UNIVERSITY OF TARTU
Faculty of Social Sciences and Education
Institute of Government and Politics

Henry Rõigas

A Small State Utilising its Niche Capability for Influence in Foreign and Security Policy: the Case of Estonia and Cyber Security

Master's thesis

Supervisor: Eoin Micheál McNamara, M.Sc.

Tartu 2015

Olen koostanud töö iseseisvalt. Kõik töö koostamisel kasutatud teiste autorite tööd, põhimõttelised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on viidatud.

Olen nõus oma töö avaldamisega Tartu Ülikooli digitaalarhiivis DSpace.

……..

/ Henry Rõigas /

Abstract

The aim of the thesis is to analyse how small states utilise niche capabilities to get wider influence in foreign and security policy outside the niche area. This is done by examining the case of Estonia and cyber security. The thesis first identifies the relevant theoretical approaches that explain the possible role of niche capabilities in a small state's foreign and security policy. The thesis then offers an overview of the Estonian case by explaining its strategy for foreign and security policy and its efforts in the area of cyber security. As the theoretical approaches are limited in explaining the possible phenomena of niches generating wider influence, the thesis applies an inductive approach by basing its findings on semi-structured interviews that were conducted mainly with officials from the Estonian Ministry of Defence and Ministry of Foreign Affairs.

The thesis found that the niche was seen as generating soft power and diplomatic capital by enhancing Estonia's positive image. Therefore, the niche was perceived as an important element in Estonia's fundamental strategy to be a valued partner to its strategic allies and within international organisations with the aim to strengthen the security guarantees provided by those entities. The niche was also indicated as having other effects such as creating additional communication channels and facilitating cooperation with strategic allies. In addition, it was apparent that certain factors have increased Estonia's ability to seek wider gains: the cooperative and cross-agency nature of the cyber security niche; being active in providing strategic and political input on the international level; and, the fact that the niche has provided Estonia an internationally valued capability that is not directly connected to its traditional security concerns. The thesis also suggests that in order to maintain the *status quo* or improve the niche capability, Estonia should take a clear strategic decision to focus on a certain "niche within the niche".

Table of contents

1. Introduction

"[T]he strong do what they can and the weak suffer what they must" – this statement made by Thucydides (1972, 302) in the fifth century BC has not lost its relevance in explaining how states act in the contemporary system of international relations. Small states, having limited influence and capabilities due to the lack of resources, are both dependent on and threatened by great world powers (Bailes, Wivel, and Archer 2014). To compensate for their weakness, small states have to adopt certain policies to ensure their survival (Bailes, Rickli, and Archer 2014). In the 21st century, the most common strategy for small states has been to opt for alignment that encompasses the acts of "bandwagoning" or "balancing" by allying with big powers and joining international organisations (see Walt 1987).

In this contextual setting, small states are prone to seek policies with the aim to strengthen their position or even gain influence. Many theories (see Joenniemi 1998, Arter 2000; Wivel 2005; Jakobsen 2009; Rickli 2009; Grøn and Wivel 2011) which explain the behaviour of small states have stated that a possible way to gain influence within a specific issue-area is to concentrate the small state's limited resources to develop a specialisation or a niche capability. However, the literature on small states has mostly neglected or insufficiently covered the question of how small states could use niche capabilities or a specialisation to have wider influence in foreign and security policy outside the niche area (Kronsell 2002, 17; Nasra 2010, 1). Therefore, this thesis aims to analyse the aforementioned phenomena by looking into the case of Estonia and its cyber security niche. Estonia, being a small state that has chosen the alignment strategy, was identified as a suitable case since it has been successful in developing an internationally acknowledged niche capability in cyber security (Kaljurand 2013, 70; Pernik and Tuohy 2013, 1).

Thus the thesis aims to examine how Estonia has utilised its cyber security niche to gain wider influence in foreign and security policy. The objective is to discuss both theoretical implications and the case-specific practical aspects of the findings. Since the theoretical basis to explain the phenomena is somewhat limited, the thesis takes an inductive approach. In order to understand the role of the niche in detail, eight semi-

structured interviews with officials from the Estonian Ministry of the Defence (MoD) and the Ministry of Foreign Affairs (MFA) were conducted. In addition, to balance the view presented by the Estonian side, two interviews with officials that have had experience in representing a big state in Estonia in the field of cyber security were also carried out.

The thesis is structured as follows. It first presents an overview of the relevant theoretical approaches to small states with the aim to explain the possible role of niche capabilities in a small state's foreign and security policy (chapter 2). The thesis then analyses the case of Estonia by explaining its broader strategy for foreign and security policy and its efforts in the area of cyber security (chapter 3). The subsequent chapter elaborates on the research questions and the methodology of the study (chapter 4). In chapter 5, the results of the interviews are presented. The following chapter of the thesis draws analytical conclusions by discussing both the theoretical and practical implications (chapter 6). The main findings of the thesis are listed in the final chapter (7).

2. Theoretical Approaches to Small States

Since the thesis seeks to identify possible new theoretical approaches building upon the existing literature on small state studies, the following chapter will focus on the historical developments of the study, discuss problems surrounding the definition of a small state and describe the basic foreign and security policy options as presented in the relevant literature. The chapter will then look into the theoretical approaches which can be useful in explaining the role of niches in the context of small states' influence.

The overall development of small state studies could be described as somewhat unstable. First, the incoherence in small state studies is characterized by the broad spectrum of topics taken up by different authors. While analysing the history of small state studies, Olav F. Knudsen (2002, 182) identified three main streams of literature, each having self-contained research areas and separate specialists focusing on them: (1) literature dealing with the basic foreign policy options of small states – neutrality, isolation and alignment; (2) comparative studies on politics and policy formation; and (3) work on issues connected to recognition, self-determination, secession in the context of justifying small state's existence in a world dominated by great powers.

Second, one can also view small state studies as largely influenced by different periods of historical developments. Neumann and Ghstöl (2006, 18) have indicated three distinguishable periods to characterise the influence of global events on small state literature. The first period, from the 1950s until the 1970s during the beginning of the Cold War and the decolonization process, is seen as the height of small state studies, with the study reaching its seminal influence in 1959 when A. B. Fox's "The Power of Small States: Diplomacy in World War II" was published (Knudsen 2002). Fox (1959) focused on the interactions of small and large powers by analysing the cases of five neutral states during WWII.

The next separate period in the study of small states is a described as a "standstill" when some of the previous hypotheses were falsified and the concept of small states struggled to prove its value as an applicable analytical tool (see Baehr 1975; Neumann and Gstöhl 2006, 12). Nevertheless, during the "stagnation" period in the 1980s, there were some

scholars who focused on smallness as a possible variable influencing economic interdependence and development (Katzenstein 1985).

Studies on small states experienced a revival period in the 1990s when, similarly to the decolonization process, a wave of global events created a number of small states mainly due to the end of the Cold War and the start of regional (dominantly European) integration processes (Neumann and Gstöhl 2006, 16). As one would assume, the issues addressed from the perspective of small states throughout the three periods are also dependent on the characteristics of the corresponding periods and finding clear theoretical consistency is difficult. In this regard, the progress of small state literature has also been accompanied by the developments in international relations theory during the three periods described above (I - realism/neorealism; II - neorealism vs. neo-liberal institutionalism; III - rationalism vs. social constructivism) (ibid).

2.1. Definition and the Importance of Context

A substantial issue-area characterizing the different approaches and the "inconsistency" in small state literature is the problem surrounding the definition of a small state. One of the streams within the literature is, in fact, exclusively focusing on the question of definition (see Värynen 1971, Crowards 2002). A widely accepted definition has not been found and this was one of the concerns leading to the described "standstill" period in the studies (see Baehr 1975, 495). Nevertheless, difficulties in defining smallness are certainly not an issue only in the context of states and international relations; one could also view this as an inevitable problem in other disciplines.

In the relevant literature, there are two basic approaches – objective and subjective – typically used to develop a definition of a small state. First, there are authors who prefer strictly measurable criteria to form an absolute definition. An absolute definition can take into account variables such as population, land area, GDP or military capacity which should theoretically indicate the (lack of) power a state possesses. For instance, while analysing soon-to-be member states of NATO, Männik (2004) uses Tom Crowards' framework in which small states are identified by having a population

between 0,5 and 7 million, a land area between 7,000-124,000 km^2, and a GDP from US$ 0.7 to 7 billion. By using these indicators, Männik (2004) indicates the three Baltic States, Slovakia and Slovenia as small states in the context of NATO enlargement in 2004. Naturally, there are also a number of other alternative indicators that have been used as objective criteria (e.g., looking at the number of votes in a specific organisational context, the size of diplomatic corps etc.) (see Panke 2010) The basic problem with applying only objective criteria is the question of drawing lines between small and big, or even between such categories as "micro" and "middle" that are also applied, although not very often, as units of analysis by some authors (see Duursma 1996, Cooper 1997). Another aspect that needs to be taken into account is that the measurable/objective indicators may not necessary characterize the influence of a state in a certain contextual setting (e.g., the effects of military capacity to EU decision making) (Thorhallsson and Wivel 2006, 654).

Since using only objective criteria can be too rigid, some scholars have, in contrast, exclusively applied a subjective method. The classical example here is the approach provided by Keohane (1969, 296) who proposed that scholars should mostly focus on the state leaders' perceptions of the role and their level of impact on the international system. Keohane (1969, 297) claims that self-perceptions of the leaders are the main factor influencing the distinctive behaviour of small states. A similar "psychological" approach is provided by Rothstein (1968) who argues that "a small power is a state which recognizes that it cannot obtain security primarily by use of its own capabilities, and it must rely fundamentally on the aid of others." The subjective method can be summarized by Jeanne Hey's (1995) rather straightforward solution to the problem: "I know one when I see it". The problem with the subjective method is again its arbitrariness in distinguishing different categories.

There are also authors who combine the two methods in order to create a more reliable definition. For example, Goetschel (1998, 17–18) connected the quantitative, relational aspects with the psychological dimension by linking the above-mentioned Keohane's and Rothstein's approach with objective factors that create a "relative power deficit" in influence and autonomy[1] in a *certain environment*. Similarly, Thorhallsson and Wivel

[1] Goetchel includes the factors of power deficit and autonomy based on the work of David Vital (1971)

(2006, 654) argue for the combining of measurable and subjective factors by taking into account the specific contextual setting of the small state(s) under question.

Taking the aforementioned aspects into account, this thesis uses a definition that emphasizes the spatio-temporal context in defining a small state. Therefore, a small state is simply defined as a weak part in an asymmetric relationship (Mouritzen and Wivel 2005). Additionally, to make the definition more universal, the weakness is identified by both subjective and objective criteria which are chosen based on the specifics of the case which is being analysed.

The aforementioned importance of the "contextual factor" could also provide a possible solution to the problem of inconsistency that has put the practical value of small states studies under question. Even by using the simplified Hey's "I know it when I see it" approach, one can easily come to the conclusion that the lion's share of world states could be indeed identified as being small. The large number also comes with very different sets of political environments where the states operate and it would be naive to assume that all the states face similar constrains in all contextual settings – instead, it is reasonable to narrow down groups of states which have commonalities and operate in a similar political environment (Thorhallsson and Wivel 2006, 654). Therefore, one could claim that the instability or the vagueness in the study and the problems surrounding the definition may derive from the fact that there are simply a large number of very different cases which all need a tailored approach to a certain extent. And, as along as one accepts the fundamental claim that smallness, characterized by having less resources and influence, impacts behaviour of states in a specific contextual setting, the lack of theoretical consistency is not a significant issue.

Is Estonia a small state if this approach is applied? Even if all of the aforementioned methods are applied, Estonia easily qualifies as small state by both objective and subjective criteria. Estonia is small by its population (ca 1,3 million), territorial size (45 227 km^2), GDP (one of the lowest members of EU and NATO), military capabilities, and it is also subjectively viewed as a small state. These criteria also hold true if one takes into account the contextual setting: as EU and NATO can be regarded as the most relevant international organisations for Estonia, it is clear that Estonia is identifiable as

a small state which has fewer resources and therefore holds less influence in comparison to big states.

2.2. Basic Foreign and Security Policy Options for Small States

Building upon the importance of context and the aim of the thesis to develop more specific concepts, the next subchapter will identify the relevant theoretical approaches in the literature which could be used to explain the foreign and security policy options of small states in a similar contextual setting as Estonia.

The underlying problem of a small state is its limited resources which translate into less power and influence vis-à-vis big states that have more means, and therefore more influence over smaller units in the international system (see Jurkynas 2014). Since the fundamental objective is to ensure survival, small states need to choose a strategy to cope with the possible threat from big states (Bailes, Wivel, and Archer 2014). As identified before by Knudsen (2002, 182), there are three basic policy options for a small state to survive: neutrality, isolation, or alignment. This conceptualization relies on a realist premise where states operate in a zero-sum, self-interest environment and therefore the security of a less-powered states is seen as being under constant danger (Jurkynas 2014).

Apart from opting for isolation or neutrality, small states have essentially two fundamental policy options in relation to bigger nations which, in the context of the state-centred theory of (neo)realism, can be described as "bandwagoning" or "balancing" (Walt 1987). A small state engages in bandwagoning when they join a dominant large state in order to preserve its security; balancing takes place when a small state joins a less dominant state in order to match up against a bigger threat (ibid).

The neorealist approach is state-centred, but as liberal internationalists, institutionalist and constructivist theories emerged, possible small state options with regard to international organisations became more relevant (Bailes, Wivel, and Archer 2014). The basic policy options in this context can be explained as choice between "hiding" –

opting for neutrality to avoid being involved in the power-games of big states – and "binding" – preventing conflict and creating stability by promoting international rules and institutions to limit big states (see Steinmetz and Wivel 2010, 9–11). For small states, the role of international organisations and norms are seen as reducing general power asymmetries and "cushioning the effects of international anarchy" by providing small states more opportunities to voice their interests and constraining big states with the organisational order (Wivel 2005, 395). By looking at the contemporary world and the prevalent policy choices made by small states, it is clear that the most applied strategy is to rely on international institutions. This is especially the case in the post-Cold War Europe, where most of the small states have integrated to numerous international organisations such as the EU or NATO.

Another relevant factor in explaining the behaviour of small states is the tendency to have a narrow foreign and security policy scope which can be largely dependent on the small states' geographical position (Bjol 1968, 158; Pastore 2013, 69). Therefore, having the need to prioritise and narrow the scope of interests due to limited resources, small states are often preoccupied by issues that are dependent on their immediate neighbourhood (Pastore 2013, 69).

2.3. Strategies within International Organisations and Alliances

Based on the relevant literature, the next subchapter will focus on the specific strategies which explain possible behaviour of small states that have chosen the alignment strategy and seek to maximize their influence in international organisations or alliances (i.e., influence can also be sought in bi- or multilateral relations with big states). For the purposes of the thesis, "influence" is defined in relational terms – influence is achieved when a small state succeeds in making other states or institutions "act in a manner they would not otherwise have acted in" (Evans 1998 via Grøn and Wivel 2011, 524).

As already explained, small states see international organisations as tools which can limit or influence great powers to a certain extent. However, this effect comes with the price of giving away autonomy, which, in turn, may still result in being substantially

influenced by the policies of the organisations that could be dominated by bigger states (Wivel 2005, 396). Essentially, all states operating in international organisations face an "integration dilemma" between autonomy and influence (ibid). The dilemma is especially relevant in the case of "deeply integrated" small states who are in danger of being "entrapped" in certain initiatives without having a decisive say in the process (ibid).

An important aspect that links to small-big relations within international organisations is the issue of burden-sharing (Olson and Zeckhauser 1966). This is especially relevant in alliances where small members are inevitably dependent on the assistance from the large states, whose contributions are essential for the organisation to serve its function (Männik 2004, 23). For example, in an alliance like NATO, big members such as the US may be reluctant to act according to their possibly disproportionate obligations since they can view small states as "free-riders" who use the "public good" of security without bearing their fair burden (ibid).

The literature provides different strategic options for a small state to minimize the dependence, get rid of the "free-rider" image, and even have some influence on policy formation within an international organisations and alliances. A possible strategy to escape the "free-rider" image with the aim to get security assurances or strengthen security guarantees is to support policies that are favoured by the alliance (or by the states that are essential powers in the alliance) (see Männik 2004, 22). This strategy assumes finding a certain balance in the aforementioned "integration dilemma" - e.g., deciding on the level of support to conflict that is not in the direct interest of the small state in order to present a certain level of burden-sharing (ibid).

In addition to just strengthening existing security guarantees or support by big states, gaining influence might also be possible. While analysing the influence of Scandinavian states in EU policy-making, Jakobsen (2009, 86) identifies four factors based on the existing literature on small states[2] to explain how small states could gain impact in a specific issue-area. First, a state must have a "forerunner reputation" in the issue-area where the influence is sought (ibid). This reputation of being a leader or an expert creates much needed authority for the small state in front of its bigger allies who

[2] See Arter 2000; Kronsell 2002; Tallberg 2004; Wallace 2005; Romsloe 2005

possess a “strong” reputation by default (based on their large resources). The second factor identified by Jakobsen (2009, 87) is the importance of developing and using “convincing” arguments that contain innovative, progressive elements and would appeal to fundamental norms and values shared by the members of the organisation. The third important factor is engaging in “honest broker coalition-building”, emphasising neutrality and impartialness to highlight the aim to work for the common interest of the organisation by the small state (ibid). In this context, if a small state “breaks” the norm and clearly pursues national interests that are not commonly accepted, other states may “punish” the state by blocking or not cooperating on the self-interested policies (ibid). The fourth factor that Jakobsen (2009, 88) identifies is the importance of actually allocating financial and human resources to the issue-area.

Another complementing strategy for a small state to maximize influence is to act as a “smart state” (see Joenniemi 1998, Arter 2000; Wivel 2005; Grøn and Wivel 2011). The concept was initially developed with regard to small states operating within the institutional environment of the EU, but it is the view of the author that the approach is not highly context dependant and the logics can be also applied to other organisations. The smart state strategy has three fundamental characteristics (Grøn and Wivel 2011, 529). First, since a small state has limited resources to pursue a broad agenda, its goals and means have to be highly focused with its preferences (ibid). In this regard, smart states have to focus on issue-areas which are not regarded as of vital importance by sticking to “low politics” (e.g., not military but economic, cultural and climate issues) where achieving influence is seen as achievable (Wivel 2010, 25). Second, the “political substance” of the strategy has to provide a solution to an issue that has also identified as relevant by most of the relevant (big) actors in the organisation (Grøn and Wivel 2011, 529). The third aspect in the strategy for a smart state links with the previous “honest broker” model presented by Jakobsen (2009) – initiatives have to be dealt with by acting as a neutral party that focuses on the common good of the organisation (Wivel 2010, 25). In this regard, the smart state approach argues that the initiatives must not conflict with other general initiatives of the organisation and they cannot be too closely associated with the interests of other (bigger) actors in the organisation, adding a relevant point to Jakobsen’s reasoning for this behaviour (ibid). While self-interest oriented great powers in the organisation view a small state as an honest broker, the

state can “punch above its weight” and have an impact on *selected* issue-areas (Wivel 2010, 25)

2.4. Niches Generating Influence

The next chapter will first draw upon the (scarce) examples in the literature that have explained the specific role of niches or specialisations in small state foreign and security policies. It will then map out the concepts which might be useful to analyse the possible broader influence a niche capability might generate.

The strategy to allocate resources to focus on specific areas can be relevant for a small state to gain influence in *military* alliances. In order to do that, small states need to utilise its limited resources to develop niche specialisations in the context of military operations (Rickli 2008). By adopting a niche strategy, a small state can gain “co-decision power at the operational level and strategic leverage if its specialized capabilities are desperately needed” (ibid, 318). An alternative to the niche capabilities strategy within a military alliance, is to adopt “a framework or a lead nation” strategy by taking up the responsibility for the command and control (C4I) of an operation (e.g., Sweden and the Nordic EU Battlegroup) (ibid). Nevertheless, the lead nation strategy also implies a certain level of role specialisation. The possible problem with these strategies is that the state would not have enough resources to develop capabilities in other vital sectors, making the state individually vulnerable and dependent on its alliances (ibid). Furthermore, a niche strategy may lead to recognized responsibilities, making the small state actions more open to criticism (ibid). On the other hand, influence is gained by having unique capabilities and expertise which can be used as “bargaining chips” in international negotiations (Jurkynas 2014).

From a constructivist perspective, a possible “specialisation” strategy for a small state may entail acting as a “norm entrepreneur” or a “norm advocate” (Finnemore and Sikkink 1998). By acting as a norm advocate, a state is strongly committed to specific set of norms, and acts to promote them to shape the behaviour of others (Björkdahl 2008, 137). If a state also acts as a forerunner (i.e., abides strictly by the norms) and the

norms themselves are morally appealing, it becomes more convincing to others and therefore is likely more influential in the subject matter (ibid). While analysing Sweden's initiatives regarding conflict prevention in EU, Björkdahl (2008, 138) listed a typology of norm advocacy tactics: framing (constructing a normative "fit" to convince a target audience), agenda-setting (introducing a new idea or bringing a particular issue to the forefront), diplomatic tactics (e.g., bilateral consultations or coalition-building) and, making most of the institutional opportunities provided by the organisation (by referring specifically to the EU's rotating presidency).

As mentioned before, some authors have made a distinction between small, middle and large powers. In this respect, the concept of "niche diplomacy" has been used in describing middle powers who are also seen as lacking capacity to be influential in many sectors (see Cooper 1997; van Genderen and Rood 2011; Henrikson 2005). Some have linked niche diplomacy to the logic of economics – for a diplomacy to "generate returns", a state has to carefully select "policy product lines" with an accurate reading of the political market conditions and assess whether the policy position can be "sold" to domestic and foreign audiences (Henrikson 2005, 68). Therefore, creating and maintaining a niche needs publicity which can be mainly achieved through advocacy by the state's officials and diplomats (ibid, 70). An interesting aspect in the niche diplomacy framework is the claim by Henrikson (2005, 71) that the specialisation has to be more or less permanent, (e.g., an advantage based on locations or traditions). Having said that, Henrikson (2005, 72) agrees that it is difficult to keep a niche in the "dynamic flux of globalisation" and therefore constantly adapting to the environment is necessary.

Most of the abovementioned theoretical approaches which focus on niches or specialisations do not describe or mention passingly the influence that a small state might gain *outside* of the area of specialisation. Therefore, theoretical approaches which could provide possible explanations on how small states can gain *broader* influence by having a niche specialisation will be explored below.

In this context, the concept of "side-payments" may be useful to explain the possible phenomena. To use a very broad definition, "side-payments refer to compensatory measures aimed at facilitating agreement between actors" and the "measures do so by roughly balancing inequities arising from cooperation" (Friman 1993). The concept is

often linked with purely economic matters as side-payments are mostly seen either as monetary or other indirect compensation in a material form (ibid). As this thesis applies an inductive approach and broader influence in foreign and security policy is analysed, the notion is broadened: i.e., a side-payment is viewed as it could also encompass security assurances or non-material concessions which, in essence, can be translated as the influence gained by the small state.

The range of possible side-payments that a small state may seek or receive can be therefore rather wide. For instance, while analysing Denmark's political gains from the US as a result of strongly supporting US policies by contributing troops to operations in Afghanistan and Iraq in the early 2000s, Henriksen and Ringsmore (2012, 158) identified three possible types of benefits received: reputation, access and concrete gains. A certain hierarchy between those gains was identified: a positive reputation can lead to increased access to key policy-makers which is a perquisite for being able to influence the foreign policy of the partner (ibid). Henriksen and Ringsmore (2012) claim that through its privileged relations with the US, Denmark had concrete influence to US policymaking, and got concrete gains, although limited, in the areas of military assistance, intelligence, and economic trade. It is also pointed out that a prominent reason behind Denmark's success is the fact that it did not exploit its good reputation too obviously or aggressively (ibid, 160). Denmark's pro-US military policies where not exactly a niche but rather a prioritisation of or specialisation in a certain policy, which allowed the state to stand out in the eyes of an important ally in contrast to other states similar to Denmark (ibid).

Denmark provides a relevant example as it explains how influence was achieved in a bilateral relationship. Having a good standing with individual great powers plays certainly an important part in a small state's strategy, but having an influence within an international organisation is also necessary. In this context, presumably the side-payment from providing a niche capability works in a similar way – being a capable player in a certain field increases reputation which leads to more willingness to cooperate by the members of the organisation, allowing to seek policies beneficial to the small state. Since coalition building is regarded as one of the (dominant) ways for small

states to have influence, building bilateral relations within international organisations by using a niche can therefore be beneficial (Björkdahl 2008, 138; Jakobsen 2009, 86).

With regard to side-payments and transforming influence from one policy area to another, the concept of "issue-linkage" may be relevant if the possible broader effects of niches are analysed (Keohane 1982, 340). The neoliberal institutionalist Keohane states that "international regimes often seem to facilitate side-payments among actors within issue-areas covered by comprehensive regimes, since they bring together negotiators to consider a whole complex of issues." Here, Keohane (1982, 340-341) is referring to the literature on the European Community (now the EU) and the "spillover" effects in bargaining by presenting the assumption that international agreements can be expanded to other issue-areas through side-payments (ibid, 341). In this regard, a successful spillover of influence may depend on the issue density (ibid, 339). Keohane speaks of issue density in the context of whether it is profitable for governments to establish international cooperation frameworks or not, but similar logic can also be applied to small states and niches. Simply put, a small state should ideally invest in a niche with high issue density which would mean that other issue-areas arise within the niche's "policy space". The so-called denseness of the niche specialisation may be an influential factor in determining the possibility to successfully receive side-payments. In addition, only choosing a certain area won't lead to success; it is also claimed that issue-linkage will not work if the "distribution of benefits from an agreement is fairly even across countries" (Tollison and Willett 1979, 426). Taking this into account, if a small state that is seeking side-payments through issue-linkage, the niche specialisation has to be something of unequal value to the partner that would allow the small state to pursue a certain gain in another area.

Overall, the literature on small states and the possible spillover of niche influence is rather limited. One of the few examples is provided by a case study analysing the Netherlands and its water diplomacy (van Gender and Rood, 2011). In addition to gaining influence in issues regarding specifically water diplomacy, the authors also cover the possible spillover effects – the effect of the niche specialisation is characterised as a "catalyst for bilateral relations", when, in addition to establishing new relations, the scope of cooperation also expands to other areas (ibid, 16). Sweden has

similarly reported to have received some broader gains in acting as a norm entrepreneur in the areas of conflict prevention and environmental policy (Björkdahl 2008; Kronsell 2002). Nevertheless, the possible phenomena of niches creating possible broader effects are mostly neglected or insufficiently covered in small state studies and further research on it is expected (see Kronsell 2002, 17; Nasra 2010, 1).

As presented above, a niche or a specialisation can theoretically produce different types of wider influence. The notion of influence can be linked with the concept of "power" – this can be useful in understanding the possible type of influence a niche capability can create. Many have explained the concept by distinguishing two categories. First, "hard power" is seen as having the ability to influence another state through coercion, which is usually achieved through instruments of military intervention, coercive diplomacy or economic sanctions (Wilson 2008, 114). "Soft power", on the other hand, is identified as an ability to influence others through attraction and persuasion (Nye 1990). Soft power, according to Nye (1990, 170), is based on ideas rather than "tangible" instruments as it seen as a combination of state's qualities such as reputation, culture and diplomatic skills. From the perspective of small states, one can assume that small states, having limited resources, are naturally more prone to possess and use soft power (Stringer 2013; Grøn and Wivel 2011, 524). However, it might also be theoretically possible that a small state develops a niche capability that can be used as a coercive measure (Dür and Mateo 2010, 684).

To further apply the concept of hard and soft power in the context of this thesis, the principle can also be used to explain the possible types of side-payments that could be received by having or using a niche capability. On one hand, a niche might generate soft power, i.e., it can create a positive international image for the small state, therefore making it easier to gain support to its initiatives from international organisations or strategic allies. The soft power concept could also be linked to the term "diplomatic capital", seen as a tradable asset in the field of diplomacy, that a state representative gains through positive demonstration of its competences, reputation and authority (Adler-Nissen 2008, 670). Hence, if the niche has generated positive reputation, it is possible that a small state uses it to get wider gains – this also follows the logics presented in the example of US-Denmark relations explained before (Henriksen and

Ringsmore 2012, 158). On the other hand, a niche that creates hard power might mean that the side-payment received by the small state could be a direct compensation or a trade-off of capabilities in international negotiations.

As presented above, there are theoretical concepts that might be useful to explain the role of niche capabilities in generating influence for a small state – the possible applicability of these concepts will be discussed in paragraph 6, after the case of Estonia and the role of its cyber security niche is analysed.

3. The Case of Estonia

The next chapter will first analyse the development of Estonia's strategy for foreign and security policy since regaining independence. In this context, the notions of "foreign" and "security" are considered as being interrelated – i.e., the analysis will look at Estonia's foreign policy choices that can be considered as affected by security considerations. This subchapter will be followed by a paragraph focusing on Estonian efforts related to the domain of cyber security.

3.1. Estonia's Foreign and Security Policy as a Small State

After regaining independence in 1991, Estonia faced challenges and had to choose between foreign and security policy options that can be seen as very typical to a small state. According to Riina Kaljurand (2013), Estonia had three theoretical foreign and security policy options: neutrality, close cooperation with Russia and other countries of the Commonwealth of Independent States, or integration into Western economic and security structures. These policy options were rightly marked as "theoretical" as it was clear that after the Soviet occupation, the only viable and acceptable option was alignment with the West (ibid). This orientation corresponds to the notion that the scope of a small state's foreign and security policy is often narrowed by the effects of its geographical surroundings – the main factor influencing Estonian policy decisions has dominantly been the negative historical experience with neighbouring Russia (Pastore 2013, 69; Jurkynas 2014)

There was a general consensus among the political elite right after regaining independence that the option of neutrality should be excluded as the policy would not assure survival for a small state (Vahtre 2011). Reliance on neutrality during the first independence (1918-1940) was viewed as a failure since it did not prevent annexation by the Soviet Union (Kasekamp 2013, 99). Andres Kasekamp (2013, 99) has described the effects of this negative experience as one of the reasons behind Estonia's foreign and security policy orientation after regaining independence: "the legacy of that tragic

experience and accompanying anxiety about its security led the restored Estonian state to pursue a policy of gaining reliable allies and embedding itself densely into numerous international organisations". In addition to seeking formal membership in international organisations, Estonia pursued the "binding" strategy by promoting the importance of international norms (see Mälksoo 2008).

The alignment strategy, i.e., integration to the West, encompassed both gaining membership in international organisations and developing bilateral relations with Western nations. In this context, the "ultimate goal" was to achieve membership in NATO and EU which were both viewed as the main security guarantors for the small state (Kaljurand 2013, 63). As a result of a stable policy direction, support from foreign partners, and vigorous political and diplomatic efforts, Estonia successfully joined both organisations in 2004 (ibid). In order to achieve that, Estonia had to contribute the lion's share of its limited (diplomatic) resources towards the objective (Mihkelson 2013). By doing so, Estonia was able to prove itself as a worthy member of the organisations by modernising its structures according to the accession criteria.

The tendency to strictly follow the requirements of international organisations has been a constant characteristic for Estonia before and after 2004, reflecting the priority to be strongly integrated into the institutions (Kasekamp 2013). Since getting the Membership Action Plan (MAP) from NATO in 1999, Estonia has aimed to bring its defence forces in line with NATO's requirements (Kaljurand 2013, 64). In this context, the most commonly highlighted aspect is the defence expenditures requirement set by NATO (2% of GDP). Since its membership in NATO, Estonia has had a steady commitment to meet the threshold and the goal was reached in 2012, making Estonia one of the very few NATO members to have ever met the target (see Estonian MoD, *Eelarve*). Estonia has also actively been contributing to several NATO-led operations: the most prominent example of that has been Estonia's participation in the International Security Assistance Force (ISAF) in Afghanistan (Estonian MFA, *Estonia and NATO*). In fact, participation in ISAF, an out-of-area conflict that has no direct threat to Estonian security, has been stated as one of the foreign policy priorities as a NATO member (ibid). Active efforts in NATO can be seen as based on Estonia's will to avoid being seen as a "free-rider" who

offers only a minor and therefore unbalanced part that is required to "be worthy of" being under the collective defence umbrella of the Alliance (see Männik 2004, 30-31).

In the context of "hard" security guarantees, NATO and its collective defence is certainly viewed as the main security guarantor for Estonia, but EU integration has also been seen as equally important. Here, again, Estonia excelled in the European integration by being the "best pupil in class" who carefully tried to meet the membership requirements without seeking any possible country-specific exceptions that might hinder the joining process (Kasekamp 2013, 99-100). Once in the EU, Estonia kept the strict policy of following EU requirements. For example, amidst the Eurozone crisis, it adopted the Euro in 2011, which was somewhat uniquely stated by the then Prime Minister Andrus Ansip to be a "matter of security" (ibid). With reference to fiscal matters, Estonia has again proven to be one of the few EU Member States that has been able to act according to the requirements of the organisation. The "model student" role was, for example, presented when Estonia showed its consistent support to the union by contributing to the European Financial Stability Facility (EFSF) and the European Stability Mechanism (ESM). The decision to support economically more developed members who have not acted according to EU rules received criticism from the public, but reluctance to do so was not shown by the decision makers (Kasekamp 2013, 101). Estonia has also contributed to several military missions and structures operating under the EU banner.[3]

In terms of bilateral cooperation, Estonia's most prominent alliance has clearly been established with the US in what could be seen as a bandwagoning strategy from a neorealist perspective on small state behaviour (Berg and Ehin 2009, 6). Cooperation and good relations with the US has been one of the top priorities for Estonia since regaining independence. Estonia has provided troops to the US-led mission in Iraq in 2003 which can again be seen as a move to support a strategic ally in an out-of-area conflict to get security assurances and not to be seen as a "free-rider" (see Mouritzen 2006). The decision to support the mission could also be indicated as an example where Estonia showed that its strategic priority is to bandwagon with its main ally rather than being a strong proponent of international norms. Furthermore, in the context of military

[3] For example, Estonia contributes to the EUFOR RCA (Central African Republic), EUTM (Mali), KFOR (Kosovo), and UNTSO (Middle-East), see Estonian Defence Forces. *Operations abroad.*

matters and US-Estonian relations, the proportionally large contribution to ISAF and other efforts in the US-dominated alliance are also strong factors in the relationship with the US (The White House, *The United States and Estonia - NATO Allies and Global Partners*). Indeed, Estonia is seen as being a "striver" in the ISAF mission – a state who has contributed more substantially to the mission in order to have a more favoured position in the relations with the mission's "owner" and the hegemonic power in NATO, the US (Marton and Hynek 2012).

To conceptualise and simplify the overall historical development of Estonian foreign and security policy objectives, one could divide it into two main periods: (1) efforts towards integrating to the main Western organisations, and (2) getting used to, finding a role and strengthening the state's position within the Western structures (see Laar 2011; Maasikas 2014; Ilves 2011; Vahtre 2011; Sillaste-Elling 2013). While the policy orientation was very clear in the first period, there has been a certain "diffusion" of specific foreign and security strategies after becoming members of EU and NATO.

As presented above, Estonia continued its policy to be an exemplary member state in different organisations by acting according to the rules and supporting the strong role of these organisations. Also, it further integrated itself to Western structures by, for example, becoming a part of the Schengen Area, adopting the Euro and becoming a member of OECD. Building upon those developments, some have claimed that since the basic goals have been achieved, the aim is to move towards a stabilisation period where the focus should be on strengthening the established ties (see Maasikas 2014). Therefore, in general, Estonian foreign policy has still been seen with its main focus on work within international organisations as they provide an effective tool for small states to have their "voices" heard (Kolga 2013; Mihkelson 2013). In this context, Estonia has widened the scope of the international organisations that receive active attention as there is more "diplomatic resource" available after achieving membership in EU and NATO (Sillaste-Elling 2013).

For example, in the context of the United Nations (UN), Estonia's strategy has been seen as being actively involved in different global initiatives, building coalitions with like-minded states, and using the opportunities provided by the institutional bodies within the organisation (Kolga 2013). The rationale behind dealing with global issues in

the UN is linked again with the aim to minimise the “free-rider” image: Estonia seeks to act as an ”unselfish” actor that works for global issues and therefore, in turn, creates a basis to get support by other states once itself might need it (ibid). Here, the continuation of the “binding” strategy towards international norms could be identified as well: Estonia is basing its actions on norms that ultimately have assured its independence through gaining a position in the Western system (e.g., democracy, rule of law, human rights, transparency etc.)

Nevertheless, as small states inevitably cannot focus on a very broad agenda that does not correspond to its core interests, Estonia could still be viewed as mainly operating in a more narrow scope of topics. Naturally, a bulk of activities have been dominated by the need to “mitigate” the Russian threat: be it “informing” the Western states of the possible threat and highlighting the need to deal with it, or supporting other former Soviet Union states that are not under the “umbrella” of Western structures or the influence of Russia (Laar 2011). For example, Estonia has been engaged in development cooperation by building on its experience as a successful post-Soviet reformer and moderniser to countries like Ukraine, Moldova, and Georgia (ibid). Estonia has also been actively involved in the EU’s Eastern Partnership process (Ehin 2010). Paradoxically, being actively involved in the Eastern Partnership process has been identified as a move from the traditional “Russia-only” orientation towards a more EU-centric view (Made 2011).

The topic of Russia became once again undoubtedly the top priority for Estonia after the 2014 Ukraine crisis. The situation has been seen as a confirmation that the threat from Russia exists – the notion that has been constantly highlighted by Estonia to its Western partners. A turn back to Estonia’s focus on traditional security concerns was clearly visible if one takes into account Estonia’s main goal to assure the efficient functioning of NATO’s collective defence during the Wales summit in 2014 (Sakkov 2014). This aim was considered successfully achieved as NATO’s air-policing mission remained in the Baltics, companies of the US Army confirmed continuing their rotation in Estonia, and NATO agreed to develop a Very High Readiness Join Task Force in response to the post-Ukraine security environment in Europe (ibid). Effects of the Ukraine crisis to Estonian foreign and security policy strategy remain to be seen, but it is fair to assume

that the event will not result in drastically new directions; instead, it is probable that Estonia will strengthen a stance which prioritises the small nation's main security threat.

The latest National Security Concept of Estonia (2010) helps to further explain Estonia's security policy in the context of foreign affairs. First, Estonia adopts a broad security concept, i.e., security is not only based on military capabilities and involves all sectors of society. And second, the document summarises the main security strategy for foreign policy: "Estonia strives for an international environment necessary for ensuring its security and pursues the most favourable possible position within that environment. Estonia's foreign policy objective in reinforcing security is the stability of the security environment, the functioning and unity of the European Union and NATO, strong transatlantic co-operation, the promotion of human rights and democratic values as well as extensive bilateral and multilateral relations."

In sum, Estonia's foreign and security policy has followed classical logics of a small state. Estonia has chosen the alignment and binding policy with the West that has been strongly influenced by a traditional threat perception of Russia. It is evident that Estonia views integration into international organisations and close relations with Western allies as the main guarantors of security. Estonia therefore supports the strong role of the organisations and aims to prove itself as a valuable member within them. And, if one looks at the latest developments and support from allies with regard to the crisis in Ukraine and NATO's response, this strategy has been effective and justified.

Nevertheless, there are also many who have criticised Estonian foreign policy strategy as being stuck in old visions, lacking clear objectives and fresh ideas to maximise Estonia's role within the "comfort zone" of Western structures (Ilves 2011; Laar 2011; Mihkelson 2013). The orientation has been identified as firmly established and (too) stabilised, as Luukas Ilves writes: "as a small nation, we are interested in the existence of a boringly liberal and open society: we strive for an integrated Europe, for a world that adheres to multilateral agreements, for markets that are open and for freedom and democracy." To overcome this vagueness or even a "standstill" in the foreign policy strategy, many have discussed the idea to utilise the cyber-related initiatives to create a bigger influence for Estonia in international affairs (see Ilves 2011; Laar 2011; Areng

2014); Estonian developments in the area of cyber security will be separately introduced in the next subchapter.

3.2. Estonia and the Cyber Security Niche

To assess Estonia's activities and present the existence of the niche of cyber security, the next chapter will map out the initiatives that can be regarded as substantial when comparing Estonia to other states. Before doing so, a definition of "cyber security" is provided and the specific characteristics of this issue-area in the context of small states are described.

Firstly, there is no agreed definition of "cyber security" (Klimburg 2012, 7). Without going into further detail on this somewhat problematic issue, this thesis adopts a broad definition of "cyber security" that does not set any specific limitations with regard to the secured technologies or the possible range of measures to achieve a certain state of security. The International Telecommunication Union's (ITU's) approach is used; cyber security is defined as a "collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, trainings, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets" (International Telecommunication Union, *Definition of cybersecurity*.) By applying this approach, the term "cyber security" can, in the context of Estonia's efforts, cover a wider range of activities from developing specific military cyber defence capabilities to generating international cyber-related policies.

In the context of small states, cyber security is seen as an area that can provide small states an opportunity to "punch above their weight" (Nye 2010, Areng 2014, Austin 2014). Joseph Nye (2010) has described the effect of "cyber" as follows: "the low price of entry, anonymity, and asymmetries in vulnerability means that smaller actors have more capacity to exercise hard and soft power in cyberspace than in many more traditional domains of world politics." Nye's approach highlights the opportunities to use offensive cyber means to exercise power within the cyber domain. Others have, by taking Estonia as an example, claimed that cyber security and other digital affairs can be

a suitable “comparative advantage” to small states to have more clout in international relations (Areng 2014). This comparative advantage is based on utilising the positive features of a small state: flexibility and effective internal communication mechanisms; proneness to international cooperation and being able to act as an “altruist” in international relations; and the natural need to save resources that encourages digital innovation (ibid).

In order to understand Estonia’s current position in matters of cyber security, roots in historical developments have to be explained. Estonia was left with an absent Soviet infrastructure after regaining independence in the early 1990s (Tuohy 2012). To bridge the cap, the government started to strongly focus on developing its information systems by heavily investing in information technology and digital solutions (e.g., the Tiger’s Leap programming for computing education) (ibid). The early initiatives resulted in successful e-government solutions such as the ID-card system which allowed Estonia to be the first country in the world to use a legally binding e-vote in municipal elections (ibid). As for the latest [2014] developments in this context, Estonia introduced the concept of e-residency that has created wide international interest (see Shabbir 2014). What is more, Estonia’s private sector has been praised for producing successful IT solutions. For example, Estonia has been dubbed as the birthplace for many globally successful programs such as the file sharing platform Kazaa, or most prominently the telecommunications application Skype. The development of innovative e-services has its direct link to cyber security as it is natural that the solutions also have to include different security measures (see Ilves 2013)

Cyber security as a more distinguished issue-area became firmly linked with Estonia when a series of cyberattacks targeted many Estonian public and private organisations such as government institutions, media portals and banks. The distributed denial of service attacks occurred in the spring of 2007, during and after the Bronze soldier crisis (see Tikk, Kaska, and Vihul 2010, 18-24). While analysing the actions of Estonian officials and IT specialists after the crisis, it is claimed that they successfully managed to securitize the incident in such a way that it was accepted by international media as an unprecedented “first war in cyberspace” (Hansen and Nissenbaum 2009, 1169). Although Estonia had been successfully implementing and promoting its e-government

initiatives to the international public, the 2007 attacks arguably created a strong momentum, global image and an appreciated experience to specifically focus on the area of cyber security. To give a clear example of the experience gained during the 2007 attacks, the Estonian Computer Emergency Response Team (CERT) cooperated actively with other CERTs and specialists from different international organisations such as NATO, EU dispatched their security teams (Tiirmaa-Klaar 2010). Also, in 2007, Estonia established the unique Cyber Defence League that consolidates volunteer cyber security specialists; the organisation is a part of the Estonian Defence League and, inter alia, participates in crisis management to protect with protecting Estonian critical infrastructure (Estonian Defence League, *Estonian Defence League's Cyber Unit*). What is more, in 2008, Estonia also stood out by being one of the first countries in the world to publish a cyber security strategy (Pernik and Tuohy 2013).[4] A second cyber security strategy was adopted in 2014, making Estonia again one of the few countries that has an updated version of a cyber security strategy.

Since the attacks of 2007, Estonia has proved to be an active advocate of cyber security policies in NATO. For example, in response to the 2007 incident, Estonian politicians promoted the notion that a cyberattack could reach the threshold of Article 5 (Hansen and Nissenbaum 2009). The topic of cyber defence rose clearly to the Alliance's policy agenda after the 2007 attacks and Estonia was regarded as one of the most active members in assisting NATO in developing its first policy on cyber defence (Tiirmaa-Klaar 2010). The NATO Cooperative Cyber Defence Centre of Excellence (CCD COE), a NATO accredited research centre, was also established in Tallinn in 2008. The centre was not created, in fact, in response to the 2007 cyberattacks – the idea of establishing a NATO's cyber defence centre was already proposed by Estonia in 2004, and the concept was approved by NATO Supreme Allied Commander Transformation (ACT) in 2006 (NATO Cooperative Cyber Defence Centre of Excellence, *History*). Although Estonia only provides host nation support to the CCD COE and the international military organisation works officially for NATO and its Allies, its work has been certainly fed into the positive image of Estonia. For example, in 2013, CCD COE commissioned a project which resulted in the "Tallinn Manual on the International Law Applicable to Cyber Warfare" – a research on how the existing international law applies

[4] A similar strategy was adopted before Estonia only by Sweden, the US and Germany

(focusing on *jus ad bellum* and *jus in bello*) to cyber conflicts and warfare (see Schmitt 2013). Although the book was created by a group of international experts, it received a great deal of international publicity and just the name itself, "Tallinn Manual", put Estonia on the map in the discipline of international law and amplified Estonia's image as an substantial actor in the field of cyber security (Mälksoo 2013). Estonia has also hosted NATO's cyber defence exercise "Cyber Coalition" in 2013 and 2014. Furthermore, in 2014, the Estonian Defence Forces successfully proposed the Estonian cyber range to be used as the Alliance's main cyber defence training field (NATO Allied Command Transformation 2014).

NATO may be regarded as the organisation where Estonia's role in cyber security is most visible, but activities in other organisations can also be identified. Estonia has been arguably successful in many cyber security-related activities in the EU that mainly focuses on the protection of civil infrastructure (Tiirmaa-Klaar 2010; Czina 2013). In this regard, the experience with the e-government services and the 2007 attack again helped to promote Estonia's position in cyber security issues within the EU. For instance, the Estonian Ministry of Economic Affairs and Communications showed initiative by hosting an EU ministerial meeting to push the idea to create an EU policy for defending critical infrastructure (Tiirmaa-Klaar 2010). The EU's 2010 Internal Security Strategy is also described as being influenced by the Estonian discourse on cyber security threats (Czina 2013). A very tangible proof of Estonian position in the field is that the EU IT Agency, managing large-scale IT systems in the area of EU Home Affairs, has been established in Tallinn. The aforementioned examples all serve as a proof that, at large, Estonia has been able to successfully have more influence than other small states in influencing cyber security related developments in the EU – arguably, this was done, referring to small state strategies, by (1) acting as a role model; (2) agenda-setting by political leaders; (3) and using special framing of the issue[5] (Czina 2013).

The United Nation's (UN) has also been increasingly active in cyber security issues. In the UN, the First Committee (the Disarmament and International Security Committee) serves as one of the few forums where global cyber security issues are discussed

[5] Interestingly, the research found that coalition-building was not an important factor in Estonia's influence on cyber security initiatives in the EU

between great powers (see Lewis 2014). Since 2001, the committee has established four groups of governmental experts (GGEs) to discuss developments in the field. The third report (A/68/98) is seen a substantial breakthrough in the context of international cooperation on cyber security norms (ibid). The group of experts consisted of only 15 representatives and Estonia was the smallest state in the discussion among the world's main powers. Estonia is also part of the fourth GGE which was established in 2014.

In addition to the most relevant international organisations, Estonia has stood out in such organisations as Organisation for Security and Co-operation in Europe (OSCE) and the Council of Europe where it has been acting as an "agenda-setter"' by leading and promoting some cyber security related initiatives (Tiirmaa-Klaar 2010; Pernik and Tuohy 2013). Furthermore, Estonia has been an active participant in the other activities concerning broader topics related to cyberspace: for example, the meeting of the "Freedom Online Coalition" was hosted in Tallinn in 2014.

Estonia has also successfully developed bilateral cyber security cooperation mechanisms. The most relevant example of this is certainly the "US-Estonian Cyber Partnership Statement" signed in 2013 between Estonian foreign minister Urmas Paet and US Secretary of State John Kerry (see Maldre 2014). Again, the bilateral agreement is regarded as something that is unprecedented (bilateral) state practice and therefore a sign of Estonia's leader position in the field (ibid). Official statements made by both states after signing the agreement quite bluntly summarise the essence of the bilateral cooperation as the US department of State statements emphasised that "Estonia is a key ally of the United States and a recognised leader on issues of cyber security and internet freedom."; and the Estonian Foreign Ministry responded: "Estonia's security is better than ever before, and this is largely thanks to US support" (ibid). Regarding other big states involved in bilateral relations in cyber security, collaboration with France is also an interesting example (Pernik 2014). The Estonian-French cyber security cooperation that is mainly taking place between educational and military organisations (ibid).

An important aspect that cannot be left out in explaining Estonia's substantial role in promoting cyber security is the initiatives taken by the Estonian President Toomas-Hendrik Ilves, who has been, in addition to regularly speaking on the topic in different high-level meetings and conferences, chosen to chair the Steering Board of the

European Cloud Partnership. President Ilves was also asked to be the co-leader of the prestigious Advisory Panel of the World Bank report “Internet and Development”. Furthermore, the former Prime Minister of Estonia, Andrus Ansip, serves as the European Commission Vice-President for the Digital Single Market since 2014.

In conclusion, Estonia has been able to develop a niche capability in the field of cyber security that is internationally recognised (Kaljurand 2013). Due to the specialisation, Estonia has had remarkable influence in international settings in the matters of cyber security (Pernik and Tuohy 2013, 5). Taking these developments into account, maximising the effects of cyber-related initiatives with regard to Estonia’s foreign policy is identified as one of the challenges in the near-future (Sillaste-Elling 2013; Ilves 2011).

4. Research Method and Questions

This thesis seeks to look into how small states utilise niche capabilities to gain wider influence in foreign and security policy by examining the case of Estonia and its international efforts related to cyber security. Here, once more, it has to be highlighted that the terms of "foreign" and "security" policy are seen as interconnected – i.e., the focus is on foreign policy initiatives which aim to improve Estonia's international security posture.

Since the theoretical basis on the particular topic of using niches to gain wider influence is insufficient, the thesis adopts an inductive approach with the aim of identifying possible new approaches to conceptualise small state behaviour. The lack of theoretical concepts on the possible phenomena is also why a single-case study is applied – the objective is to seek "conceptual innovation" by identifying the "general from the particular" (Bennett and Elman 2007, 178). Focusing on a single case provides the opportunity to obtain a necessary level of detailed knowledge to provide new conceptual ideas (ibid). Nevertheless, in doing so, it is crucial to highlight that the generated ideas are most likely to apply to small states operating in a similar contextual setting as Estonia.

The reasons why Estonia was chosen as a case study are twofold. First and foremost, as presented in the chapters above, Estonia, being a "textbook example" of a small state, has focused on and been successful in being a forerunner in a specific issue-area. Therefore, Estonia is seen as a representative example that can be used to analyse the role of niches in a small state's foreign and security policy. Second, in addition to the theory-oriented aim, the thesis also seeks to produce practical value in analysing Estonia's "niche-oriented" strategy towards foreign and security policy by identifying the success factors as well as discussing how to tackle the possible challenges that may occur in the future.

Inspired by these aims and the theoretical approaches outlined before, the main research question is the following:

> How does Estonia utilise its cyber security niche to have wider influence or gains in foreign and security policy?

The research question is further elaborated by looking into the following sub-questions:

- What have been the effects of having the cyber security niche for Estonia's foreign and security policy?
- Is Estonia seeking wider influence in foreign and security policy by utilising its cyber security niche and what type of influence or gains are sought?
- What attributes of the niche have contributed to Estonia's success in developing the internationally recognised capability?
- How could Estonia maintain the niche capability?

The case study is based on semi-structured interviews that were carried out with Estonian public officials during the summer and autumn of 2014. As the study takes an inductive approach, the method of semi-structured interviews were chosen since it provides the interviewer flexibility by using open-ended questions and the possibility to ask for specifications or follow-up questions (May 2001). As the thesis looks into the role of the niche with regard to wider foreign and security policy, the interviewees were selected from the two institutions that are involved with these areas on the policy-making level: the Estonian Ministry of Defence (MoD) and the Estonian Ministry of Foreign Affairs (MFA).[6]

Eight interviews were conducted with low, medium or high level officials who were either working or had recently been working for the MoD (5) or MFA (3). The specific positions and the names of the interviewees were anonymised. While illustrating the results with quotes, the interviewees were assigned with a number and a letter to demonstrate their position ("D" representing the MoD and "F" the MFA). The respondents were also classified as either officials whose duties were mainly related to

[6] Other stakeholders in matters of cyber security are, inter alia, the Ministry of Economic Affairs and Communications, the Estonian Information System's Authority (EISA), Estonian Defence Forces (EDF), and the Government Office

cyber policies or who were responsible for dealing with broader questions of foreign or security policy. Since most interviewees had had some experience in both of these categories, the distinction was only mentioned if their answers could have been influenced by a lack of expertise in the subject matter analysed.

A predesigned framework of questions and topics was used during the interviews (see Appendix 1). The questions asked during the interviews varied to a certain extent based on the specific background, experience, and answers of the respondent. The aims and general research questions of the thesis were introduced to the interviewees beforehand. Seven out of eight interviews were recorded and later transcribed; one interview was noted down as the respondent preferred not to be recorded. The transcriptions and notes from the interviews were compiled, analysed, and relevant ideas were identified. The results were categorised based on the identified topic areas.

A possible weakness in using the aforementioned research design is the reliance on the Estonian internal position which can heavily depend on the respondents' assumptions on the effects the cyber security niche creates within international organisations and in relations with big states. Therefore, the thesis also includes a tentative chapter which focuses on Estonia's strategic allies and their view on the effects of the cyber security niche to Estonian foreign and security policy. For that end, two interviews[7] were conducted with individuals who have had experience in representing a big state in Estonia in the sphere of cyber security. Again, the persons and concrete positions were anonymised. The objective of this brief chapter was to have a general impression of how big states might view the role of the cyber security niche in order to see if there are any substantial inconsistencies with the views presented by Estonian officials. More comprehensive research is definitely necessary to produce substantial conclusions on the possible effects of small state niches as identified by big states.

[7] The questions covered in the interviews corresponded to the framework that is presented in appendix 1

5. Results

The following chapter will first present the results of the interviews with officials from the Estonian Ministry of Foreign Affairs (MFA) and Ministry of Defence (MoD). The chapter will be divided into six subchapters based on the main outcomes and topics covered in the interviews. An additional seventh subchapter presents the results of the interviews that were conducted with two officials who had experience in representing a big state in Estonia in the area of cyber security.

5.1. Influence within the Niche Area

To establish a necessary starting point, all the interviewees were first presented with the claim that Estonia has specialised in the area of cyber security and has therefore gained influence in matters concerning cyber security in bi- or multilateral relations and international organisations. There were no respondents challenging the statement; one interviewee (D1) summarised Estonia's role as follows: "*If we would compare us with other countries, then we are playing in a different league in matters of cyber security*"[8]. Estonia's positive international image was also characterised by a high level official (F1): "*Estonia has taken the issue seriously. It [cyber security] is a topic where others look at us as a trustworthy partner. It is a topic where we have something to say and provide. […] It is a topic where Estonia is 'in the picture' in international security and we are being listened more to than one would expect from a country like Estonia.*"

While discussing Estonia's efforts in the sphere of cyber security, a distinction has to be mentioned as to the different views and approaches to cyber-related matters by the MoD and MFA. MoD representatives identified that they are mainly involved with the issue in a military context (within NATO, the EU or in bilateral relations). Interviewees from the MFA, on the other hand, highlighted that they approach the matter in a wider context. First, the list of institutions where the topic is addressed is much broader. For example, activities in such organisations as the UN, EU, OSCE, CoE and the ITU were

[8] Since all the interviews were conducted in Estonian, the quotations are translations by the author

mentioned. This is dependent by the fact that the MFA does not approach cyber security as a clearly separate issue-area when the existence of the niche was discussed. The Estonian niche or internationally recognised position was viewed as involving "*all topics concerned with cyber*" (F1). Cyber security is approached by the MFA as a part of other cyber-related topics such as e-services, internet freedom, human rights in the internet, education, capacity building, development cooperation.

Nevertheless, this does not imply that the MFA's role in the specific area of cyber security is less important as it has been representing Estonia in initiatives that can be regarded as highly significant in the context of international developments. For example, the MFA has sent its representative to the UN Group of Governmental Experts (GGE) which has proven to be an important global forum to discuss threats from the cyber-sphere (see Lewis 2014). Also, the MFA is representing Estonia in the OSCE that has adopted an initial set of confidence building measures (CBMs) to reduce risks stemming from cyberspace (ibid).

5.2. A Strategic Plan to Develop and Utilise the Niche?

Before discussing possible broader gains from the niche, the interviews analysed if there initially was or currently is a clear strategic plan to develop and utilise a niche with the aim to have wider influence in foreign and security policy. To sum up the results, the reason behind creating and further utilising the niche could be seen as a mixture of an inevitable practical need due to technological dependencies, an incentive to specialise by NATO, a general strategic thought, and the "positive" effects of the 2007 cyberattacks.

As expected, it was apparent that the development of the niche was not based on a very evident or elaborated strategic decision which could be identified in a specific source (e.g., in a policy document). Nevertheless, the notion that specialisation in cyber security is aimed to produce wider gains for foreign and security policy was understood and expressed by all interviewees as a logical strategic choice for Estonia to get

influence in international affairs.[9] With regard to having a very clearly established plan to utilise the niche for wider gains, a respondent (D2) expressed a critical view: "*There is awareness that we have a 'special weight' in cyber. […] But I would be rather critical as to how aware we are of this as a nation. And how could we consciously improve our relative activities."*

To present the initial strategic thought, one interviewee (D4), who was substantially involved in the establishment of the NATO CCD COE in Estonia since the early 2000s, explained the reasons behind the decision to focus on cyber security. First, the interviewee explained that after having its "*dreams accomplished*" by becoming full members of the EU and NATO, Estonia started to seek out new topics in order not be a small state in the periphery of NATO that can only be seen as focusing on one issue (Russia). Therefore, one of the goals was to expand the scope of topics where Estonia could be competent in. In this regard, the aim was *"not to produce only warm air, but to do something concrete and useful. To produce rational ideas and provide technical solutions which improve NATO."* Furthermore, the interviewee emphasised the importance of a NATO that would not lose its significance: "*The vital interest for the Estonian people is a NATO that is as modern and effective as possible and we have a duty to do our part in the modernisation of NATO*". For the interviewee, the aim to get international recognition was not a priority, but has rather emerged as an "*additional value*" in comparison to the initial objectives. The decision to specialise was also seen (D3, D4) as influenced by NATO's narrative in the early 2000s that promoted developing niche capabilities.

When analysing whether Estonia was initially strongly focusing on the development of cyber security as part of a broader strategic plan, the effects of and Estonia's actions during and after the cyberattacks of 2007 was assessed. In general, the effect of the attacks was somewhat paradoxically viewed as positive in the context of getting international support and publicity in the sphere of cyber security. One respondent (D1) described the situation within NATO: "*This is where our success story of cyber in NATO begun. […] In the beginning, it [the attack] was a practical nuisance but later, a political convenience"*. Many interviewees viewed the cyberattacks as an example

[9] The identified broader gains will be explained separately in a following subparagraph (5.4) under this chapter

which could be effectively used by Estonia to get support to its initiatives and present the importance of cyber threats in front of international audiences. One interviewee (F1) claimed that the year 2007 could be seen as a starting point where a decision was consciously taken to promote the importance of cyber threats to the international community (this goal was also set in the 2008 cyber security strategy).

The 2007 attacks unquestionably heightened Estonia's image in the sphere of cyber security, but could the event be regarded as one of the essential reasons behind Estonia's positive, internationally acknowledged image? In this regard, a very dominant position among the respondents was that Estonia's success in matters of cyber security derives mainly from the high level of technical development. While commenting the effects of the 2007 attacks, an official (D5), assigned to deal with cyber security issues, presented the following opinion: "*I think there would not be an 'equal sign' between Estonia and 'cyber'. But the level of technical development would be the same. It would be so due to the high e-dependency. We would have the necessity to provide the level of [cyber] security anyway. […] How would have we achieved this position without the attacks? 2007 provided us with an opportunity, without it, we would have simply climbed there through sweat and tears.*" In short, the effects of the 2007 attacks were seen as very substantial by proving a strong impulse, but the main reason behind advancements in cyber security was seen as based broader developments in the information society. For example, this factor is characterised by the fact that the establishment of the NATO CCD COE was already planned well before the attacks occurred. But nevertheless, one respondent (D4) mentioned that the event created further international legitimacy and sped-up the process of accreditation.

5.3. Existing Capabilities

As side-payments or wider gains in foreign and security policy might be dependent on the actual capabilities which could be theoretically used to get "trade-offs" in international negotiations, the interviewees were asked to assess the capabilities that Estonia has in the field of cyber security. Simply put: does Estonia have distinguishable capabilities in cyber security, such as technical expertise or know-how, which could be

"traded" with international partners for support in other areas? In this context, it is important to highlight that the interviewees were operating on the policy level and specialists from institutions that deal with the specific technical matters were not interviewed. Furthermore, a lack of information presented on the specific capabilities might be caused by the factor that this information could have been either too sensitive or classified to be disclosed in the interviews. Nevertheless, as the thesis focuses on the possible effects that the niche has on the international level in the context of foreign and security policy, the respondents were seen as being able present adequate views on the matter. All in all, the interviewees indicated that Estonia is an internationally valued actor as it is able to provide both specific technological solutions as well as being active and generating strategic ideas on the political level. That said, no "hard security" capabilities that could be viewed as being able to generate concrete side-payments in security were identified.

Many interviewees used the term "cyber bubble" when discussing the question of capabilities; the term suggests a view that Estonia has possibly gained or promoted a reputation as a very advanced actor in matters of cyber security that might not be realistic if the actual capabilities are taken into account. There were some respondents who leaned towards agreeing with this idea with the caveat that they might not be aware of the capabilities which are classified or very technical. However, most of the interviewees tended to disagree with the notion by saying that Estonia has considerable capabilities and that Estonia's own actions in representing its competences correspond to reality.

The main doubt in terms of capabilities was expressed in the context of Estonia being able to provide hard security capabilities that would be valued by bigger partners. This notion was expressed by one interviewee (D2): "*I am not so sure that we have something to put 'on the table' which would be very important to the US in terms of 'hard security'*." Another official (F2) expressed this aspect as well: "*Let's put it this way: I doubt that the US will send our CERT a request to fight an extensive cyberattack*." Nevertheless, this aspect was not seen as a big issue as the majority of interviewees were confident that Estonia has real or "tangible" assets that are appreciated by its partners. Furthermore, it was highlighted that Estonia has not

represented itself as having those very specific hard security capabilities – it was claimed that an unrealistic impression might be a result of a lack of knowledge in the field of cyber security. For example, while discussing Estonia's general image in this context, one interviewee (D5) explained the situation: *"Because they [journalists, diplomats, foreign officials] are not knowledgeable in the field, a certain unrealistic impression is created."*

Interviewees highlighted many examples to argue against the claim that Estonia might be seen as presenting an unrealistic image of its capabilities. First, a prominent example given in the context of providing military capabilities was the Estonian cyber range that will be used for NATO's cyber range capability. In this regard, it was underlined (D5) that although most of the bigger countries have their own cyber range capability, Estonia's contribution is special since it has "opened it up" by offering the expensive service for international use, providing a cost-effective solution for less resourced nations. Furthermore, the NATO CCD COE was also characterised as an organisation that is strongly linked to Estonia by other states as it provides substantial host nation support in terms of resources and specialists in comparison to other sponsoring nations of the Centre. In addition, the Cyber Defence League was mentioned as a unique institution that has rightfully created international interest. In this regard, some interviewees mentioned that the concept of Cyber League might be not a realistic or scalable for bigger allies as its functioning might be dependent on Estonia's smallness and specific cultural factors.

As for other technical solutions that Estonia has to "offer" to other states or international organisations, the interviewees strongly emphasised the role of e-services. Although these capabilities are not strictly related to matters of cyber security, they naturally cover the area as having advanced e-services also create the need to secure these services. In this context, Estonia was seen as providing technical know-how and solutions that have clearly created interests globally for both big-state allies and developing countries. This was expressed by one interviewee (F1): "*We are being very specific; we just don't talk about what is in the textbooks. We are talking about our own real-life experience. Come, have a look, and see what you can learn. In other words, the things we are providing to the world are very real. We have over 3000 e-services."* This

reflects the aforementioned point that competences in cyber security issues were often viewed as a part of the overall technological advancements.

Next to the practical solutions Estonia has to offer to the international community, a very strong competence in providing a strategic vision on international matters of cyber security was emphasised. This notion was expressed by an interviewee (F2): "*If we think about international organisations, Estonia is viewed as an opinion leader on the political level, and not as much on the technical or operational level.*" The most stressed organisation in this regard was NATO, where Estonia was seen as one of the main actors promoting and involved in the development of NATO's first cyber defence policy after the 2007 events. "*There is certainly a lot of strategic input and this is mainly on the level of security policy. Our people are very active within NATO in the cyber-related discussions. […] We can look to the future and are included in the discussions*" (F1). "*We are good developers of strategy. I see that we think much more about the role of cyber in military issues than other NATO nations" (D2).* The importance and positive role of President Toomas-Hendrik Ilves being a "strategic thinker" on cyber security issues was also highlighted by many respondents.

The role of Estonia acting as an advocate for cyber security by creating more general international awareness was also mentioned in the context of capacity building, development cooperation, as expressed by an MFA official (F1): "*The fact that we realise the threat does not mean that we are safe within NATO or the EU, all organisations and the region must follow. Cyber isn't something you can do alone like a porcelain painting, it has to be done cooperatively. It is a clear strategic decision to share this ideology and to get more nations to understand the issue as we do.*" Building on this, it was also indicated that IT-related issues, including cyber security, are "*integrated horizontally in the development cooperation activities*."

5.4. Gains from the Niche

When asked about the possible foreign and security policy gains that are sought or received as a result of having the competences or capabilities in cyber security, the

interviewees presented a wide array of answers. As presented above, the respondents did not identify specific hard security capabilities in cyber security that could be analysed as "bargaining chips" in international negotiations. Put differently, very concrete side-payments in the form of "tit-for-tat" exchanges were not identified. However, several indirect gains such as strengthening security guarantees and enhancing cooperation with strategic partners were recognised as results of having the niche. In this regard, many respondents highlighted that the gains in influence in the context of foreign and security policy are difficult to measure.

The underlying benefit from having the niche, as identified by all respondents, was the assurance of Estonia's security guarantees which are provided by its strategic allies and international organisations. As NATO is seen as the main security guarantor for Estonia, the acknowledged competences and capabilities in cyber security were seen as an important part of the strategy to contribute its "fair share" (i.e., not being viewed as a free-rider) in the alliance in order to assure support. The niche's part in this fundamental aim to strengthen Estonia's security guarantees was summarised very well by one respondent (D2): "*We are those who do what we say. This concerns 2% and contributing to missions. We are on the foreground. Cyber is a part of the 'model ally' image. […] We do everything what is required. Therefore, if, at some point - probably not - we need assistance, it would be very difficult to say 'no' to us because we have done everything as requested*." This basic strategic gain was also expressed by another respondent (D4) who was describing effects of the overall success in the field of IT: "*The more Estonia's image gets positive acknowledgement, the harder it is for the 'green men' or whoever to come here. […] It increases our security substantially.*"

Therefore, efforts in cyber security were seen as an item in the bigger "package" of Estonia's activities or image that aim to demonstrate its contribution to NATO and its allies. "*It [cyber security] is always in our rhetoric if we want something*" (D3). In this context, majority of the respondents assessed the fulfilment of the 2% defence expenditure requirement and contribution to out-of-area missions as being more valuable to Estonia's partners. One respondent (D3) explained the reasoning behind this view: " '*Cyber' is soft security. It is not so emotional […] The tangible benefits are limited and the levels of risk are different.*" By "the levels of risks", the respondent

meant that cyber-related contributions might be less valued in comparison to missions, where Estonian and its allies' soldiers are actually fighting side-by-side and there are actual casualties. Again, it was emphasised by the interviewees that it is difficult, if not impossible, to measure or anticipate the reasoning behind a support of an ally.

In the broader context of foreign policy, a high official from the MFA presented a slightly different view with regard to "cyber" and other Estonia's activities that are valued by big states or international organisations. The official (F1) mapped out the following strong points of Estonia in hierarchical order: (1) successful reform experience as a post-Soviet country transforming to democracy; (2) Estonia's "trustworthiness" as a member of international organisations who follows the requirements (mentioning both the EU and NATO); (3) and competences in specific fields, including "cyber".

As said before, finding concrete "proof" that the niche has increased the support of Estonia's strategic allies was difficult to identify. When looking at the latest developments in the context of support by allies, the deployment of US troops in Estonia after the events in Ukraine [2014] was discussed with the aim to analyse the possible effects of the good reputation in cyber-related matters. As expected, the interviewees dominantly expressed the view that the increase in hard security guarantees after the Ukraine crisis is certainly not an effect of the efforts in cyber security, but a result of geopolitical factors and well-established support by NATO and allies. An interviewee (F1) expressed this viewpoint: "*Estonia is good in 'cyber' and let's send soldiers?' Definitely not*." With regard to the Ukraine conflict and the US president Barack Obama visit in 2014, a respondent (D3) highlighted that the cyber-related activities of Estonia are relevant in a different framework within NATO: "*We can't confuse the influence of daily politics that are dependent on certain events and the so-called capability development side. These are two different things: capability planning and operative planning. Figuratively, Obama's visit [to Estonia in September 2014] was operational planning, a reaction to an event. And cyber defence today is a kind of a capability development."* Therefore, cyber-related efforts by Estonia were seen as having an effect in the context of long-term development of NATO's capabilities. Nevertheless, one interviewee (D1) expressed the possible effects of the niche with

regard to the positive outcomes of the Wales summit: "*We would have probably had to work for it more. […] If you look at 'image-building', the benefits are not clear. There are no concrete 'cash-ins' involved. "*

Therefore, efforts in cyber security were seen as a part of Estonia's positive international image that, in turn, enhances its position in international relations. With regard to Estonia's image, many respondents mentioned that focusing on cyber security provided a way to make Estonia interesting in NATO and getting more "air-time". Also, this relates to the aim of "diversifying" the image of being only able to focus and give input on one topic (i.e., Russia). In this context, a respondent (D2) explained that Estonia has been (and is being more and more in the context of the Ukraine crisis) involved and acknowledged in Russian-related security discussions because "*we know Russia better than most in Europe."* Taking into account the effect cyber-related matters have had in making Estonia's voice heard before the Ukraine crisis, the respondent explained: *"A year ago [referring to the changed situation after the events in Ukraine] it was a lot more difficult to be involved in discussions, because we were not on the so-called mental map. […] 'cyber' was the thing that gave this opportunity, it opened doors."*

With regard to using the cyber-related initiatives to make the small state more appealing or interesting, the interviewees pointed out that the topic is included to a certain level in the majority of the official visits either in Estonia or abroad that have a broader, "non-cyber" agenda. Therefore, success in technological developments (and not only cyber security) was seen as a strong item that creates interest to states to either visit or invite Estonian entities. Again, this was seen as feeding into the larger positive image of Estonia as a capable state that is able to produce value for bi- or multilateral relations.

As for the niche influencing the occurrence of visits, some possible wider gains were analysed during the interviews. First, the interviewees were asked whether cyber security-related visits might generate more access to influential officials of strategic allies. In general, the respondents agreed that these cyber-related meetings with high officials naturally have a positive effect and provide an opportunity to also discuss other issue-areas. Once more, the effects were seen as difficult to measure and concrete examples of gains in influence were not given. On the other hand, one respondent (D1)

was sceptical with regard to the added value of these meetings as Estonian officials have many opportunities access high officials through different international organisations. Nevertheless, one respondent mentioned that simply having a very high (military) official visiting Estonia (because of cyber-related matters) creates deterrence. A positive effect on deterrence was also mentioned when discussing the fact that the NATO CCD COE as a perceived NATO body is located in Estonia.

Estonia's valued position in matters of cyber security was also seen as creating additional forums or communication channels with big states. For example, it was pointed out that Estonia is a part of a smaller group of like-minded nations within NATO that discusses cyber-related issues – this is relevant since the group consists of big states who can be seen as Estonia's main strategic allies and key players in NATO. An interviewee (D3) explained this aspect further when asked whether being a member of this group creates positive effects outside the area of cyber security: *"Of course it does, because the 'elite' is behind the table. Others also see that you a part of a forum, a club, and this indisputably increases your trustworthiness."* An interesting point was mentioned by an MFA official (F1) in the context of the niche creating communication channels – cyber-related forums are also creating unique opportunities to communicate with non-Western big states.

The interviews also discussed whether international agreements in cyber security might work as "catalysts" for bilateral cooperation, i.e., whether a cooperation initiative in cyber security has formed a basis for cooperation in other areas or has created international partners with whom cooperation was previously limited. Respondents agreed that the niche probably could have the aforementioned effect by providing some examples, but no outstanding cases were evident and clearly identifiable effects were yet to be seen. One interviewee (D1) expressed this position: "*Yes, you can refer to it [cyber] that we are already cooperating in this area and now let's cooperate in another area as well*."

Although not directly linked to gains in foreign and security policy, positive effects to the private sector were emphasised when possible influence of the niche was discussed. Once more, it has to be highlighted that these possible effects on the economic level are very difficult to measure and they are probably not specifically linked to Estonia's

image within the domain of cyber security, but rather to the broader image of being a technologically advanced state. Nevertheless, there were examples given which can be seen as influenced by the positive image precisely in cyber security. For instance, an Estonian company (BHC Laboratory) won a European Defence Agency's bid to organise a strategic cyber security exercise in 2014.

5.5. Possible Setbacks and Recommendations

The interviewees were also asked to discuss the possible setbacks or vulnerabilities the "niche-oriented" strategy may entail. First, the interviewees were asked whether it is possible for a small state to keep up a strong, positive image as an advanced actor in cyber security. This question referred to the general developments in the field: big states strongly investing in cyber security, making it questionable if a small state can sustain its forerunner image. In this regard, naturally, the question of resources was the principal issue.

"*The most relevant issue is that we do not have enough people.*" (D4). Another respondent (F1) mentioned that although Estonia has been increasingly investing in the area and has created positions that only deal with cyber-related matters, the amount of officials dealing with the area is starting to become noticeably lower in comparison to Estonia's allies. From the perspective of the MFA, it was noted that the number of international forums where cyber security is addressed is constantly rising. The respondent (F2) highlighted that it is very important that Estonia is able to send capable representatives to these international forums to keep up Estonia's positive image on the political or strategic level. The importance of international forums and political discussions was highlighted since they were seen as providing effective opportunities for small nations as every state usually has one seat behind the table.

While discussing how to keep the niche, many respondents highlighted the need to be constantly able to produce innovative ideas. This notion was expressed by one respondent (F1): *"If you are a small fish among sharks, you have to swim faster."* Referring to the questionable innovativeness of the recently [2014] adopted cyber

security strategy, a respondent (D1) had a similar view: *"If you don't have ideas, you won't be spoken to."* Another substantial issue was expressed by many with regard to Estonia producing new ideas – the question of whether these innovative ideas are actually being implemented in practice. *"This situation of being intellectually interesting could change to practical cooperation. For example, we should have cyber officers. […] Practical stuff is necessary for sustainable cooperation"* (D2). *"Practicians always say that if the idea is good, let's implement it then"* (D1).

Many respondents also referred to the need to have a clear political decision to invest more resources in the area. One respondent (F2) mentioned that although it has clearly been Estonia's the course of action, a high level political decision to focus on IT-related matters, including cyber security, should be "visibly" taken (e.g., mentioned in a coalition agreement). Another interviewee (D3) expressed a similar view in the context of NATO: *"If we don't raise the ambition quickly, if we won't do a quick manoeuvre, then I am afraid that the picture won't look like this in 5 years."* In terms of having a more focused effort, some respondents highlighted the need to put more effort into "educating" or raising more awareness on Estonia's efforts in cyber-related issues among officials who are engaged in relations with international partners. In this context, again, it was mentioned that the developments with e-services have been very considerable, but the area of cyber security in terms of hard security capabilities needs more focused attention.

While discussing the possibility to be able to have concrete, tangible capabilities in cyber security, the importance of public private partnership (PPP) was highlighted. For example (D2): *"Estonia can't pay for top programmers. […] We need to find a system on how to involve the private sector."* Additionally, some respondents emphasised the importance to utilise all the existing resources as cost-effectively as possible – for example, by having precise coordination between government agencies, and involving other entities such as think-tanks, universities and students as interns.

Another idea, put forward by many, was to find a certain specialisation within the area of cyber security; i.e., to find a "niche within the niche" to be able to sustain the positive image. *"I think that a key to our success […] would be to take a niche within this area and develop our capabilities as much as possible"* (D3). In addition to focusing on

certain niche capabilities, a respondent (F2) also expressed an opinion that it could be more realistic for a small state to focus mainly on being forerunners on the strategic and political level: "*I think we need to focus on those areas where we have a comparative advantage, where we could really be forerunners while taking into account our limited human resources.*"

As for the possible "niches within the niche", many ideas were put forward. One respondent (D3) highlighted the possibility to focus and develop further capabilities on international exercises as Estonia has already provided the cyber range for international use. In addition, the idea to develop an "IT military service" was seen (D1) as a possible area to focus on in the future. One interviewee (D4), again referring to efforts on the political and strategic level, stated an ambition to organise a *global* meeting of states in Estonia with the aim to sign an international agreement (e.g., CBMs) in order to agree on certain areas which should not be targeted via cyberspace (e.g., financial systems). "*Estonia, a small state, viewed as being able to produce global solutions – this is my dream*" (D4).

The interviewees were also asked whether some technological setbacks can cause a substantially negative effect to Estonia's international position on cyber security. In general, the respondents did not indicate a big risk in having a technological breakdown or suffering another cyberattack which could damage Estonia's image – it was expressed that being in the forefront in terms of innovation and new solutions naturally might cause technological setbacks and hence some problems are probably viewed as acceptable.

In addition, when asked whether it might be too obvious to Estonia's international partners that the state is constantly emphasising and focusing on its technological advancements to enhance its international position, the respondents did not see an issue by saying that specialisation by small states is a valued policy. One respondent (D3) expressed this view in the context of NATO: "*If you talk about niche capabilities and small states, and whether the strategy is obvious to our partners, of course it is. This is even promoted. Everybody understands that we can't be good in everything. […] It is important that they see that we provide a fair-share that corresponds to our resources.*"

5.6. Properties of the Niche

The discussions also looked into how the area of cyber security could be viewed as a small state's niche with properties to be used to get influence in other areas. Two main positive characteristics were identified: the interconnected nature of cyber security and the possible cost-effectiveness.

Overall, cyber security was viewed as a suitable modern issue-area that could be linked with a very wide set of topics. *"I do not know any areas which are not connected to it [cyber]: security, economics, it is tied with human rights, development cooperation. It is 'soaked' into absolutely every domain."* (F1). In addition, cyber security was naturally seen as an issue-area that has received a lot of attention and where almost all partners have an interest in. Furthermore, cyber security was viewed as a field that is prone to be addressed in international cooperation due to the interconnected nature of globalised technology.

On the other hand, an interviewee expressed a different opinion with regard to military affairs by saying that cyber security tends to be very technical and "transforming" influence might be difficult: *"[…] Cyber security is very much a niche topic in militaries; it is 'stove piped'. They have their own commands, own hierarchy, own career models. […] cyber is, in general, a very prominent and 'sexy' topic, but it is still a very technical thing."*

Another very important aspect repeatedly mentioned while discussing the properties of cyber security as a niche within the military realm was the notion that cyber security can work as a very cost-effective solution for a small state in comparison to developing conventional capabilities: *"There's an optimal balance in 'income' and expense. It seems to me that in order to successfully develop the field of cyber a lot less costly and functioning prerequisites are needed [referring to infrastructure]."* (D3). *"For example, a cyber defence unit, in a NATO mission, which has five-six members, 'armed' with laptops, is in my opinion hundreds or thousands of times cheaper to maintain than an armoured infantry battalion. Estonia would contribute to a NATO mission and our politicians would have an equal say" (D4).*

5.7. An Outside Perspective

The following chapter will present the results of two interviews that were conducted with officials who had experience in representing a big state in Estonia in the area of cyber security. Once more, it has to be pointed out that the respondents did not express official positions of the states as they were asked to provide personal views. Furthermore, as the chapter is based on two interviews, the summary presents a tentative look on how Estonia's big state allies may view the effects of the niche of cyber security on Estonia's wider foreign and security policy.

At large, the interviewees had similar views and ideas that were presented in the previous chapter by officials from the Estonian MFA and MoD. Firstly, Estonia was viewed as a strategic partner in IT-related issues (not only cyber security). This point was illustrated with the fact that the states have created positions in Estonia that exclusively deal with cyber-related issues; this is significant since Estonia was one of the few states where these positions were reported to be established.

Regarding concrete examples of Estonia's internationally valued capabilities in the field of cyber security, a respondent highlighted the EDF's cyber range and the Locked Shields cyber defence exercise hosted by the NATO CCD COE. In this regard, an interviewee said that the CCD COE, although being an international military organisation, is primarily viewed as an Estonian entity. Therefore, other initiatives besides the mentioned exercise were also seen as subjectively connected to Estonia. In addition, as evident from the interviews with Estonian officials, efforts in cyber security on the strategic level were acknowledged. First, Estonia's capability to raise awareness on cyber-related issues was appreciated. And second, Estonia, having "political capital" in the in the area of cyber security, was viewed as a valuable strategic partner that can provide support and legitimacy to like-minded big states to pursue cyber-related political agendas in international organisations.

Nevertheless, in general, the cyber security niche was viewed as a part of Estonia's wider competence in IT-related issues. Both Estonia's innovative e-services and start-up companies were clearly identified as valued assets; cooperation within these areas was identified as being very active by one respondent. Furthermore, successful cooperation

in education and capacity building was emphasised. In conclusion, a respondent said that Estonia has not created a "cyber bubble" – possible unrealistic expectations of Estonia's capabilities were rather seen as the product of lack of knowledge in the area.

As for the wider gains generated by the niche, the interviewees reiterated the views presented by Estonian officials. As expected, both interviewees emphasised that hard security guarantees and assurances (e.g., troop deployment) should not be seen as affected by Estonia's efforts in cyber security but as results of both firmly established bilateral relations and security obligations stemming from Estonia's membership in NATO.

The main indirect effect of the Estonia's niche to wider cooperation was explained by one respondent as follows: *"Estonia's niche certainly serves as a 'lubricant' for relations/cooperation. […] over the longer-term, the cyber security reputation and the subsequent cooperation/assistance (whether higher visibility or more often lower visibility, running in the background) sets the stage, and perhaps facilitates, broader cooperation."* In addition, one interviewee explained that the Estonian authorities or private companies have a privileged position in comparison to other similar states when they want to present their initiatives to the big state or its companies.

Estonia's specialisation in a certain issue-area was a welcomed strategy as it was mentioned that this is inevitably an option for s mall state to actually provide valued capabilities to bigger states. In this regard, a respondent also stated that cyber-related cooperation was one of the main areas that generated interest and cooperation before the events in Ukraine which have tilted the discussion towards more classical security considerations.

The sphere of cyber security was again viewed as a suitable issue-area that can induce further cooperation; one interviewee explained this notion: *"some aspects of cyber security have probably accelerated or enhanced that 'lubrication': cyber security's visibility and perceived importance/urgency and its cross-agency nature (law enforcement, financial, military, commerce, etc)."* In addition, Estonia's smallness was identified as a positive property – it was seen as providing opportunities to develop and test innovative technological solutions. However, it was mentioned that many solutions

might be, in fact, dependent on this smallness and the scalability to bigger levels may be problematic.

6. Analytical Conclusions

The subsequent chapter will be divided into two parts: the first will focus on the possible theoretical implications of the research results and the second subchapter will discuss the factors specific to the case of Estonia with the aim to give practical recommendations.

6.1. Theoretical Implications

The case of Estonia provided many insights on how a small state's niche capability could generate wider influence or gains in foreign and security policy. First, as expected, it was confirmed that a small state can have influence within the area of the niche. Second, the case proved that a small state can also use a niche capability to have wider gains or influence in foreign and security policy. Although it was apparent that Estonia has not been able to use the niche as a "bargaining chip" to get specific trade-offs or receive particular side-payments, many other significant indirect gains were identified.

According to the interviews, the main (assumed) gain from having the niche capability in the context of foreign and security policy was the strengthening of Estonia's security guarantees that are provided by its strategic allies. This indirect gain was identified since the niche capability was seen as playing an important role in Estonia's strategy to be a valuable, capable and trustworthy partner that is providing its fair share in international organisations and to its strategic allies. Other indirect gains from the niche besides the positive image were identified as well. The niche was seen as creating additional communication channels and facilitating cooperation with strategic allies, strengthening deterrence, and having a positive effect on economic relations.

It was evident that the niche has created gains in soft power (see Nye 1990; Ilves 2011; Areng 2014) and diplomatic capital (Adler-Nissen 2008, 670) – by having the niche, the small state was able to achieve the aforementioned outcomes through its enhanced positive image and reputation. In this regard, one could claim that the type of received

gains in foreign and security policy corresponded to the type of capabilities that the small state was able to provide. This point was also characterised by the fact that other hard security contributions such as participating in missions or meeting NATO's defence expenditures threshold were seen as being more significant in terms of getting security assurances.

Furthermore, the case provided an interesting example of a niche area that has certain characteristics which make it suitable or more likely for a small state to have wider influence in foreign and security policy. In the sphere of military contributions, it was highlighted that cyber-related capabilities could provide a small state a realistic opportunity to have a significant and valued input to military operations as cyber capabilities are cheaper and therefore more realistic to develop than traditional military capabilities (see Nye 2010). Although the notion was seen as theoretically possible, the case of Estonia has not yet provided examples that would confirm this assumption. This also calls into question whether or how a small state can actually develop advanced or considerable capabilities that could be seen as highly valued or even unique by its strategic allies.

Nevertheless, the case also presented other characteristics of the niche that make it more probable for a small state to have the aforementioned positive effects in the context of foreign and security policy. First, the niche was a "good fit" if one takes into account the existing concepts[10] on how a small state can obtain influence. For example, cyber security was viewed as an issue-area that is of common interests to Estonia's strategic partners. Also, Estonia was able to use its forerunner reputation to give legitimacy to its actions. In this regard, Estonia provided an example of a small state that has utilised its so-called comparative advantages for the purposes of foreign and security policy since the development of the cyber security niche was seen as largely based on Estonia's general technological advancements.

The case of Estonia also provided an example of a more specific attribute of the niche which allows a small state to seek gains or influence in foreign and security policy. This characteristic is related to the concept of issue density (Keohane 1982) – cyber security was viewed as an area that can be used for issue-linkage and could therefore generate

[10]See concepts discussed in subchapter 2.3

certain spillover effects in international cooperation. This point was evident as the case of Estonia showed that the niche had a "wide grip" and could therefore be linked with more general matters of foreign and security policy. Furthermore, it has to be highlighted that the niche did not limit Estonia's actions to only specific organisations; it provided opportunities for Estonia to present its capabilities in most of the relevant international organisations.

While identifying Estonia's niche capabilities, it was apparent that Estonia has had the capacity to provide valued input on the strategic or political level in the area of cyber security. This course of action could be seen as a possible strategy for small states to enhance its image and get influence in foreign and security policy. The focus on strategic aspects could be viewed as a cost-effective strategy for a small state to get international recognition since it is considerably cheaper to provide strategic/policy-level input or act as a norm entrepreneur in comparison to developing highly advanced technological capabilities. In addition, focusing on the strategic level is a suitable solution as the discussions mostly take place in international organisations where small states have more equal opportunities to voice their opinions.

Conversely, the case of Estonia also provided an example where a small state has been able to produce "tangible" solutions in the niche area. On the one hand, these technological solutions that Estonia "exports" were seen as being dependent on the e-services that have mostly not been developed with a foreign or security policy related aim in mind. On the other hand, it is significant that Estonian efforts specific to cyber security, such as hosting the CCD COE or providing the cyber range to NATO, have a strong cooperative aspect to them. First, although Estonia provides substantial host nation support to the CCD COE, it is an *international* military organisation that is supported by a large number of NATO's allies and other contributing nations. Second, it was mentioned that the cyber range capability in itself is nothing exceptional – the uniqueness of it lies in the fact that the range is provided for international use. Therefore, the value of the cyber security capabilities provided to strategic partners are strongly dependant on international cooperation. In this context, the cyber security niche provides a suitable area for pursuing this strategy as it requires international cooperation. The "cooperative nature" of the niche area could be again seen as another

positive property that can be exploited by a small state to get wider influence. Estonia represents a small state that has been utilising this characteristic well to its advantage as, for example, the CCD COE is strongly linked to Estonia's capabilities by its strategic partners.

Another interesting aspect that might be relevant in explaining how small states utilise niches is connected to the inherent tendency of small states to have a narrow foreign and security policy focus (Bjol 1968, 158; Pastore 2013, 69). As the Estonian case presented, focusing on cyber security provided the small state an opportunity to show itself as a capable actor in an issue-area that is not strictly connected to its main and traditional security considerations (i.e., Russia). Therefore, the niche provided the opportunity for a small state to diversify its internationally recognised "skill-set" and be appreciated by its strategic partners without being viewed as pursuing a very obvious self-interested strategy. In this context, it was significant that before the Ukraine crisis [2014], the topic of cyber security was seen as one of the few areas that generated interest for major allies. What is more, as big states were seen as welcoming the niche-related efforts by Estonia, the idea that a small state could be too "pushy" or its strategy to get influence by using the niche might be viewed as too obvious was refuted.

The case also presented an instance of how a small state conceptualises its strategy for foreign and security policy with regard to niche capabilities. As presented in the results, the strategy to focus on the niche with the aim to get gains in foreign and security policy was understood by all, but it was not based by a very elaborated, detailed or planned concept – instead, the niche's importance was identified by the officials as an obvious and rational strategy for a small state. This might also serve as a weak-point as it is possible that a more clearly elaborated strategy to use a niche for wider influence could lead to more results.

6.2. Practical Considerations

The cyber security niche has definitely played a positive role in Estonia's foreign and security policy. In order to maintain or improve this effect of the niche, it is important to identify the success factors and discuss how to tackle possible future challenges. As explained before, the main challenge for Estonia is to keep the internationally recognised positive image in a situation where cyber security has become an issue-area that is increasingly receiving attention by most developed states. Therefore, it is questionable whether Estonia, a small state with limited resources, can maintain its current position.

The previous subchapter presented certain characteristics of the cyber security niche that provide cost-effective solutions to a small state to use its niche. First, Estonia's success in cyber security was seen as based on its overall advancements in technology and information society. Therefore, one could assume that if Estonia is able to keep producing innovative technological solutions that also encompass advanced security measures, its unique position in cyber-related matters is not going to fade remarkably. Nevertheless, it is questionable whether only having an advanced information society can produce such solutions that would be relevant or effective in the context of getting influence in foreign and security policy. Therefore, a more clear focus on identifying and promoting the relevant capabilities specifically in the sphere of cyber security could be beneficial.

As the question of how to ensure general technological innovation falls out of the scope of the thesis, aspects that are specific to the niche in the context of foreign and security policy can be analysed in more detail. In view of that, the case of Estonia has so far shown that a focus on providing international solutions on the strategic or political level has been effective (e.g., advocating the need to address cyber security, and being involved in international policy development). Being actively involved in cyber-related strategic or political developments is a viable option since this course of action does not necessarily require a high level of investment. As mentioned before, discussions on policy and strategic matters are mostly taking place in international organisations which provide small states better opportunities to voice their opinions. Therefore, one option

for Estonia could be to intentionally focus on being able to continue to produce innovative ideas on the strategic level. If one takes into account the raising number of international initiatives and forums where cyber security is addressed, it is reasonable to believe that it would be advantageous to assign or hire more officials to deal with these areas. In this regard, it has to be taken into account that by focusing on the strategic or political level, the wider gains in foreign and security policy would probably stay at the current level – i.e., there would be no specific trade-offs in security involved as the niche would mainly provide a positive image.

On the other hand, if Estonia aims to have a niche that could be used as leverage in international negotiations, specific military capabilities should be developed. For Estonia to receive concrete side-payments (e.g., in security assurances) by using the niche, the capabilities in cyber security have to be highly valued by its strategic allies. This implies major investments and therefore achieving this might be problematic due to Estonia's comparatively limited resources. In order to have highly valued military capabilities, Estonia should probably concentrate its resources and hence make deductions in other vital areas (see Rickli 2008). Another possible strategy to have a solution the "resource problem" could be to develop or further improve public-private partnerships (PPPs) with a strict focus on cyber security or cyber defence capabilities.

As cyber security is increasingly becoming a priority for many states, the mere fact that Estonia is engaged in certain aspects of cyber security will probably not be enough to maintain a strong positive image. The "beneficial" post-2007 period when Estonia gained much publicity (Hansen and Nissenbaum 2009) and was considered unique by just focusing on cyber security is over. For that reason, as the interviews with the officials presented, Estonia should consider finding "a niche within the niche" – by doing so, the small state could possibly provide something of value to its strategic partners since it would allocate its limited resources in order to have a specific highly developed capability within the issue-area.

At the moment, as the results presented, the development and utilisation of the internationally acknowledged niche for gains in foreign and security policy could been as an "organic" process – the niche has been developed and produced indirect gains without applying a very specific strategy that explicitly focuses on how to maximise the

benefits for foreign and security policy. Therefore, if the level of ambition for the future is to either maintain the current *status quo* or to utilise the niche more effectively, a more specific strategy to do so has to be outlined or developed. Without taking a conscious strategic or political decision that would concentrate the allocation of resources, the aforementioned proposed ways of action – finding a "niche within the niche" by, e.g., focusing on the strategic level or developing hard security capabilities – are probably difficult to achieve. On the other hand, Estonia has so far been relatively successful without having a very clear strategic framework or guidelines – taking into account the relatively small number of people involved in foreign and security policy, perhaps it is possible that a small state can effectively operate in such "organic" way.

7. Summary of Findings

This thesis focused on the question of how small states could use niche capabilities to have influence in foreign and security policy outside the niche area. This was done by analysing how Estonia has utilised its cyber security niche to have wider influence or gains in foreign and security policy.

The research resulted in observations that both describe the case-specific aspects and provide ideas that could be applied in further research on small states and their niche capabilities. The thesis took an inductive approach that enabled to produce many relevant findings – the main outcomes are listed below:

- The cyber security niche arguably produced soft power (see Nye 1990; Ilves 2011; Areng 2014) and diplomatic capital (Adler-Nissen 2008, 670) to Estonia by enhancing its positive image and reputation. Therefore, the niche was seen as an important part of Estonia's principal strategy to be a valued and trustworthy partner that provides its fair share in international organisations and to strategic allies. The most relevant (assumed) gain from the niche in the context of Estonia's foreign and security policy was therefore the strengthening of the security guarantees provided by Estonia's allies. However, the niche was seen as being probably less important to Estonia's allies in comparison to other military contributions such as participation in military operations and meeting NATO's benchmark for defence spending.
- The cyber security niche was also seen as providing other indirect gains outside the niche area: creating additional communication channels and facilitating cooperation with strategic allies, strengthening deterrence, and having a positive economic effect.
- As very highly valued or unique military capabilities in cyber security were not identified, the niche has not functioned as a "bargaining chip" that could be used in international negotiations to seek specific security-related side payments. In this regard, the case did not confirm the notion that cyber security capabilities

are more suitable for small states since they are cheaper to develop in comparison to traditional military capabilities.

- Estonia's image of having a cyber security niche has been strongly influenced by the state's capacity to provide international input on the strategic and policy level – this approach was identified as a cost-effective solution for a small state to utilise its niche capabilities.
- The niche area of cyber security was seen as a "dense" issue-area that can generate spillover effects in cooperation (see Keohane 1982, 340): the cross-agency nature of cyber security provided Estonia the opportunity to use issue-linkage to associate the issue-area with other matters of foreign and security policy and to be active in all of the main international organisations.
- The area of cyber security was viewed as having a "cooperative nature" – a characteristic of the niche that has allowed Estonia to develop capabilities that are appreciated by its strategic partners as the value of some of the initiatives (NATO CCD COE and the cyber range) are largely dependent on international cooperation.
- Estonia was able to utilise the cyber security niche for wider gains as it provided the state an opportunity to show itself as focusing on an issue-area that is not directly connected to its traditional narrow interests or security concerns (i.e., Russia). This allowed Estonia to prove its value to its strategic partners who have clearly welcomed and showed interest in the niche capability.
- There was no clear strategic framework identified with regard to utilising the niche to get influence in foreign and security policy. Therefore, if Estonia's ambition is to maintain the *status quo* or utilise the niche further, the thesis suggests that a clear strategic or political decision has to be taken in order to concentrate the allocation of the limited resources to develop a "niche within the niche". For example, Estonia could decide to mainly focus on being able to provide strategic level input on the international level or try to develop high-level military capabilities in cyber security.

Bibliography

Adler-Nissen, Rebecca. 2008. “The Diplomacy of Opting Out: A Bourdieudian Approach to National Integration Strategies.” *JCMS: Journal of Common Market Studies* 46(3): 663–84.

Areng, Liina. 2014. “Lilliputian States in Digital Affairs and Cyber Security.” *Tallinn Papers* 4. https://ccdcoe.org/sites/default/files/multimedia/pdf/TP_04.pdf. (December 16, 2014)

Arter, David. 2000. “Small State Influence within the EU: The Case of Finland’s Northern Dimension Initiative.” *Journal of Common Market Studies* 38(5): 677–97.

Austin, Greg. 2014. “Small States Need Cyber Diplomacy.” *neurope.eu*. http://www.neurope.eu/article/small-states-need-cyber-diplomacy (December 17, 2014).

Baehr, Peter R. 1975. “Small States: A Tool for Analysis?” *World Politics* 27(03): 456–66.

Bailes, Alyson J. K., Jean-Marc Rickli, and Clive. Archer. 2014. “Small States, Survival and Strategy.” In *Small States and International Security: Europe and beyond*, eds. Clive. Archer, Alyson J. K. Bailes, and Anders Wivel. Routledge.

Bailes, Alyson J. K., Anders Wivel, and Clive Archer. 2014. “Setting the Scene. Small States and International Security.” In *Small States and International Security: Europe and beyond*, eds. Clive Archer, Alyson J. K. Bailes, and Anders Wivel. Routledge.

Bennett, A., and C. Elman. 2007. “Case Study Methods in the International Relations Subfield.” *Comparative Political Studies* 40(2): 170–95.

Berg, Eiki, and Piret Ehin, eds. 2009. *Identity and Foreign Policy: Baltic-Russian Relations and European Integration*. Farnham, England ; Burlington, VT: Ashgate.

Bjol, E. 1968. “The Power of the Weak.” *Cooperation and Conflict* 3(2): 157–68.

Björkdahl, Annika. 2008. “Norm Advocacy: A Small State Strategy to Influence the EU.” *Journal of European Public Policy* 15(1): 135–54.

Cooper, Andrew Fenton. 1997. *Niche Diplomacy: Middle Powers after the Cold War*. Houndmills, Basingstoke, Hampshire; New York: Macmillan ; St. Martin’s Press.

Crowards, Tom. 2002. “Defining the Category of ‘Small’ States.” *Journal of International Development* 14(2): 143–79.

Czina, Veronika. 2013. “Small State Influence in the European Union: The Case of ‘E-Stonia.’” Master Thesis. Central European University. http://www.etd.ceu.hu/2013/czina_veronika.pdf. (October 16, 2014).

Duursma, Jorri. 1996. *Fragmentation and the International Relations of Micro-States: Self-Determination and Statehood*. Cambridge: Cambridge University Press.

Ehin, Piret. 2010. *In Favour of an Open-Door Policy and an Ambitious Eastern Partnership*. EU-27 Watch. http://www.eu-28watch.org/?q=node/461.

Estonian Defence Forces website. *Operations abroad.* http://www.mil.ee/en/defence-forces/operations-abroad (December 2, 2014).

Estonian Defence League website. *Estonian Defence League’s Cyber Unit*. http://www.kaitseliit.ee/en/cyber-unit (December 4, 2014).

Estonian Ministry of Defence website. *Eelarve.* http://www.kmin.ee/et/eelarve (December 1, 2014).

Estonian Ministry of Defence website. *National Security Concept of Estonia.* http://www.kaitseministeerium.ee/files/kmin/img/files/National_Security_Concept_of_Estonia.pdf (December 2, 2014).

Estonian Ministry of Foreign Affairs website. *Estonia and NATO.* http://vm.ee/en/estonia-and-nato (December 1, 2014).

Evans, Graham. 1998. *The Penguin Dictionary of International Relations*. London: Penguin Books.

Finnemore, Martha, and Kathryn Sikkink. 1998. “International Norm Dynamics and Political Change.” *International Organization* 52(4): 887–917.

Fox, Annette Baker. 1959. *The Power of Small States*. Chicago; London: University of Chicago Press.

Friman, H. Richard. 1993. “Side-Payments versus Security Cards: Domestic Bargaining Tactics in International Economic Negotiations.” *International Organization* 47(3): 387–410.

Van Genderen, Ruben, and Jan Rood. 2011. *Water Diplomacy: A Niche for the Netherlands?*. Netherlands Institute of International Relations “Clingendael.”

Goetschel, Laurent. 1998. *Small States Inside and Outside the European Union Interests and Policies*. Boston, MA: Springer US. http://dx.doi.org/10.1007/978-1-4757-2832-3 (November 30, 2014).

Grøn, Caroline Howard, and Anders Wivel. 2011. “Maximizing Influence in the European Union after the Lisbon Treaty: From Small State Policy to Smart State Strategy.” *Journal of European Integration* 33(5): 523–39.

Hansen, Lene, and Helen Nissenbaum. 2009. “Digital Disaster, Cyber Security, and the Copenhagen School.” *International Studies Quarterly* 53(4): 1155–75.

Henriksen, Anders, and Ringsmose, Jens. 2012. “What Did Denmark Gain? Iraq, Afghanistan and the Relationship with Washington.” In *Danish Foreign Policy Yearbook 2012*, eds. Nanna Hvidt and Hans Mouritzen. Copenhagen: DIIS.

Henrikson, Alan K. 2005. “Niche Diplomacy in the World Public Arena: The Global ‘Corners’ of Canada and Norway.” In *The New Public Diplomacy*, eds. Jan Melissen and G.R. Berridge. Basingstoke: Palgrave Macmillan.

Hey, Jeanne A. K. 1995. “Foreign Policy in Dependent States.” In *Foreign Policy Analysis: Continuity and Change in Its Second Generation*, eds. Jeanne A. K. Hey, Laura Neack, and Patrick J. Haney. NJ: Prentice Hall.

Ilves, Luukas. 2011. “E-Estonian Foreign Policy.” *Diplomaatia* 98. http://www.diplomaatia.ee/en/article/e-estonian-foreign-policy/ (December 17, 2014).

Ilves, Luukas. 2013. “Küberturvalisus Ja Rõuged.” *Diplomaatia* (121). http://www.diplomaatia.ee/artikkel/kuberturvalisus-ja-rouged/ (December 18, 2014).

International Telecommunication Union website. *Definition of cybersecurity*. http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx (December 4, 2014).

Jakobsen, Peter Viggo. 2009. “Small States, Big Influence: The Overlooked Nordic Influence on the Civilian ESDP*.” *JCMS: Journal of Common Market Studies* 47(1): 81–102.

Joenniemi, Pertti. 1998. “From Small to Smart: Reflections on the Concept of Small States.” *Irish Studies in International Affairs* 9: 61–62.

Jurkynas, Mindaugas. 2014. “Security Concerns of the Baltic States in the Twenty-First Century.” In *Small States and International Security: Europe and beyond*, eds. Clive. Archer, Alyson J. K. Bailes, and Anders Wivel. Routledge, 113–29.

Kasekamp, Andres. 2013. “Estonia: Eager to Set an Example in Europe.” In *The New Member States and the European Union: Foreign Policy and Europeanization / Edited by Michael Baun and Dan Marek*, Routledge advances in European politics, eds. Michael J. Baun, Dan Marek, and Michael J. Baun. New York: Routledge, 99–111.

Katzenstein, Peter J. 1985. *Small States in World Markets: Industrial Policy in Europe*. Ithaca, N.Y: Cornell University Press.

Keohane, Robert O. 1969. "Lilliputians' Dilemmas: Small States in Internatinal Politics." *International Organization* 23(02): 291.

Keohane, Robert O.. 1982. "The Demand for International Regimes." *International Organization* 36(2): 325–55.

Klimburg, Alexander., ed. 2012. *National Cyber Security Framework Manual*. [Talinn, Estonia]: NATO Cooperative Cyber Defense Center of Excellence. http://www.ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf (December 6, 2014).

Knudsen, Olav F. 2002. "Small States, Latent and Extant: Towards a General Perspective." *Journal of International Relations and Development* 5(2): 182–98.

Kolga, Margus. 2013. "Väikeriik ÜROs – Kas Tulutu Jahmerdamine Või Kaasumisvõimalus?" *Diplomaatia* 113/114. http://www.diplomaatia.ee/artikkel/vaikeriik-uros-kas-tulutu-jahmerdamine-voi-kaasumisvoimalus/ (December 17, 2014).

Kronsell, Annica. 2002. "Can Small States Influence EU Norms?: Insights From Sweden's Participation in the Field of Environmental Politics." *Scandinavian Studies* 73(3): 287–304.

Laar, Mart. 2011. "Eesti Vabariigi Kaks Kakskümnendit." *Diplomaatia* 96. http://www.diplomaatia.ee/artikkel/eesti-vabariigi-kaks-kakskumnendit/. (December 17, 2014).

Lewis, James A. 2014. *Liberty, Equality, Connectivity: Transatlantic Cybersecurity Norms*. Center For Strategic and International Studies.

Maasikas, Matti. 2014. "Eesti Välispoliitika Kolmas Faas – Argipäev." *Riigikogu Toimetised* 30. http://www.riigikogu.ee/rito/index.php?id=14466. (December 10, 2014).

Maldre, Patrik. 2014. "Estonia and the US: Paving a Way Forward in Cyber Security." *estonian world*. http://estonianworld.com/security/estonia-us-paving-way-forward-cyber-security/ (December 1, 2014).

Mälksoo, Lauri. 2008. "Väikeriik Ja Rahvusvaheline Õigus." *Diplomaatia*. http://www.diplomaatia.ee/artikkel/vaikeriik-ja-rahvusvaheline-oigus/ (November 27, 2014).

Mälksoo, Lauri. 2013. “The Tallinn Manual as an International Event.” *Diplomaatia* 120. http://www.diplomaatia.ee/en/article/the-tallinn-manual-as-an-international-event/ (November 27, 2014).

Männik, Erik. 2004. “Small States: Invited to NATO — Able to Contribute?” *Defense & Security Analysis* 20(1): 21–37.

Marton, Péter, and Nik Hynek. 2012. “What Makes ISAF S/tick: An Investigation of the Politics of Coalition Burden-Sharing.” *Defence Studies* 12(4): 539–71.

May, Tim. 2001. *Social Research: Issues, Methods and Process*. 3rd ed. Buckingham [UK] ; Philadelphia: Open University Press.

Mihkelson, Marko. 2013. “Eesti Välispoliitika Kompassist Ja Eesmärkidest.” *Diplomaatia* 122. http://www.diplomaatia.ee/artikkel/eesti-valispoliitika-kompassist-ja-eesmarkidest/ (December 17, 2014).

Mouritzen, Hans. 2006. “The Nordic–Baltic Area: Divisive Geopolitics at Work.” *Cambridge Review of International Affairs* 19(3): 495–511.

Mouritzen, Hans, and Anders Wivel, eds. 2005. *The Geopolitics of Euro-Atlantic Integration*. London ; New York: Routledge.

NATO Allied Command Transformation 2014. Press release. “SACT and the Estonian Minister of Defence sign an agreement to establish the NATO Cyber Range Capability.” http://www.act.nato.int/sact-and-the-estonian-minister-of-defence-sign-an-agreement-to-establish-the-nato-cyber-range-capability (December 4, 2014).

NATO Cooperative Cyber Defence Centre of Excellence website. *History.* https://ccdcoe.org/history.html (December 4, 2014).

Neumann, Iver B., and Sieglinde Gstöhl. 2006. “Lilliputians in Gulliver’s World?” In *Small States in International Relations*, New directions in Scandinavian studies, Seattle : Reykjavik: University of Washington Press ; University of Iceland Press, 18.

Nye, Joseph S. 1990. “Soft Power.” *Foreign Policy* 80: 153–71.

Nye, Joseph S. 2010. *Cyber Power*. Belfer Center for Science and International Affairs, Harvard Kennedy School. http://belfercenter.ksg.harvard.edu/publication/20162/cyber_power.html. (November 27, 2014).

Olson, Mancur, and Richard Zeckhauser. 1966. “An Economic Theory of Alliances.” *Review of Economic Statistics* 48(3): 266–79.

Panke, Diana. 2010. *Small States in the European Union: Coping with Structural Disadvantages*. Farnham, Surrey, England ; Burlington, VT: Ashgate.

Pastore, Gunta. 2013. “Small New Member in the EU Foreign Policy: Toward ‘Small State Smart Strategy’?.” *Baltic Journal of Political Science* 2: 67–84.

Pernik, Piret. 2014. “Koostöö Tugevdamine Prantsusmaaga on Eesti Poliitiline Ja Pragmaatiline Huvi.” *International Centre for Defence Studies blog*. http://blog.icds.ee/article/242/koostoeoe-tugevdamine-prantsusmaaga-on-eesti-poliitiline-ja-pragmaatiline-huvi. (November 27, 2014).

Pernik, Piret, and Emmet Tuohy. 2013. *Cyber Space in Estonia: Greater Security, Greater Challenges*. Tallinn: International Centre for Defence Studies.

Rickli, Jean-Marc. 2008. “European Small States’ Military Policies after the Cold War: From Territorial to Niche Strategies.” *Cambridge Review of International Affairs* 21(3): 307–25.

Riina Kaljurand. 2013. “Security Challenges of a Small State: The Case of Estonia.” *Defence and Security for The Small: Perspectives from the Baltic States*: 55–81.

Romsloe, B. 2005. *Finland and the Case of a Northern Dimension for the EU: Inclusion by Bargaining or Arguing?*.

Rothstein, Robert L. 1968. *Alliances and Small Powers*. New York: Columbia University Press.

Sakkov, Sven. 2014. “Rock ‘n’ Roll and Heavy Metal. The Wales Summit and Estonia.” *Diplomaatia* 133. http://www.diplomaatia.ee/en/article/rocknroll-ja-heavy-metal-walesi-tippkohtumine-ning-eesti/ (December 17, 2014).

Schmitt, Michael N., ed. 2013. *Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence*. Cambridge ; New York: Cambridge University Press.

Shabbir, Nabeelah. 2014. “Estonia Offers E-Residency to Foreigners.” *The Guardian*. http://www.theguardian.com/world/2014/dec/26/estonia-offers-e-residency-to-world-what-does-it-mean (December 2, 2014).

Sillaste-Elling, Kyllike. 2013. “Pilguheit Eesti Välispoliitika Üldseisule.” *Diplomaatia* 122. http://www.diplomaatia.ee/artikkel/pilguheit-eesti-valispoliitika-uldseisule/ (December 17, 2014).

Steinmetz, Robert, and Anders Wivel, eds. 2010. *Small States in Europe: Challenges and Opportunities*. Farnham, England ; Burlington, Vt: Ashgate Pub. Company.

Tallberg, Jonas. 2004. “The Power of the Presidency: Brokerage, Efficiency and Distribution in EU Negotiations*.” *JCMS: Journal of Common Market Studies* 42(5): 999–1022.

Thorhallsson, Baldur, and Anders Wivel. 2006. “Small States in the European Union: What Do We Know and What Would We Like to Know?” *Cambridge Review of International Affairs* 19(4): 651–68.

The White House website, *The United States and Estonia - NATO Allies and Global Partners.* http://www.whitehouse.gov/the-press-office/2013/08/30/fact-sheet-united-states-and-estonia-nato-allies-and-global-partners?utm_medium=referral&utm_source=t.co (December 2, 2014).

Thucydides. 1972. *History of the Pelepennesian War*. London: Penguin Books.

Tiirmaa-Klaar, Heli. 2010. “Rahvusvaheline Koostöö Küberjulgeoleku Tagamisel.” *Diplomaatia* 85. http://www.diplomaatia.ee/artikkel/rahvusvaheline-koostoo-kuberjulgeoleku-tagamisel/ (December 2, 2014).

Tikk, Eneken, Kadri Kaska, and Liis Vihul. 2010. *International Cyber Incidents: Legal Considerations*. Tallinn, Estonia: Cooperative Cyber Defence of Excellence (CCD COE).

Tollison, Robert D., and Thomas D. Willett. 1979. “An Economic Theory of Mutually Advantageous Issue Linkages in International Negotiations.” *International Organization* 33(4): 425–49.

Tuohy, Emmet. 2012. *Toward an EU Cybersecurity Strategy: The Role of Estonia*. International Centre for Defence Studies.

Vahtre, Lauri. 2011. “Eesti Vabariigi Kaks Kakskümnendit.” *Diplomaatia* 96. http://www.diplomaatia.ee/artikkel/eesti-vabariigi-kaks-kakskumnendit/ (December 17, 2014).

Värynen, Raimo. 1971. “On the Definition and Measurement of Small Power Status.” *Cooperation and Conflict* 6(2): 91–102.

Wallace, H. 2005. “‘Power and Influence: Assessing Member States’ Roles in EU Governance and Negotiation’.” In *Member States and the European Union*, eds. S. Bulmer and C. Lequesne. Oxford: Oxford University Press, 25–44.

Walt, Stephen M. 1987. *The Origins of Alliances*. Ithaca: Cornell University Press. http://site.ebrary.com/id/10747056 (December 1, 2014).

Wivel, Anders. 2005. “The Security Challenge of Small EU Member States: Interests, Identity and the Development of the EU as a Security Actor.” *Journal of Common Market Studies* 43(2 (06)): 393–412.

Wivel, Anders. 2010. “From Small State to Smart State: Devising a Strategy for Influence in the European Union.” In *Small States in Europe: Challenges and Opportunities*, eds. Anders Wivel and Robert Steinmetz. Farnham, England ; Burlington, Vt: Ashgate Pub. Company.

Appendix 1 – Questions addressed during the interviews with officials of the Estonian MFA and MoD

1. What role does the area of cyber security play in Estonia's foreign and security policy?
2. Has Estonia specialised in cyber security? Could it be regarded as a "niche" in foreign and security policy? Are Estonia's efforts in cyber security valued by its strategic partners and international organisations? Does Estonia have influence in matters of cyber security?
3. Does Estonia use the cyber security niche to gain wider influence in foreign and security policy? In what type of relations does the niche have its effect (bilateral relations and international organisations)?
4. What type of influence is sought by using the niche? In which areas influence is sought? Or what type of influence is gained by having the niche? What are the effects on wider security and foreign policy (i.e., not only gained influence within the cyber-related issues)?
    a. Has there been any concrete trade-offs and gains?
    b. Has the niche generated "reaffirmation" of security guarantees by strategic partners?
    c. Has the niche provided more access to prominent officials?
    d. Has the niche worked as a "catalyst" for new bilateral relations?
5. Is the development of the niche based on a conscious decision (i.e., is or was there a clear strategy to develop and utilise the niche)? How and why was the niche developed? What were the effects of the 2007 cyberattacks?
6. How would you characterise the area of cyber security in the context of it being a niche that could be used to have wider influence in foreign and security policy?
7. What are the possible problems in having the niche in the context of foreign and security policy?
    a. Is having a niche in cyber security sustainable while most Estonia's partners are heavily investing in the issue? How could Estonia sustain the positive image? Could Estonia find a "niche within the niche"?

b. May there be unrealistic expectations of Estonia's capabilities?
c. Could the "niche-oriented strategy" be viewed as "too obvious" by strategic partners? Could Estonia be viewed as exaggerating its capabilities? Could Estonia be viewed as being "too pushy" by using the niche to get wider gains?

Kokkuvõte

Väikeriik kasutamas ära nišivõimekust omamaks mõju välis- ja julgeolekupoliitikas: Eesti ja küberjulgeoleku näitel

Käesoleva magistritöö eesmärk oli Eesti näitel uurida, kuidas saavad väikeriigid kasutada ära oma nišivõimekusi, et omandada laiemat mõju välis- ja julgeolekupoliitikas. Selleks vaadeldi lähemalt, millist rolli on mänginud Eesti välis- ja julgeolekupoliitikas tema rahvusvaheliselt tunnustatud nišivõimekus küberjulgeoleku valdkonnas.

Magistritöö teoreetiline raamistik põhines lähenemistel, mis keskenduvad väikeriikide käitumisele. Siinkohal on oluline mainida, et olemasolev väikeriike käsitlev kirjandus on keskendunud eelkõige sellele, kuidas saavutada mõju valdkonnas, millele väikeriik on spetsialiseerunud (Joenniemi 1998, Arter 2000; Wivel 2005; Jakobsen 2009; Rickli 2009; Grøn ja Wivel 2011) – nišivõimekuse mõju väikeriigi laiemale välis- ja julgeolekupoliitikale on üldjoontes jäänud tähelepanuta (Kronsell 2002, 17; Nasra 2010, 1). Seetõttu lähenes magistritöö uurimisprobleemile eelkõige induktiivselt, kuid samas loodi ka ülevaade teoreetilistest lähenemisest, mis võivad antud kontekstis relevantsed olla. Lisaks kirjeldas magistritöö Eesti välis- ja julgeolekupoliitika põhimõtteid väikeriike käsitlevate teooriate raames – kokkuvõtvalt saab väita, et Eesti on käitunud vastavalt teooriates sätestatud loogikatele, olles valinud Venemaast juhinduvatel julgeolekupoliitilistel kaalutustel selgelt n-ö liitumisstrateegia (ingl *alignment strategy)* sidudes end tugevalt lääneriikide ja rahvusvaheliste organisatsioonidega. Magistritöö analüüsis ka Eesti edusamme küberjulgeoleku valdkonnas, mille tulemusena kinnitati selge nišivõimekuse olemasolu.

Selleks, et saada detailne ülevaade „kübernišši“ rollist Eesti välis- ja julgeolekupoliitikas, viidi läbi kaheksa poolstruktureeritud intervjuud Eesti Vabariigi Välisministeeriumi ja Kaitseministeeriumi ametnikega. Vältimaks liiga Eesti-keskset vaadet, intervjueeriti ka kahte suurriigi ametnikku, kes on töötanud Eestis küberjulgeoleku valdkonnas.

Toetudes intervjuude tulemustele ning töös eelpool välja toodud teoreetilisele ja empiirilisele taustainfole, olid magistritöö peamised järeldused järgnevad:

- Nišivõimekus küberjulgeolekus on väidetavalt tugevdanud Eesti positiivset imidžit ja mainet, ning seeläbi loonud Eestile n-ö pehmet jõudu (Nye 1990; Ilves 2011; Areng 2014) ja diplomaatilist kapitali (Adler-Nissen 2008, 670). Intervjuudele põhinedes saab järeldada, et nišš on mänginud olulist rolli Eesti printsipiaalses välis- ja julgeolekupoliitilises strateegias, mille eesmärk on olla väärtuslik ning usaldusväärne partner, kes panustab oma „õiglase osa“ rahvusvahelistes organisatsioonides ning bilateraalsetes suhetes. Seetõttu saab väita, et kõige olulisim nišist tulenev eeldatav kasu on Eesti strateegiliste partnerite poolt pakutavate julgeolekugarantiide kinnistamine. Siinkohal tuleb siiski märkida, et nišivõimekust ei nähtud sama olulisena Eesti strateegiliste partnerite jaoks kui välisoperatsioonidesse panustamist ja kaitsekulutuste kõrget taset.
- Nišivõimekus küberjulgeolekus on tekitanud ka teisi positiivseid mõjusid. Küberišš on loonud täiendavaid suhtluskanaleid ning hõlbustanud koostööd Eesti strateegiliste partneritega, tugevdanud heidutust ning tekitanud positiivset majanduslikku mõju.
- Kuna väga kõrgelt väärtustatud või unikaalseid sõjalisi võimekusi küberjulgeoleku valdkonnas ei tuvastatud, siis ei saanud nišši vaadelda kui selgelt eristatavat võimekust, mida võiks rahvusvahelistes läbirääkimistes kasutada n-ö kaubana, mis oleks vahetatav toetuse vastu teistes julgeolekuvaldkondades. Seetõttu ei kinnitanud Eesti näide ka teoreetilist eeldust, et väikeriigil on kergem omada kõrgelt hinnatud kübervõimekusi, mille arendamine on oluliselt odavam võrreldes konventsionaalsete sõjaliste võimekustega.
- Eesti positiivne imidž ning edu küberjulgeoleku valdkonnas on oluliselt põhinenud võimel olla aktiivne ja pakkuda rahvusvahelisi lahendusi poliitilisel ja strateegilisel tasemel. Taoline lähenemine tuvastati kui väikeriigi jaoks sobilik kulutõhus meetod nišivõimekuse presenteerimiseks.

- Küberjulgeolekut kui nišivaldkonda nähti kui „tihket“ valdkonda, mis võib tekitada n-ö ülekanduvat mõju (ingl *spillover*) rahvusvahelises koostöös (Keohane 1982, 340): küberjulgeoleku erinevaid valdkondi kattev olemus andis Eestile võimaluse kasutada n-ö teemaseostust (ingl *issue-linkage*), et siduda nišš ka teiste välis- ja julgeolekupoliitiliste küsimustega. Küberjulgeoleku „laia haarde“ tõttu oli Eestil võimalus ka oma nišivõimekust rakendada kõikides olulistes rahvusvahelistes organisatsioonides.
- Küberjulgeolekut vaadeldi kui valdkonda, mis eeldab rahvusvahelist koostööd – see omadus on soodustanud Eesti nišivõimekuse teket ning selle laiemat mõju, kuna mitmed Eesti poolt loodud ning rahvusvaheliselt hinnatud ettevõtmiste (nt NATO CCD COE või küberlabor) väärtus on oma olemuselt sõltuvad rahvusvahelisest koostööst.
- Eesti suutis kasutada ära nišivõimekust, et saada laiemat mõju, kuna nišš pakkus riigile võimaluse näidata end keskendumas valdkonnale, mis ei ole väga kitsalt seotud väikeriigi piiritletud (Venemaast lähtuvate) huvidega. See võimaldas Eestil esitleda oma väärtuslikkust strateegiliste partneritele, kes on nišivõimekuse arendamist selgelt pooldanud ning selle vastu huvi näidanud.
- Uurimustulemused ei tuvastanud väga selgelt strateegilist raamistikku, mis määratleks, kuidas saaks Eesti nišivõimekust kasutada, et omandada mõju välis- ja julgeolekupoliitikas. Kui Eesti ambitsioon on säilitada või suurendada nišivõimekuse positiivset rolli välis- ja julgeolekupoliitikas, siis oleks soovitatav vastu võtta selge strateegiline või poliitiline otsus, mille tulemusena koondada väikeriigi piiratud ressursid eesmärgiga kujundada välja konkreetne võimekus kübervaldkonna raames. Eesti võiks näiteks panustada võimekusse olla jätkuvalt rahvusvaheliselt väärtustatud kui innovaatiliste poliitiliste ja strateegiliste suuniste looja või võimalusel arendada välja kõrgetasemeline sõjaline võimekus küberjulgeoleku valdkonnas.