanding of active cyber defense is defensive in nature, deploying offensive cyber capabilities seems to encompass attacks on systems located outside the UK's territory. The NCSS 2016-2021 conceptualizes offensive cyber capabilities as "the use of cyber capabilities to disrupt, deny, degrade or destroy computers networks and internet connected devices."[165] Regarding the development of offensive cyber capabilities, the strategy leaves little room for interpretation. The paper states:

> "Offensive cyber capabilities involve deliberate intrusions into opponents' systems or networks, with the intention of causing damage, disruption or destruction. Offensive cyber forms part of the full spectrum of capabilities we will develop to deter adversaries and to deny them opportunities to attack us, in both cyberspace and the physical sphere."[166]

According to the strategy, the government seeks to deploy offensive cyber capabilities "at a time and place of our [the UK's] choosing, for both deterrence and operational purposes"[167]. The paper underlines that the UK "respond(s) to cyber attacks in the same way as we [the UK] respond to any other attack, using whichever capability is most appropriate, including an offensive cyber capability"[168] and integrates these capabilities into the arsenal of the armed forces.[169] The use of offensive cyber capabilities does not seem to enrich the methods of the secret service alone, but also contributes to the UK's

[162] Levy, 'Active Cyber Defence - One Year On', 8
[163] Ibid., 1
[164] British Government, 'National Cyber Security Strategy 2016-2021', 51
[165] Ibid., 76
[166] Ibid., 51
[167] Ibid.
[168] Ibid., 10
[169] British Government, *National security strategy and strategic defence and security review 2015*, 41; See also: ibid.

military power in conflicts. Close cooperation between the GCHQ and the Ministry of Defense in the field of cyber security in the framework of a National Offensive Cyber Programme (NOCP) has been in place since 2015.[170]

The UK's approach to develop and make use of offensive cyber capabilities is reflected in speeches and statements by cyber security officials. Some month before the NCSS 2016-2021 was published, George Osborne, Chancellor of the Exchequer from 2010-2016, underlined in his November 2015 speech that "we [the UK] are building our own offensive cyber capability – a dedicated ability to counter-attack in cyberspace."[171] Osborne emphasizes the UK's wide range of tools to cyber threats when possessing offensive cyber capabilities, which increases the level of security. Others supported this view and argued in the same vein. Ciaran Martin, Chief Executive of the National Cyber Security Center, points out that the UK deploys offensive cyber measures "to combat and deter the most aggressive threats"[172]

The analysis of the UK's cyber doctrine through the prism of offense/defense posture points out that the UK's cyber defense includes offensive components. In other words, the UK develops offensive tools in addition to their defensive capabilities. The most recent cyber security strategy as well as political statements indicate that UK does not only establish an offensive cyber force, but is also willing to use it in case of hostile cyber-attacks on national networks and for operations to strengthen its military power.

### 4.1.2 Cyber capabilities

The previous section scrutinized the National Cyber Security Strategies and examined statements in order to illustrate the place of cyber capabilities in the UK's doctrinal thinking. However, as discussed in the theoretical part, this thesis defines cyber posture as comprising the components doctrine *and* capabilities. The following section scrutinizes UK's cyber capabilities to understand whether the UK possesses the capabilities to carry out offensive actions as described in its doctrine.

[170] Ministry of Defence, *Annual Report and Accounts*, 26
[171] Osborne, *Chancellor's speech to GCHQ on cyber security*
[172] Martin, *A new approach for cyber security in the UK*

Firstly, this section attempts to identify the offensive and defensive cyber capabilities that the UK possesses in its defense arsenal. The aim is to gain an impression of the current state of affairs and evaluate whether offensive or defensive capabilities predominate. Secondly, this part examines whether the UK has deployed offensive cyber capabilities in real world situations to evaluate the UK's preparedness to implement what it claims in the cyber doctrine.

In September 2013, Philip Hammond, Defense Secretary at the Ministry of Defense, announced that the British army had established a cyber unit to increase the UK's national security in cyberspace. The new Joint Cyber Reserve was assigned to develop "a full-spectrum military cyber capability, including a strike capability, to enhance the UK's range of military capabilities"[173]. The nature of these capabilities is not further specified. For strategic reasons, the ministry treats offensive cyber similarly to its nuclear arsenal, special forces or submarine patrols.[174] When Hammond introduced the NCSS 2016-2021 in November 2016, he underlined that UK further invests in offensive cyber technologies in order to have the opportunity to "strike back" when being attacked.[175] It is certain that the UK possesses offensive cyber technologies but difficult to examine the power of these capabilities.

One method of evaluating the strength of the arsenal is to look at the budget that has been spend for cyber security and offensive capabilities in particular. Since 2009, the British government has extensively invested into their cyber security. For a period of five years, the National Cyber Security Strategy 2011-2016 allocated investments of £860 million (around 980 million euro) into a cyber security program.[176] The final report illustrates that more than half of the budget (£441.8 million) has been invested into "National Sovereign capability to detect and defeat high end threats" and 117.0 million into the "support to full spectrum effects capability".[177] There is no distinct number of the budget spend on offensive cyber capabilities. The report does not make a distinction between offensive and defensive capabilities. However, it can be assumed that investments into these

[173] Hammond, *New cyber reserve unit created*
[174] Roberts and Lawson, *Written submission for the Joint Select Committee on National Security Strategy inquiry into Cyber Security.*, 12
[175] Hammond, *Chancellor speech: launching the National Cyber Security Strategy*
[176] Cabinet Office, 'The UK Cyber Security Strategy 2011-2016', 32
[177] Ibid.

capabilities are higher, as the budget does not include investments by the Ministry of Defense. According to expert assumptions, the Ministry of Defense invests around £200 million into offensive cyber capabilities per year.[178] This figure is considerable high, but in relation to the total investments that the UK spends on cybersecurity, it can be expected that the UK invests a higher amount into defensive cyber capabilities.

Moreover, the Annual Report 2016-2017 of the Intelligence and Security Committee of Parliament reveals an insight into the UK's offensive cyber capabilities. The report states a considerable increase in the development of offensive cyber capabilities since 2014. Regarding the progress of the National Offensive Cyber Program, GCHQ has outperformed the stated objectives and doubled the number of capabilities, which the security organization aimed to reach.[179] Even though the concrete numbers are redacted in the report, it points out the UK's ability to use offensive strikes against advisories in cyberspace.

Furthermore, the British government reveals in the NCSS 2016-2021 an allocation of £1.9 billion to the cyber security institutions for the period of five years.[180] The budget includes the establishment of a National Cyber Security Centre (NCSC) as part of the British intelligence service GCHQ, which combines the Centre for Cyber Assessment (CCA), the Computer Emergency Response Team UK (CERT UK) and GCHQ's information security arm.[181]

The doubling of investments into cyber security underlines the UK's efforts to achieve cyber resilience. The development of offensive cyber capabilities seems to be a crucial element to achieve this goal. In September 2018, newspapers announced that the Ministry of Defense and the GCHQ received funding in the amount of £250 million to build up a group of 2000 experts from security, military and industry in order to combat cyber threats.[182] In how far these experts develop offensive or defensive capabilities is not clear.

[178] Roberts and Lawson, *Written submission for the Joint Select Committee on National Security Strategy inquiry into Cyber Security.*, 12
[179] Intelligence and Security Committee of Parliament, 'Annual Report 2016-2017', 44
[180] British Government, 'National Cyber Security Strategy 2016-2021', 10
[181] The NCSC was opened in October 2016.
[182] Fisher, Lucy, 'Britain launches £250m cyber-force to wage war on terrorists'. *The Times,* 21 September 2018

To sum up, while the UK's expenditure in cyber security is no more than a rough estimate, it helps to receive an inside look into the UK's intentions in cyberspace. In the theoretical part, the thesis pointed out that developing full-scale attacks require considerate resources. The UK makes these resources available to strengthen its position in the cyber domain. Therefore, without being able to determine the exact offensive capability, the evidence allows to conclude that most likely, the UK backs its offensive doctrine with substantive offensive capabilities.

Having illustrated the UK's efforts to build develop offensive cyber capabilities, the question that brings together doctrine and capabilities is under which conditions the British government could use this arsenal. In the theoretical part, the thesis underlined the immense advantage of having offensive capabilities as a force multiplier in terms of military conflicts. When developing these capabilities, it is likely that the British military makes use of them not only for protection purposes but also to enhance their military power. Even though it is difficult for scientists to evaluate how and when the military or intelligence services use offensive capabilities, various statements indicate that the UK's military has already used its offensive capabilities to attack a foreign server.

Defense Secretary Michael Fallon, for instance, admitted several times that the UK made use of cyber-attacks in military operations against the Islamic State. In June 2017, in a speech at the Cyber 2017 Chatham House Conference, Fallon pointed out that

> "(…) we're [the UK] making sure that offensive cyber is now an integral part of our arsenal. (…) Our National Offensive Cyber Planning allows us to integrate cyber into all our military operations. And I can confirm that we are now using offensive cyber routinely in the war against Daesh, not only in Iraq but also in the campaign to liberate Raqqa and other towns on the Euphrates. Offensive cyber there is already beginning to have a major effect on degrading Daesh's [the Islamic State's] capabilities."[183]

Jeremy Flemming, director of the GCHQ, confirms these operations by stating that the GCHQ and the Ministry of Defense are deployed offensive cyber capabilities against the Islamic State in order to "suppress their propaganda, hinder their ability to coordinate attacks and protected coalition forces on the battlefield."[184] These statements indicate that the UK prepared to deploy offensive cyber capabilities. As theorized in the first part of

[183] Fallon, *Defence Secretary's speech at Cyber 2017 Chatham House Conference*.
[184] Fleming, *Director's speech at CYBERUK*.

this thesis, the crucial difference between cyber and kinetic weapons is that cyber operations are difficult to observe. While it is possible to take pictures of armed soldiers, tanks or combat aircrafts crossing a border to another state's sovereign territory, the use of cyber weapons take place in secret and may remain covered. Even though the topic is often classified as secret information, open statements by security officials indicate the UK's self-confidence in its pro-active approach in the cyber domain and has certainly deterrent effects. For this thesis, it highlights the UK's offensive posture in cyberspace and underlines the preparedness of the UK government to make use of offensive cyber capabilities.

## 4.2 Cyber posture of the Republic of Estonia

### 4.2.1 Cyber doctrine

In 2008, the Estonian Ministry of Defense published Estonia's first cyber security strategy as one of the first states in the world to do so.[185] The strategy highlights the necessity of inclusing the cyber domain in national security planning and creating a "cyber security culture"[186] to increase the level of resilience in cyberspace. The strategy identifies threat actors, security vulnerabilities and outlines various areas to coordinate, discuss and develop Estonia's cyber security for individuals, companies and government institutions. The document focuses on the following strategic objectives: implementation of a "graduated system of security measures", increasing the competence and awareness of security related risks though research and training, development of a contemporary legal framework to ensure standards in cyber security and the promotion of international collaboration.[187]

To ensure Estonia's readiness in case of a cyber-attack, the strategy identifies three measures. First, imposing stricter requirements for companies operating with critical infrastructure should reduce the risk of major economic or human disasters in case of a cyber-attack. Second, the "identification and management of cyber- attacks, the

[185] At that time, only the US, Sweden and Germany have published a cyber security strategy. See i.e.: Pernik and Tuohy Emmet, 'Cyber Space in Estonia: Greater Security, Greater Challenges', 2
[186] Estonian Ministry of Defense, 'Cyber Security Strategy 2008-2013', 3
[187] Ibid.

efficiency of network traffic monitoring and the ability to perform strategic and tactical analyses"[188] should increase Estonia's ability to counter cyber-attacks. Finally, the responsibilities, coordination and allocation of tasks between governmental institutions, agencies and companies should be clearly defined in order to establish an effective organizational structure.[189] These measures indicate that Estonia's first cyber security strategy takes a rather defensive stance. They aim at securing Estonian infrastructure systems without any contemplation of attacking networks that are located outside of Estonia's territory. Thus, the strategy does not provide evidence of offensive actions in cyberspace.

In 2014, Estonia adopted its second cyber security strategy for the period of 2014-2017.[190] The document revises the previous strategy and adopts objectives and ambitions to new challenges and developments in the cyber domain. The strategy includes an appraisal of current cyber security developments, sets guidelines to increase resilience in cyberspace, formulates aims and ambitions to be reached by 2017 and illustrates the evolved authorities which are part of Estonia's organizational cyber security structure. To reach the general objective of the strategy[191], the strategy formulates subgoals, which provide an insight into Estonia's cyber posture. Various pre-emptive measures demonstrate Estonia's defensive stance in cyberspace. First, Estonia constantly aims to manage, map and update ICT systems and establish alternative solutions in case of attacks on the cyber infrastructure or e-services.[192] Second, Estonia seeks to store critical data in secure computer centers inside and outside of Estonian territory.[193] In addition, the strategy outlines the adoption of a "national comprehensive monitoring, analysis and reporting system"[194], which guarantees hazard detection in a timely manner.

[188] Ibid., 14
[189] Ibid., 14–5
[190] Estonian Ministry of Economic Affairs and Communication, 'Cyber Security Strategy 2014-2017'
[191] General objective: "The four-year goal of the cybersecurity strategy is to increase cybersecurity capabilities and raise the population's awareness of cyber threats, thereby ensuring continued confidence in cyberspace." ibid., 8.
[192] Ibid., 8 and 9
[193] Estonia is about to open a data embassy in Luxembourg to store critical data outside the state's territory. The aim is to protect critical information from cyber-attacks, natural disasters or physical attacks on datacenters. See for instance: E-Estonia, 'Estonia to open the world's first data embassy in Luxembourg' and ibid.
[194] Estonian Ministry of Economic Affairs and Communication, 'Cyber Security Strategy 2014-2017', 9

Moreover, the strategy dedicates one subgoal to the development of defensive cyber capabilities. Estonia seeks to use "active defense" in cyberspace by developing "military cyber defence capabilities"[195]. What exactly these defensive capabilities encompass and whether active defense includes the intrusion into foreign networks remains unclear. Strategic papers and documents lack a clear definition of how Estonia defines the term active defense. Official publications do not conceptualize whether active defense includes the intrusion into foreign networks.[196] Therefore, it would be misleading to conclude that Estonia has offensive elements in its overall cyber strategy. At least Estonia has no intents to make use of offensive capabilities according to their doctrinal thinking. However, as the following section points out, various sources indicate that Estonia is considering the development of offensive cyber capabilities in a new cyber command. Furthermore, Estonia's National Cyber Security Concept, which was published by the Ministry of Defense in 2017, affirms the state's defensive cyber posture. The document outlines what the government must do to ensure updated information systems and provide trainings and advice to service providers.[197]

To conclude, the analysis of Estonia's cyber security strategies suggest that Estonia's cyber doctrine is rather defensive in character. Accordingly, in terms of doctrine, Estonia's cyber posture can similarly defined as defensive. The main measures Estonia uses to defend itself in the cyber domain are the constant mapping, managing and updating of networks, training of personnel, extending international cooperation and developing cyber defense capabilities. The elements coincide with the characteristics a defensive cyber posture as defined in the first part of this thesis.

### 4.2.2 Cyber Capabilities

The previous section pointed out that in terms of doctrine, Estonia's cyber posture is rather defensive. However, when looking at cyber capabilities, there are various indications that Estonia develops offensive cyber capabilities in a targeted way. As

[195] Ibid., 10

[196] Piret Pernik from the International Centre for Defense and Security comes to the same result that Estonia does not officially define active cyber defense. According to her, it includes "cyber-attacks, i.e. unauthorised intrusion to the information systems (hacking) of another country." Pernik, 'Estonian Cyber Command: What Is It For?'

[197] Estonian Ministry of Defense, 'National Security Concept', 17

highlighted in the theoretical part of this thesis, every state has a certain amount of offensive cyber capabilities, which governments can use against aggressive threats. Therefore, it can be assumed that Estonia possesses capabilities that enable to counter a variety of devices that might attack Estonian critical infrastructure. However, it does not indicate that Estonia's cyber posture is offensive, as Estonia's doctrine does not mention under which circumstances these capabilities could be deployed and whether these measures are used to attack foreign networks.

While the overall emphasis of capabilities in the last years has been on setting up defensive capabilities, it seems that Estonia is in the process of developing limited offensive cyber capabilities to strengthen its defense. In August 2018, Estonia opened a new Cyber Command with the task of defending Estonian networks from hostile attackers and "to be prepared to carry out active cyber defence operations"[198]. The aim of the Cyber Command is to assamble a troop of up to 300 cyber specialists by 2020.[199] Even though Estonia's definition of active defense is blurred, various statements indicate that Estonia seeks to develop offensive code to penetrate foreign networks in times of war or allied military operations.

For instance, Andres Hairk, commander of the Cyber Command, explains that the new Command is developing cyber capabilities that provide it with an extra tool to attack. Additionally, he stresses that this does not mean that Estonia will attack its neighbours in peacetime, but rather that it supports national defense.[200] In another speech, Hairk states that in order to protect its own cyber infrastructure, the country must attack its own systems to find vulnerabilities on the one hand, and use these capabilities to support military operations in times of conflicts on the other hand.[201] Moreover, Erki Kodar, undersecretary for legal and administrative affairs at the Estonian Ministry of Defense, points out in a speech on the new Cyber Command, that in order to increase cyber defense, states need to "develop the full range of cyber capabilities", which means to focus not only on defense, but "on offense as well"[202]. Even though Estonia is reluctant to give clear

[198] Estonian Ministry of Defense, 'National defence development plan 2017–2026'
[199] Estonian Information System Authority, 'Annual Cyber Security Assessment 2018', 32
[200] Krjukov, Aleksander, 'Kaitseväes alustab küberväejuhatus [Defense Forces establish Cyber Command]'. *Eesti Rahvusringhääling (ERR),* 20 July 2018
[201] Pau, Aivar, 'Tehtud! Eesti kaitsevägi lõi küberväejuhatuse [Done! The Estonian Defense Forces establishes the cyber command]'. *Postimees Tehnika,* 1 August 2018
[202] Kodar, *Presentation at the NATO cyber symposium NIAS'17, Mons, Belgium, October 17-19, 2017*

statements on the development of offensive cyber capabilities, the statements indicate that the country is at least considering the development of these tools.

The theoretical part of this thesis discussed the high costs of making network systems resilient to cyber-attacks or developing offensive cyber capabilities. Regarding skilled labor, the public sector is in constant competition with private cyber security companies, especially in a small nation like Estonia. Obviously, Estonia has much fewer financial resources to invest into its cyber security than larger states. To guarantee the security of the state in cyberspace, the Estonian government established a cyber unit of the Estonian Defense League (Kaitseliit). The cyber unit consists of experts and security practitioners from the private, public and the third sectors. The civilian militia group aims to strengthen Estonia's cyber resilience by conducting trainings and coordinated exercises. In addition, they are involved in the protection of critical infrastructure in case of attacks.[203] Estonia's strategic documents constantly highlight close cooperation between the public, private and third sector.[204] The Cyber Unit pools cyber expertise from companies and government institutions and acts as an integrated part of Estonia's national defense system. The National Defense League Act, adopted in 2013, provides the Cyber Unit a legal mandate, organisational framework and membership conditions.[205] To sum up, the approach to create a voluntary based expert group of cyber specialists circumvents high costs for the Estonian state and offers a useful opportunity to share information between sectors.

To conclude, this section identified Estonia's cyber posture by analysing cyber doctrine and capabilities. In terms of intentions, it seems that Estonia adopts a defensive oriented posture in cyberspace. The intentional missing conceptualization of the vague term "active defense" allows a range of activities and makes it difficult to conclude that Estonia adopts offensive components into its cyber doctrine. In terms of capabilities, Estonia develops predominantly defensive cyber tools. However, the recent creation of a Cyber Command, whose work seems to include the development of offensive cyber capabilities, suggests that Estonia becoming active in developing offensive tools as an addition to its

[203] Kaska et al., 'The Cyber Defence Unit of the Estonian Defence League', 22–4
[204] See for instance: Estonian Ministry of Defense, 'National Security Concept', 17
[205] Estonian Parliament, 'The Estonian Defence League Act'

defensive measures. Due to the lack of clear statements regarding these tools, there has not been a comprehensive discussion on costs and benefits for Estonia's cyber protection.

### 4.3 Comparison and discussion

The analysis of the cyber posture of the UK and Estonia illustrates that deploying offensive cyber capabilities is a debated topic in both states. Regarding the overall posture, it can be concluded that while the UK has pursued an offensive cyber posture including offensive elements, Estonia adopts a defensive posture almost exclusively focused on defensive elements. The difference in offense and defense posture can be most clearly identified from the cyber doctrines. Whereas the UK adopts a doctrine that contains intentions to develop and deploy offensive capabilities, the Estonian cyber doctrine contains merely defensive measures. Whereas the UK publicly states their intentions to deploy offensive cyber capabilities whenever they considered it as necessary, Estonia's doctrine does not provide any indication suggesting that the state adopts an offensive posture at present time.

In terms of capabilities, the distinction is less clear. The UK demonstrates that it develops offensive cyber capabilities and admits that these have been already used for wider military ends. Estonia is more reluctant in this regard. Merely official statements and interviews indicate that Estonia develops offensive capabilities in its new established Cyber Command. Nevertheless, even when Estonia possesses limited offensive capabilities, the difference remains. The UK adopts an offensive and Estonia a defensive posture, as Estonia's doctrine is, at present time, merely focused on the defense.

Furthermore, the UK's doctrine and development of cyber tools suggest that offensive cyber capabilities are rather an addition to the existing defensive measures. This opens the debate on the explanatory power of the offense-defense balance theory. In as much as a current advantage of the offensive can be assumed in cyberspace (see chapter 2.2.4), states as rational actors would be expected to adopt a posture which reflects this advantage, as it would maximize their security with most efficient use of resources. However, empirical evidence from the UK and Estonia indicate that this is not the case. Offensive capabilities are rather an additional tool that supplements a state's cyber security. Even though various factors may indicate that offense has the advantage in

cyberspace, it would not lead to a situation that states predominantly invest into offensive cyber capabilities.

Overall, this finding suggests that in contradiction with the incentives of an offense advantage, states still primarily invest in defense. Only some, in this case the UK as a large state, invests a portion of its resources in offensive capabilities. Estonia as a small state, which could be expected to be even more sensitive to the offense-defense balance, even focuses almost exclusively on defense. This means that while offense is thought to have the advantage, states rather invest in defensive cyber capabilities. Whereas large states seem to afford offensive cyber capabilities, small states rather opt for the defense.

These findings requires explanation. The focus on defense instead of offense could be explained by various considerations. First, as indicated in the discussion on the offense-defense advantage (chapter 2.2.4), the high costs to develop and maintain effective offensive cyber capabilities could not be justified in a cost-benefit calculation. Financial constraints force states to evaluate precisely whether the costs of developing offensive cyber capabilities are justified. Employing skilled labor is costly, especially in the highly competitive ICT sector. Even though offense has the advantage, this advantage pays only off in most sophisticated cyber-attacks, which are predominantly conducted on a state-to-state level and occur relatively rare compared to low-level cyber-attacks. In this sense, the explanatory power of the offense-defense balance is reduced.

Second, offense-defense balance and the security dilemma are limited to states as the most acute threat to national security. However, in the cyber domain, most threats do not come from state actors. Without investing into defensive capabilities, a state is exposed to a much larger amount of threat actors. When network systems are not secure, even attackers with limited knowledge are able to intrude and cause danger to a state's infrastructure. This can explain predominant investments defensive capabilities, even if, at the upper end of the intensity spectrum of threats, offense might have the advantage.

To sum up this discussion, state size seems to have an effect on a state's cyber posture. While the UK adopts an offensive posture, Estonia's cyber posturing is rather defensive. These findings do not coincide with majority view of an offensive advantage in cyberspace that was discusses in chapter 2.2.4. It seems that the development of offensive cyber capabilities are merely an addition to defensive measures, which primarily large

states can afford. Contrary to the expectations that small states are more sensitive to the balance and adopt an offensive cyber posture, the results of the analysis of Estonia's cyber posture do not confirm this assumption.

## 5 Conclusion

This research examined the effect of state size on cyber posturing of states bringing together assumptions of IR theory and the cyberspace. The thesis followed three main strands. First, it theorized the conventional offense-defense balance and explained its impact on state posture. Based on existing literature of neorealist thinkers, it outlined the factors that influence the balance and theorized how these factors could suggest states adopting an offensive or defensive posture. Second, the research applied the theoretical assumptions to the cyber domain and adjusted concepts according to the cyber environment. Finally, the thesis scrutinized how state size matters in adopting a particular cyber posture. The thesis argued that small states are more sensitive to the offense-defense balance due to their susceptibility to pressures (e.g. resource constraints, smaller margin of error). Whereas large states have more leeway, it was expected that small states mirror the offense-defense more closely. Using a most similar systems design, the empirical part examined the cyber posture of the UK and Estonia to elaborate the effect of the small/large factor on cyber posture of states.

The thesis made several findings that have implications for further research. First, to answer the research question, the thesis demonstrated that state size has an impact on the cyber posture of state. Empirical evidence demonstrated that there is a difference in the cyber posture of small and large states. While the UK adopts an offensive cyber posture, Estonia's strategic documents do not indicate the development of offensive cyber capabilities at present the time. In this regard, the empirical evidence does not coincides with the theoretical assumption that both small and large states adopt an offensive cyber posture.

Second, the study demonstrated the applicability of the offense-defense balance to the cyber domain. The thesis pointed out that offensive and defensive cyber capabilities are better to distinguish than in the traditional domains. There is a clear difference between software that is programmed with the aim to monitor networks and prevent cyber-attacks on the one hand, and software that seeks to penetrate other network systems on the other hand. This consideration addresses the long-standing debate in the offense-defense literature, where the differentiation of offensive and defensive weapons and the question

of whether offense or defense has an advantage are controversially discussed. The literature-based comparison of arguments found out that most of the authors favoring an offensive advantage in cyberspace merely take technical features of offensive code into account. In contrast, adherents of a defensive advantage include the costs of developing these capabilities and argue that defensive capabilities overweigh in a cost benefit calculation. At present time, there is not enough empirical evidence to verify one of these assumptions.

In addition, various conceptual factors needed adjustments to theorize the balance in cyberspace. Digitalization was utilized as an analogy to geography. Byte power and versatility in cyberspace were characterized according to firepower and mobility in the traditional domains. Theorizing digitalization as equivalent to geography is a new contribution to existing cyber security literature. The theoretical assumptions indicated that all factors in the cyber offense-defense balance seem to favor the offense. This finding is in line with the majority opinion that the offense has the advantage in cyberspace.

Third, the research found explanations on how the offense-defense balance influences cyber posture. With the neorealist presumption that states take rational decisions and adopt a strategy that fits best to their aim of maximizing national security, the offense-defense balance was expected to have an impact on a state's cyber posture. The thesis demonstrated that the currently assumed offensive advantage does not imply that states predominantly invest in offensive cyber capabilities. Empirical evidence suggest that states develop offensive cyber capabilities rather as a complementary element in addition to defensive cyber measures. Whereas large states can afford offensive tools, small states rather focus on defensive cyber capabilities and adopt a defensive cyber posture.

Fourth, the study contributed to the existing small state literature and theorized small state's behavior in cyberspace. The thesis underlined that factors digitalization, byte power and versatility equally effect small and large states. Therefore, in line with offense-defense theory, the thesis suggested that both small and large states follow the majority view and opt for an offensive cyber posture. However, as stated above, the empirical case of Estonia demonstrates the opposite. Moreover, the thesis demonstrated theoretically that small states are more sensitive to the offense-defense balance than larger powers.

Empirically, the sensibility of states towards the balance was difficult to measure without being confident regarding the advantage of offense or defense in cyberspace. Based on the assumption that small states are more sensitive to the balance, empirical findings rather indicate that defense has the advantage in the cyber domain.

The difference between theoretical assumptions and empirical evidence can be explained by various reasons. First, the scrutinized states might not act rational. The offense-defense balance assumes that states take optimal decisions to increase their security. Both states could act irrational and disregard an offensive advantage. It requires further research in order to identify whether the cases are exceptional. Second, the offense might not have the advantage in cyberspace. As indicated in the second finding of this conclusion, the offense advantage in cyberspace is not accepted without criticism. Even though the majority assumes an offense advantage, this might not be the case. Another explanation is that decision makers do not perceive the offense as being advantageous. States adopt their cyber posture according to how they perceive the balance. In the relatively new cyber environment, they might be reluctant in following the majority view and invest in offensive rather than defensive cyber capabilities.

In light of the above considerations, the thesis has various limitations. First, it compared only two cases. To confirm a difference in small and large cyber posture requires the examination of more cases. Nevertheless, this limited study of two cases provides an initial insight and suggests that there is a difference. Confirming this finding requires further exploration with a greater variety of cases.

Second, the empirical discussion relied on relatively crude measurements. The availability of information is a challenge for all cyber researchers. At least the development of offensive cyber capabilities is often confidential information and not available to the public. While it poses a challenge for the validity of findings, the measurements used in this thesis are sufficient to conclude on offensive and defensive cyber posture.

Finally, this study exclusively attempted to apply the logic of the offense-defense balance in the cyber domain. It derived its arguments mainly from theoretical assumptions that authors theorized for the traditional domains. However, the offense-defense balance is a debated variable in terms of measurement and applicability both in the traditional and the

cyber domain. Whereas nature of capabilities are better to distinguish in cyberspace, the advantage of offense or defense is unclear. It requires further research to evaluate whether the offense-defense balance can be considered as a useful tool to explain cyber posture.

## 6 Bibliography


Aquilla, John, 2012. ‘Cyberwar Is Already Upon Us’. Available at: https:// foreignpolicy.com/2012/02/27/cyberwar-is-already-upon-us/ [Accessed 15 November 2018]

Areng, Liina, 2014. ‘Lilliputian States in Digital Affairs and Cyber Security’. Tallinn Paper 4).

Ayala, Luis, 2016. Cybersecurity Lexicon, New York.

Bejtlich, Richard, 2013. The practice of network security monitoring: Understanding incident detection and response, San Francisco.

Booth, Ken and Nicholas J. Wheeler, 2008. The Security Dilemma: Fear, cooperation and trust in world politics. Palgrave Macmillan, Houndmills.

British Government, H. M., 2015. National security strategy and strategic defence and security review 2015: A secure and prosperous United Kingdom, London.

British Government, H. M., 2016. ‘National Cyber Security Strategy 2016-2021’.

Browning, Christopher S., 2006. ‘Small, Smart and Salient?: Rethinking Identity in the Small States Literature’. Cambridge Review of International Affairs 19(4), 669–684.

Bryant, William D., 2016. International conflict and cyberspace superiority: Theory and practice. Routledge studies in conflict, security and technology. Routledge, London.

Buchanan, Ben, 2017. The Cybersecurity Dilemma: Hacking, trust and fear between nations. Oxford University Press, New York, NY.

Cabinet Office. ‘The UK Cyber Security Strategy 2011-2016: Annual Report 2016’.

Cabinet Office, 2009. ‘Cyber Security Strategy of the United Kingdom 2009-2011: safety, security and resilience in cyber space’.

Cabinet Office, 2011. ‘The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world’.

Carr, Jeffrey, 2012. Inside Cyber Warfare: Mapping the Cyber Underworld. 2nd ed. , Sebastopol, California.

Center for Strategic and International Studies. ‘Significant Cyber Incidents Since 2006’. Available at: https://csis-prod.s3.amazonaws.com/s3fs-public/190103_Significant_ Cyber_Events_List.pdf [Accessed 6 January 2019]

Choucri, Nazli, 2012. Cyberpolitics in international relations. MIT Press, Cambridge Mass.

Clark, David, 2010. ‘Characterizing cyberspace: past, present and future’. MIT Working Paper Series Version 1.2, March 12.

Clarke, Richard A. and Robert K. Knake, 2012. Cyber war: The next threat to national security and what to do about it, New York.

Coburn, A. W., J. Daffron, A. Smith, J. Bordeau, É. Leverett, S. Sweeney and T. Harvey, 2018. ‘Cyber Risk Outlook 2018’. Centre for Risk Studies, University of Cambridge, in collaboration with Risk Management Solutions, Inc.

Coden, Michael and Nadya Bartol, 2017. ‘Our critical infrastructure is more vulnerable than ever. It doesn’t have to be that way’. World Economic Forum. Available at: https://www.weforum.org/agenda/2017/02/our-critical-infrastructure-is-more-vulnerable-than-ever-it-doesn-t-have-to-be-that-way/ [Accessed 15 November 2018]

Cohen, Bret, Britanie Hall and Charlie Wood, 2017. ‘Data Localization Laws And Their Impact on Privacy, Data Security And the Global Economy’. Antitrust 32(1).

Denning, Dorothy E. and Bradley J. Strawser, opyright 2017. ‘Active Cyber Defense: Applying Air Defense to the Cyber Domain’. In Understanding cyber conflict. 14 analogies, ed. George Perkovich and Ariel Levite. Georgetown University Press, Washington, 193–209.

East, Maurice A., 1973. ‘Size and Foreign Policy Behavior: A Test of Two Models’. World Politics 25(4), 556–576.

E-Estonia, 2017. ‘Estonia to open the world’s first data embassy in Luxembourg’. Available at: https://e-estonia.com/estonia-to-open-the-worlds-first-data-embassy-in-luxembourg/ [Accessed 28 December 2018]

Ehrenfeld, Jesse M., 2017. ‘WannaCry, Cybersecurity and Health Information Technology: A Time to Act’. Journal of medical systems 41(7), 104.

Estonian Information System Authority, 2018. ‘Annual Cyber Security Assessment 2018’.

Estonian Ministry of Defense, 2008. ‘Cyber Security Strategy 2008-2013’.

Estonian Ministry of Defense, 2016. ‘National defence development plan 2017–2026’. Available at: http://www.kaitseministeerium.ee/riigikaitse2026/arengukava/eng/ [Accessed 28 December 2018]

Estonian Ministry of Defense, 2017. ‘National Security Concept’. Available at: http://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_security_concept_2017.pdf [Accessed 17 December 2018]

Estonian Ministry of Economic Affairs and Communication, 2014. ‘Cyber Security Strategy 2014-2017’.

Estonian Parliament. ‘The Estonian Defence League Act’. 28.02.2013. Available at: https://www.riigiteataja.ee/en/eli/525112013006/consolide [Accessed 28 December 2018]

Fallon, Michael, 2017. ‘Defence Secretary’s speech at Cyber 2017 Chatham House Conference’, 27 June.

Fisher, Lucy, 2018. ‘Britain launches £250m cyber-force to wage war on terrorists’. The Times, 21 September.

Fleming, Jeremy, 2018. ‘Director's speech at CYBERUK’, 12 April.

Freedman, Lawrence, 2004. Deterrence. Polity Press, Cambridge, UK, Malden, MA.

Gartzke, Erik, 2013. ‘The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth’. International Security 38(2), 41–73.

Gerring, John, 2009. Case study research: Principles and practices. Cambridge Univ. Press, Cambridge.

Glaser, Charles L., 1997. ‘The Security Dilemma Revisited’. World Politics 50(1), 171–201.

Glaser, Charles L. and Chaim Kaufmann, 1998. ‘What is the Offense-Defense Balance and Can We Measure it?’. International Security 22(4), 44.

Goldsmith, Jack L. and Tim Wu, 2006. Who controls the Internet?: Illusions of a borderless world. Oxford University Press, New York.

Graham, David E., 2010. ‘Cyber Threats and the Law of War’. Journal of National Security Law & Policy 4(1), 87–102.

Guernsay, Lisa, 2001. ‘Welcome to the World Wide Web. Passport, Please?’. New York Times, 15 March.

Hammond, Philip. New cyber reserve unit created: Britain will build a dedicated capability to counter-attack in cyberspace and, if necessary, to strike in cyberspace.

Hammond, Philip, 2016. ‘Chancellor speech: launching the National Cyber Security Strategy’, 1 November.

Hare, Forrest, 2009. ‘Borders in Cybespace: Can Souvereignty Adapt to the Challanges of Cyber Security?’. In The virtual battlefield. Perspectives on cyber warfare, ed. Christian Czosseck and Kenneth Geers. Vol. 3 of Cryptology and information security series. IOS Press, Amsterdam, Washington DC, 88–105.

Intelligence and Security Committee of Parliament, 2017. ‘Annual Report 2016-2017’.

International Telecommunication Union. ‘The ICT Development Index (IDI): conceptual framework and methodology’. Available at: https://www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2017/methodology.aspx [Accessed 19 December 2018]

International Telecommunication Union, 2015. ‘Getting ready for the digital economy’. In: Trends in telecommunication reform.

International Telecommunication Union, 2017. ‘Global Cybersecurity Index (GCI) 2017’.

International Telecommunication Union, 2017. ‘Measuring the Information Society Report 2017’. Available at: https://www.itu.int/net4/ITU-D/idi/2017/index.html [Accessed 19 December 2018]

Jackson, William, 2011. ‘The security singularity: When humans are the biggest problem’. GCN, 23 September.

Jervis, Robert, 1978. ‘Cooperation under the Security Dilemma’. World Politics 30(2), 167–214.

Joyce, Rob, 2016. ‘USENIX Enigma 2016—NSA TAO Chief on Disrupting Nation State Hackers’. Available at: https://www.youtube.com/watch?v=bDJb8WOJYdA [Accessed 12 December 2018]

Kaska, Kadri, Anna-Maria Osula and Jan Stinissen, 2013. ‘The Cyber Defence Unit of the Estonian Defence League: Legal, Policy and Organisational Analysis’. Available at: https://ccdcoe.org/sites/default/files/multimedia/pdf/CDU_Analysis.pdf [Accessed 17 December 2018]

Kello, Lucas, 2017. The virtual weapon and international order. Yale University Press, New Haven, London.

Keohane, Robert O., 1986. Neorealism and its critics. The political economy of international change. Columbia Univ. Pr, New York.

Kodar, Erki. ‘Presentation at the NATO cyber symposium NIAS’17, Mons, Belgium, October 17-19, 2017’.

Krjukov, Aleksander, 2018. ‘Kaitseväes alustab küberväejuhatus [Defense Forces establish Cyber Command]’. Eesti Rahvusringhääling (ERR), 20 July.

Kuehl, Daniel T., 2009. ‘From Cyberspace to Cyberpower: Defining the Problem’. In Cyberpower and national security, ed. Franklin D. Kramer, Larry K. Wentz and Stuart H. Starr. 1st ed., Washington DC, 24–42.

Lamoreaux, Jeremy W., 2014. ‘Acting small in a large state's world: Russia and the Baltic states’. European Security 23(4), 565–582.

Levy, Ian, 2018. ‘Active Cyber Defence - One Year On’. UK National Cyber Security Centre. Available at: https://www.ncsc.gov.uk/information/active-cyber-defence-one-year [Accessed 11 December 2018]

Lewis, James Andrew, 2018. Rethinking cybersecurity: Strategy, Mass Effect, and States, Washington, DC, Lanham, MD.

Libicki, Martin C., 2009. Cyberdeterrence and Cyberwar. RAND, Santa Monica CA.

Lieber, Keir A., 2000. ‘Grasping the Technological Peace: The Offense-Defense Balance and International Security’. International Security 25(1), 71–104.

Lieberthal, Kenneth and Peter W. Singer, 2012. ‘Cybersecurity and U.S.-China Relations’. Available at: https://www.brookings.edu/research/cybersecurity-and-u-s-china-relations/ [Accessed 11 December 2018]

Lindsay, Jon R., 2013. ‘Stuxnet and the Limits of Cyber Warfare’. Security Studies 22(3), 365–404.

Lin, Herbert S., 2010. ‘Offensive Cyber Operations and the Use of Force’. Journal of National Security Law & Policy 4(1), 63–86.

Lin, Herbert S., 2012. ‘Operational Considerations in Cyber Attack and Cyber Exploitation’. In Cyberspace and national security. Threats, opportunities, and power in a virtual world, ed. Derek S. Reveron. Georgetown University Press, Washington DC, 37–56.

Locatelli, Andrea, 2013. ‘The Offense/Defense Balance in Cyberspace’. Analysis 203).

Lynn-Jones, Sean M., 1995. ‘Offense-Defense Theory and Its Critics’. Security Studies 4(4), 660–691.

Martin, Ciaran, 2016. ‘A new approach for cyber security in the UK’, Washington DC, 13 September.

Mearsheimer, John J., 2001. The Tragedy of Great Power Politics. Norton, New York.

Mearsheimer, John J., 2013. ‘Structural Realism’. In International relations theories. Discipline and diversity, ed. Timothy Dunne, Milja Kurki and Steve Smith. 3rd ed. Oxford Univ. Press, Oxford.

Ministry of Defence, 2018. Annual Report and Accounts, London.

Monte, Matthew, 2015. Network attacks and Exploitation: A framework, Indianapolis.

NATO Cooperative Cyber Defence Centre of Excellence. ‘Cyber Security Strategy Documents’. Available at: https://ccdcoe.org/cyber-security-strategy-documents.html [Accessed 31 December 2018]

North Atlantic Treaty Organization, 2017. ‘NATO Glossary of Terms and Definitions: AAP-06’.

Nye, Joseph S., 2010. Cyber Power, Cambridge.

Osborne, George, 2015. ‘Chancellor's speech to GCHQ on cyber security’, Cheltenham, 17 November.

Pau, Aivar, 2018. ‘Tehtud! Eesti kaitsevägi lõi küberväejuhatuse [Done! The Estonian Defense Forces establishes the cyber command]’. Postimees Tehnika, 1 August.

Pernik, Piret and Tuohy Emmet, 2013. ‘Cyber Space in Estonia: Greater Security, Greater Challenges’. International Centre for Defense Studies.

Pernik, Piret, 2018. ‘Estonian Cyber Command: What Is It For?’.

Peterson, Dale, 2013. ‘Offensive Cyber Weapons: Construction, Development, and Employment’. Journal of Strategic Studies 36(1), 120–124.

Presidential Policy Directive - Critical Infrastructure Security and Resilience [2013].

Reveron, Derek S., 2012. ‘An Introduction to National Security and Cyberspace’. In Cyberspace and national security. Threats, opportunities, and power in a virtual world, ed. Derek S. Reveron. Georgetown University Press, Washington DC, 3–19.

Rid, Thomas, 2012. ‘Cyber War Will Not Take Place’. Journal of Strategic Studies 35(1), 5–32.

Rid, Thomas, 2013. Cyber war will not take place. Oxford University Press, Oxford, New York.

Rid, Thomas and Ben Buchanan, 2015. ‘Attributing Cyber Attacks’. Journal of Strategic Studies 38(1-2), 4–37.

Roberts, Peter and Ewan Lawson, 2017. Written submission for the Joint Select Committee on National Security Strategy inquiry into Cyber Security.

Saltzman, Ilai, 2013. ‘Cyber Posturing and the Offense-Defense Balance’. Contemporary Security Policy 34(1), 40–63.

Sammarco, Natalie E., 2013. ‘The Great Firewall and the Perils of Censorship in Modern China’. Yale Journal of InternatIonal affairs 8(2), 136–138.

Shaheen, Salma, 2014. ‘Offense-Defense Balance in Cyber Warfare’. In Cyberspace and International Relations, ed. Jan-Frederik Kremer and Benedikt Müller. Springer Berlin Heidelberg, Berlin, Heidelberg, 77–94.

Skierka, Isabel, Robert Morgus, Robert Hohmann and Tim Maurer, 2015. ‘CSIRT Basics for Policy-Makers: The History, Types & Culture of Computer Security Incident Response Teams’. Available at: http://www.gppi.net/fileadmin/user_ upload/media/pub/2015/CSIRT_Basics_for_Policy-Makers_May_2015_WEB.pdf [Accessed 9 August 2018]

Slayton, Rebecca, 2017. ‘What Is the Cyber Offense-Defense Balance?: Conceptions, Causes, and Assessment’. International Security 41(3), 72–109.

Tang, Shiping, 2010. A Theory of Security Strategy for Our Time: Defensive Realism. Palgrave Macmillan US, New York.

TeleGeography. ‘Submarine Cable Map’. Available at: https:// www.submarinecablemap.com/ [Accessed 9 August 2018]

The Economist, 2010. ‘War in the fifth domain: Are the mouse and keyboard the new weapons of conflict?’, 1 July.

The Wallstreet Journal. ‘Cataloging the World's Cyberforces’. Available at: http:// graphics.wsj.com/world-catalogue-cyberwar-tools/ [Accessed 1 January 2019]

Thorhallsson, Baldur and Sverrir Steinsson, 2017. ‘Small State Foreign Policy’. Oxford Research Encyclopedia of Politics.

United Nations, 2018. ‘E-Government Survey 2018: Gearing e-government to support transformation towards sustainable and resilient societies’.

van Evera, Stephen, 1998. ‘Offense, Defense, and the Causes of War’. International Security 4(22).

Vassil, Kristjan, 2016. ‘Estonian e-Government Ecosystem: Foundation, Applications, Outcomes’. Background paper for the World Development Report 2016.

Waltz, Kenneth N., 1979. Theory of International Politics. Addison-Wesley series in political science. Addison-Wesley, Reading/Mass.

Wivel, Anders, Alyson J.K. Bailes and Clive Archer, 2016. ‘Setting the scene: small states and international security’. In Small States and International Security. Europe and beyond, ed. Clive Archer, Alyson J.K. Bailes and Anders Wivel. Routledge, New York, 3–25.

World Economic Forum, 2018. The Global Risks Report 2018. 13th ed. , Geneva.