UNIVERSITY OF TARTU

Faculty of Social Sciences and Education

Master's Thesis

Aaron Melby

Discourse Analysis and Small State 'Cyber Norms': Estonia's Views on Benefits, Limitations, and Cooperation

Supervisor: Eoin McNamara, M. Sc.

Tartu 2016

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

…….

/Aaron Melby/

Abstract

Cyber norms are a topic of growing importance, but very little work has been done in relation to a small states ability to create and promote cyber norms. This thesis argues that Estonia is a traditional small state and seeks to determine how Estonia perceives its ability to create and promote cyber norms. To do this this Martha Finnemore's theory of the cyber norm cultivation has been used. In addition, this thesis uses Alam and Chantzos theory on how the private sector contributes to the creation of norms to determine how successful Estonia has been at integrating the private sector.

Five interviews were conducted with officials and experts that are knowledgeable on cyber issues, from a variety of departments in the Estonian government. Discourse analysis was used in order to analyze and determine the official the dominate view of Estonia in relation to three areas, protection of critical infrastructure, e-governance as a norm, and the free and open internet. Through discourse analysis official views on the ability of Estonia to create and promote norms in these areas was determined. In addition the benefits and limitations that Estonia faces while promoting norms and their perceived relationship with the private sector was also analyzed.

This thesis finds that despite Estonia being considered a small state they perceive themselves as being fairly effective at promoting cyber norms in most of the areas. Estonia also perceives itself as facing many of the limitations that have traditionally been attributed to small states. Specifically, limited resources are perceived as limiting Estonia's ability to promote cyber norms in most cases. The benefits that Estonia perceives itself to receive from the promotion of cyber norms is diverse and ranges from financial to the minimizing the risk of conflict by creating clarity. Like the diverse range of benefits that Estonia is perceived to receive from promoting these cyber norms, their ability to cooperate with the private sector varies from topic to topic. Some areas like the protection of critical infrastructure receive good cooperation between the private sector and Estonia, while other areas such as the promotion of a free and open internet or portrayed as having marginal cooperation and less of a need for cooperation.

Table of Contents

1. Introduction

The internet has both expanded existing opportunities and created new opportunities, but it has also created an environment where states, citizens, and the private sector are vulnerable to advanced and constantly changing threats.[1] The vulnerability has been highlighted by the significant cost of cyber crime, as well as the high profile cyber attacks such as Stuxnet, the Sony hack, and the 2007 attacks in Estonia.[2] Because of the threats faced by state and non-state actors a consensus has formed that some behaviors in cyberspace must be constrained in order to maintain peace and security. Although there are multiple ways in which behavior in cyberspace could be constrained, but 'cyber norms' currently appear to be the best choice.[3] This does not mean that a consensus has formed around exactly what kinds of behavior need to be constrained, or how to constrain the behavior, just that a broad consensus exists on the need to take action.

There are several definitions for that have been proposed in order to describe what a norm is. Most of these definitions mention behaviors for a certain identity. In this thesis Peter Katzenstien's more traditional definition for a norm has been used, which states that, "norms are collective expectations about proper behavior for a given identity."[4] Following

[1]Maria Osula and Henry Rõigas, "Introduction," in *International Cyber Norms: Legal, Policy and Industry Perspectives,* ed. Anna-Maria Osula and Henry Rõigas. (Tallinn: NATO CCD COE, 2016): 11.
[2] Joseph S. Nye, Jr., "Cyber Power," *Belfer Center for Science and International Affairs* (Harvard, 2010): 9, http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf.; and Tim Maurer, "Cyber Norms Emergence at the United Nations: An Analysis of the Activities at the UN Regarding Cyber Security?" Discussion paper #2011-11, Cambridge, Mass.: *Belfer Center for Science and International Affairs, Harvard Kennedy School* (September 2011): 23.
[3] Maria Osula and Henry Rõigas, "Introduction," 11.
[4] Perter J. Katzenstien, "Norms, Identity, and Culture in National Security," in *Culture of National Security: Norms and Identity in World Politics,* ed. Peter J. Katzenstien (New York: Columbia University Press, 1996), 54.

this logic cyber norms have been conceptualized as the 'expectations' of appropriate behavior for a 'given identity' acting in cyber space.

Estonia is taking action by promoting cyber norms in multiple areas of foreign policy. Specifically, Estonia is promoting norms regarding a free and open internet, internet governance, and the protection of critical infrastructure. Small states, like Estonia, have a vested interest in taking action and creating norms in these policy areas. This is reflected in the dominate discourse of Estonia, as well as the belief that Estonia can play a role in shaping the norms in these areas.

Small states face both advantages and disadvantages in cyberspace, but the disadvantages may significantly out way the advantages. One of the advantages for small states is that the cost of developing cyber capabilities is relatively low compared to the cost of developing conventional military capabilities. This means that small states are able to wield more power in cyberspace than they traditionally have been able to hold in other 'domains' (for instance sea, space, or land).[5]

However, recent scholarship suggests that despite the lower cost to develop capabilities, small states are still faced with significant disadvantages in cyberspace. First small states with specialized economies are extremely reliant on 'global flows' of information.[6] Second, small states that have wide spread internet usage and a reliance on the

[5] Joseph S. Nye, Jr., "Cyber Power," 4 and 19. There is contentious debate over whether cyber is a domain of warfare. Here "domain" only refers to an area of operation.
[6] Mika Aaltola et al., "Securing the Global Commons: A Small State Perspective" (working paper, FIIA, 2011); 6 and 27, accessed May 10, 2015 http://www.fiia.fi/en/publication/198/securing_global_commons/.

internet are increasingly vulnerable to cyber threats.[7] This is due to the fact that the more reliant a country and its citizens are on the internet the more problems a disruption of services is likely to cause. For Estonia the heavy penetration of the internet and the increasing reliance on 'e-government' and 'e-services' makes this vulnerability particularly relevant. Third, larger states are spending vast sums of money on cyber security and the development of cyber capabilities. Small states due to limited financial resources, are unlikely to be able to match the heavy spending of large countries.[8] Finally, small states face impediments to developing and maintaining knowledge. This is because, small states are simultaneously faced with smaller institutions that have less employees and difficulties in retaining the talent that they possess.[9] For a small state this should be a very relevant concern because when it comes to having influence on a particular issue administrative capabilities, knowledge, and competance are extremely important for a small state.[10]

As a result of the vulnerabilities that small states face, they have large incentives to help create 'cyber norms.' Estonia (among other nations) has recognized the need for cyber norms and has been active in the process of developing new or 'emerging norms.'[11] Collin Allan and Matthew Crandall have shown that Estonia has worked successfully as norm entrepreneurs in the emergent phase, while other authors have shown that Estonia has become

[7] Joe Burton, "Small states and cyber security: The case of New Zealand," *Political Science* 65, no. 2 (2013): 223-4, accessed February 3, 2016, DOI: 10.1177/0032318713508491.
[8] IBID, 224.; and Liina Areng, "Lilliputian States in Digital Affairs and Cyber Security," in *The Tallinn Papers: Numbers 1-9 (2014-2015)*, ed. Liis Vihul, (Tallinn: NATO CCD COE, 2015).
[9] Joe Burton, "Small states and cyber security: The case of New Zealand,", 229.
[10] IBID, 237.; and Baldur Thorhallsson, "Small States in the UN Security Council: Means of Influence?" *Hague Journal of Diplomacy* 7, (2012): 151-2 and 160, accessed February 19, 2016, DOI: 10.1163/187119112X628454.
[11] Collin Allan and Matthew Crandall, "Small States and Big Ideas: Estonia's Battle for Cybersecurity Norms," *Contemporary Security Policy* 36, no. 2 (July, 2015).

a very influential small state in relation to cyber matters.[12] However, no studies have been completed on how a small state perceives their ability to create and promote cyber norms or how the perceive cooperation with the private sector in these processes. As a result, this thesis seeks to determine how the small state of Estonia views its ability create and promote cyber norms and how it views the cooperation with the private sector throughout the processes.

Although Estonia's view on cooperating with the private may not seem important the creation and promotion of cyber norms, there are several reasons why it should influence the dominate discourse on cyber norms. First, much of the information and communication technology (ICT) infrastructure is owned by the private sector and as a result governments and private companies rely on the same infrastructure.[13] Second working with the private sector may help to increase the knowledge of public officials and institutions, which could help offset the problems related to retaining talent.[14] Third, collaborating with the private sector may create norms that are more feasible both technologically and economically. Fourth, the development of 'cyber norms' necessitates cooperation between a wide range of

[12] IBID; Piret Pernik and Emmet Tuohy, "Cyberspace in Estonia: Great Security, Greater Challenges," *International Center for Defence Studies* (August, 2013), accessed November 29, 2015, http://www.riso.ee/et/koosvoime/raamistik.; and Henry Rõigas, "A Small State Utilizing its Niche Capability for Influence in Foreign and Security Policy: The Case of Estonia and Cyber Security" (master's thesis, University of Tart, 2015),http://dspace.ut.ee/bitstream/handle/10062 /45179/roigas_henry_ma_2015.pdf?sequence= 1&isAllowed=y.

[13] Scott Charney, "Governments and APTs: The Need for Norms" in *Cybersecurity Norms: Advancing persistent Security* (n.p., Microsoft, 2014): 12-13.

[14] Shireen Alam and Ilias Chantzos, "Technological Integrity and The Role of Industry in Emerging Cyber Norms," in *International Cyber Norms: Legal, Policy and Industry Perspectives,* ed. Anna-Maria Osula and Henry Rõigas. (Tallinn: NATO CCD COE, 2016): 205-7.

actors including states and the private sector.[15] Finally, insight into how Estonia cooperates with the private sector in 'norm cultivation,' could expose successes that other states could attempt to replicate, or shortfalls that could be analyzed and improved.

To explore how Estonia frames the development and promotion of cyber norms and the role that the private sector plays, this thesis has been structured as follows. The next chapter provides a literature review and theoretical framework. Specifically, it looks at the literature on small states and norms, defines key concepts, and discusses the theory used for analysis. Chapter two is followed by a section detailing the methodology. Chapter four provides a general overview of how Estonia sees itself in terms of being able to create and promote cyber norms. Chapters five through seven provide analysis of the three different policy strands. In the final chapter (eight), conclusions are drawn from the existing literature as well as analysis from the interviews.

2. Literature Review and Theory

This chapter seeks to provide an overview of the relevant literature, concepts, and theory in order to provide a framework and necessary knowledge to understand how Estonia frames cyber norm development and cooperation with the private sector. First, a brief overview of the developments of in small state studies is provided. Next, a section is devoted to the concept of small states, which details the difficulties of defining a small state and

[15] Martha Finnemore, "Cultivating International Cyber Norms," in America's Cyber Future: Security and Prosperity in the Information age, ed. Kristin M. Lord and Travis Sharp (Washington, D.C.: Center for a New American Security, 2011), (Pages), https://www.cnas.org/files/documents/publications/CNAS_Cyber_Volume%2011_2.pdf.

proposes a definition for small states in cyber space. The third section details small states and their efforts to build norms. Finally, the last section details the developments in literature on cyber norms and explains the framework of norm cultivation, which will be used to analysis how Estonia has coordinated with the private sector in developing cyber norms.

2.1 Overview of Small State Studies

There are several branches of small state literature, but the realist/neorealist has traditionally been the dominate view of small states in international relations.[16] Christopher Browning summaries how small states have traditionally been viewed in the literature as:

> In the international relations literature and in world politics size has generally been connected to capability and influence. Whilst being big is correlated with power, being small has been viewed as a handicap to state action, and even state survival. In many discourses and debates, small states are frequently ignored, the view being that ultimately they have to go along with the frames dictated by larger, more powerful states. [17]

In this traditional view with the focus on capabilities and power offer states the ability to achieve goals, while the lack of power and capabilities leaves states largely at the mercy of other more powerful states. Examples of this can be seen in the special status the Congress of Vienna afforded several larger states.[18]

After World War II the proliferation of international institutions including the United Nations (UN) gave small states a forum to voice their opinions and promote their values.

---

[16] Iver B. Neumann and Sieglinde Gstöhl, "Lilliputians in Gulliver's World?" in *Small States in International Relations* (Reykjavik: University of Iceland Press, 2006) 9-17.
[17] Christopher S Browning, "Small, Smart and Salient? Rethinking Identity in the Small State Literature," *Cambridge Review of International Affairs* 19, no. 4 (December, 2006): 669, accessed January 11, 2016, http://dx.doi.org/10.1080/09557570601003536.
[18] Archer, Clive; Bailes, Alyson J.K.; Wivel, Anders. "Small States and International Security: Europe and Beyond." (Florence: Taylor and Francis, 2014):54, (accessed March 17, 2016) http://GLA.eblib.com/patron/FullRecord.aspx?p=1683235.

Small states began to take international organizations very seriously and were even influential in the creation of some policies and norms. This contradicted some of the premises of the realist school and as a result liberalist and constructivist theories of small states began to emerge.[19] Scholar of these theories have questioned whether there are other forms of power that lie outside of military power, and whether small states are able to wield that power to have influence.[20] Instead of following traditional assumptions, these approaches see small states as actors which may sometimes be constrained, but still are able to have influence in international relations instead of being forced to react to the actions.

Institutionalist see small states as the primary beneficiaries of international institutions like the United Nations or the EU. For small states institutions reduces anarchy by constraining more powerful actors. By being a part of institutions small states are able to balance against great powers. This does not mean that small states don not still face some level pressure form great powers, but their ability to exert pressure is constrained.[21] This constraint is accomplished through norms, which limit a state's action to that of what is deemed to be acceptable behavior by the group. Along this line of thanking the primary motivation for a small state joining NATO would be the norms that provide states with

[19] IBID, 54-7.; and Anders Wivel, "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, no. 2 (June, 2005): 393–412.
[20] Christopher S Browning, "Small, Smart and Salient? Rethinking Identity in the Small State Literature," 671.; and Baldur Thorhallsson, "Small States in the UN Security Council: Means of Influence?" *Hague Journal of Diplomacy* 7, (2012): Pages, accessed February 19, 2016, DOI: 10.1163/187119112X628454.
[21] Anders Wivel, "The Security Challenge of Small EU Member States: Interests, Identity and the Development of the EU as a Security Actor." 395.

security guarantees, such as article 5, and the ability it gives them to balance threats to sovereignty.

Although constructivist would agree that the power of norms is important, they differ on the primary reason why states join international institutions. Whereas liberal institutionalist would propose small states are primarily motivated to join institutions because they constrain other states, constructivist see identity as the primary factor.[22] Identity can be thought of as the distinctiveness of an actor that is both internalized and externalized, but changes overtime through interaction.[23] In other words, from a constructivist viewpoint, small states join institutions because they closely match their self-image. This view can also be extended to a small states decision to remain neutral. Although realist would argue that neutrality is a survival strategy used by small states to maintain sovereignty, Laurent Goetschel argues that there is an idealistic dimension, which minimizes the use of force and force project.[24] Just because a small state joins a group or organization does not that they do not try to change norms or advance new norms inside the institutions to which they belong. Identity can also have a strong influence on institutions, and by preforming an identity the institutions structures can change.[25] This point is particularly relevant for the case of Estonia and cyber norms. How Estonia frames the discourse on cyber norms is important because it

[22] Baldur Thorhallsson, "Small States in the UN Security Council: Means of Influence?" 143.
[23] Perter J. Katzenstien, "Norms, Identity and Culture in National Security," in *Culture of National Security: Norms and Identity in World Politics*, ed. Peter J. Katzenstien (New York: Columbia University Press, 1996), 59.
[24] Laurent Goetschel, "Neutrals as Broker of Peace Building Ideas?" *Cooperation and Conflict* 46 no. 3 (2011): 312-33.
[25] Perter J. Katzenstien, "Norms, Identity and Culture in National Security," 64.

can determine whether it facilitates cooperation or conflict.[26] Christine Ingebritsen and other scholars have shown that small states can indeed be 'norm entrepreneurs' and that they are particularly effective at promoting norms relating to conflict resolution and human rights.[27] Part of the reason for the success has been that these norms have built onto existing ideas of the institution. Meaning norms are more likely to be accepted if they are framed in a way that highlights there compatibility with existing ideas.

2.2 Defining a Small State

The concept of small state can vary widely depending on the context and author, and despite several efforts there is not a universal definition of small state.[28] This is partially due to the wide range of topics covered by small state studies which makes it difficult to create a universal definition that still provides quality analysis. Additionally 'small' and 'large' are both relative concepts, which means it largely depends on the context and individual perception.[29] Due to the lack of a clear definition for the concept of a small state this section reviews the prominent definitions in order to justify the definition of a small state used in this thesis.

---

[26] Henrik Larsen, *Foreign Policy and Discourse Analysis: France, Britain and* Europe (New York: Routledge, 1997), 26-27.
[27] Christine Ingebritsen, *Scandinavia in World Politics* (New York: Rowman and Littlefield, 2006).
[28] Clive Archer, Alyson J.K. Bailes, and Anders Wivel,. Small States and International Security: Europe and Beyond," 59.; and Buldur Thorhallssonn and Anders Wivel, "Small States in the European Union: What Do We Know and What Would We Like to Know?" *Cambridge Review of International Affairs* 19, no. 4 (December, 2006): (Pages), accessed January 11, 2016, http://dx.doi.org/10.1080/09557570601003502.
[29] Peter R. Baehr, "Small States: A Tool for Analysis," *World Politics* 27, no. 3 (April, 1975): 459, accessed March 17, 2016, http://www.jstor.org/stable/2010129.

In the literature on small state studies the vast majority of the definitions use objective (quantitative) criteria, subjective (qualitative) criteria, or a combination of both. Objective criteria is easily measureable and focuses on capabilities. These capabilities can consist of criteria such as geographical size, population size, gross domestic product (GDP), and military expenditures and as a result focus on power.[30] Like most definitions there are both benefits and limitations to defining small states based on these criteria.

Archer et.al, describes 3 benefits that arise from using measurable capabilities to create a definition of a small state. First, indicators for capacity of small states helps in the process of analyzing impediments, prospects, and limitations. Second, objective criteria can create a definition that is easy to understand and apply. Finally, definitions relating to the possession of power facilitate the use of the vast quantities of literature on power and security in IR, which aids in determining what differentiates security challenges of small states from those of large states.[31] Although these advantages may all be desirable, the choice to focus only on capabilities results in limitations. Although objective criteria can illuminate certain challenges, it does not reveal all challenges faced by small states or how small states are perceived by others. Additionally these criteria will to some extent always be arbitrary.[32] For instance if one country is considered a large based on military expenditures, but small in terms of geographic sizes, the decision to define it as a small or large state becomes arbitrary. Additionally the separation criteria for categories is also primarily arbitrary. An example is

[30] Clive Archer, Alyson J.K. Bailes, and Anders Wivel,. Small States and International Security: Europe and Beyond," 59.
[31] IBID, 60.
[32] Buldur Thorhallssonn and Anders Wivel, "Small States in the European Union: What Do We Know and What Would We Like to Know?" 653.

criteria for determining a small state based on population size. The World Bank defines countries with a population of less than 1.5 million people as a small state, while others define a small state as having a population of 10 to 15 million.[33] A final potential drawback is that no matter which criteria is used the objective category is largely linked to security policy.[34]

Because of the limitations of objective definition some scholars prefer subjective criteria. Robert Rothstein uses subjective criteria in his definition of a 'small power' (state) is an example that is often cited. He defined a small power as a state that knows its own capabilities are insufficient to maintain its security and as a result it must seek security from other states and institutions. The final criteria of Rothstein's definition is that the small states vulnerability in security must be confirmed by other states.[35] Keohane has also advocated for the use of subjective criteria although different from those use by Rothstein. He argues that the perceptions of a state's leaders should be analyzed to determine how they perceive their states ability to have an effect on the international system. By doing this he removes the terms large state and small state and replaces them with four categories based on ability affect the international system.[36]

In an effort to overcome the short falls of both the objective and subjective criteria some scholars have combined the criteria to create a hybrid definition. This in some cases

---

[33] Peter R. Baehr, "Small States: A Tool for Analysis," *World Politics* 27, no. 3 (April, 1975): 459, accessed March 17, 2016, http://www.jstor.org/stable/2010129.; and World Bank, 'Small States: Meeting Challenges in the Global Economy', *Report of the Common wealth Secretariat /World Bank Joint Taskforce*, (April 2000), http://siteresources.worldbank.org/PROJECTS/ Resources/meetingchallengeinglobaleconomyl.pdf.
[34] Buldur Thorhallssonn and Anders Wivel, "Small States in the European Union: What Do We Know and What Would We Like to Know?" 653.
[35] Robert R. Rothstein, *Alliances and Small Powers*, (New York: Columbia University Press, 1968): 29.
[36] Robert O. Keohane, "Lilliputians' Dilemmas: Small States in International Politics," *International Organization* 23, no. 2 (March, 1969): 295-6, accessed December 14, 2015, DOI:10.1017/S002081830003160X.

can prove more useful in terms of analysis. For instance, Thorhallsson and Wivel, note that a combined definition can be useful in analyzing small states in the EU.[37] The combined definition does also help to overcome the security bias, but it still retains a level of arbitrariness. As a result it has been argued that states should not be generalized as small based on quantitative criteria and that a universal definition should be avoided. This is because a state's ability to have influence depends on the area.[38]

These considerations have led to another way of defining a small state. Recently scholars have begun to argue that small states should be defined in a spatio-temporal context. This definition includes more context and accounts for a small states "specific role in, and adjustment to globalized features of the world scene."[39] This is important because a state can at the same time be weak in one aspect, but strong in another. In this regard the spatio-temporal definition "…of small states changes focus from possession of power to the exercise of influence."[40]

Due to the shortfalls associated with using only objective or subjective criteria this thesis utilizes a spatio-temporal definition of a small state. This thesis takes the position that in an asymmetric relationship a small state is the weak part in the relationship.[41] Additional objective and subjective criteria have also been added to take into consideration the power

[37] Buldur Thorhallssonn and Anders Wivel, "Small States in the European Union: What Do We Know and What Would We Like to Know?" 654.
[38] Baldur Thorhallsson, "Small States in the UN Security Council: Means of Influence?" 139.
[39] Clive Archer, Alyson J.K. Bailes, and Anders Wivel,. Small States and International Security: Europe and Beyond," 62-6.
[40] Buldur Thorhallssonn and Anders Wivel, "Small States in the European Union: What Do We Know and What Would We Like to Know?" 654-5.
[41] Clive Archer, Alyson J.K. Bailes, and Anders Wivel,. Small States and International Security: Europe and Beyond," 62-6.

asymmetries of cyberspace. As mentioned before although a small state is able to gain a disproportional amount of power in cyberspace, they also face significant vulnerabilities as a result of their size. Specifically they face problems regarding: knowledge retention and a limited pool to draw talent from; a financial disadvantage that makes keeping up with much larger states difficult; and increased vulnerability due to being heavily dependent on cyberspace and flows of information.

Estonia easily qualifies as a small state based on the spatio-temporal definition and the added objective and subjective criteria, which takes into account the power asymmetries of cyberspace. The population of Estonia is around 1.3 million people, which qualifies it as a small state using the World Bank's definition of 1.5 million and the much larger definitions of small states.[42] The inclusion of the population in the definition helps to take into consideration that a small state has a limited pool in which to pull knowledgeable administrators and information technology (IT) professionals from. The GDP of Estonia also qualifies it a small state as it is one of the lowest among both NATO countries and the EU.[43] GDP is an extremely important factor when taking into consideration the asymmetries of cyberspace. Not only should a lower GDP make it harder to attract and retain talent, it also has an impact on the level of research and development a country can afford.

The last criteria for this definition is subjective and relates to dependence on cyberspace. This allows for a better understanding of the asymmetries of small states in this

[42] Peter R. Baehr, "Small States: A Tool for Analysis," 459,; and World Bank, 'Small States: Meeting Challenges in the Global Economy'
[43] World Bank, "Gross Domestic Product 2014," *World Development Indicators Database,* (February 17, 2016), http://databank.worldbank.org/data/download/GDP.pdf.

particular domain. If a small state is heavily reliant on information technology then it is more vulnerable to attacks in cyberspace.[44] This does not mean that a states can't minimize the risk to their systems, but reliance creates an inherent risk. In the case of Estonia it is clear that Estonia is heavily reliant on cyberspace due to internet penetration and the focus on e-governance. For instance, Estonia uses the internet to provide many government services such as voting, registration, and taxes. This allows a small state to provide services that it would otherwise not be able to, but it results in increased dependence on the internet.[45]

Despite facing certain challenges, Estonia views itself as being able to make an impact in policy relating to cyber space. In other words, a small state in cyber space has been conceptualized to have inherent limitations that are not as acute for states with larger populations, however, small state are still able to able to influence policy. In the case of Estonia, this may be due to the fact that Estonia has internationally recognized niche capabilities in cyber issues.[46] Estonia's discourse on cyber norms reflects this, by expressing that they face challenges to in creating norms, but Estonia's opinions are valued and can be influential.

---

[44] Joe Burton, "Small states and cyber security: The case of New Zealand," 223-4.
[45] Liina Areng, "Lilliputian States in Digital Affairs and Cyber Security," in *The Tallinn Papers: Numbers 1-9 (2014-2015)*, ed. Liis Vihul, (Tallinn: NATO CCD COE, 2015): 44.
[46] Henry Rõigas, "A Small State Utilizing its Niche Capability for Influence in Foreign and Security Policy: The Case of Estonia and Cyber Security" (master's thesis, University of Tart, 2015), http://dspace.ut.ee/bitstream/handle/10062/45179/roigas_henry_ma_2015.pdf?sequence= 1&isAllowed=y.

2.3 Small States and Norms

Despite the traditional definitions of small states, which see them as objects of international relation, over the last two decades scholarship has suggested that small states can be effective norm entrepreneurs. A norm entrepreneur is an actor that promotes ideas about acceptable behavior for a given identity. To do this norm entrepreneurs need a platform which are usually international institutions, like the U.N. An effective norm entrepreneur carefully promotes a norm and guides it through what Finnemore and Sikkink call the norm 'life cycle.' [47]

The norm life cycle consists of three progressive stages, "norm emergence,' 'broad acceptance,' and 'internalization.' In the first stage, norm entrepreneurs promote new ideas regarding appropriate behavior and try to convince other states to follow the norm. Broad norm acceptance is characterized when norm entrepreneurs are able to reach a significant number of followers. If enough actors or key actors agree on the norms it can cause a 'norm cascade,' or a shift in norms, which leads to this second stage where the majority agree on the appropriateness of the norm.[48] The final stage is norm internalization, where actors preform the normative behavior without having to contemplate the value of the behavior.[49]

Throughout the norm life cycle there are several factors that can effect whether a norm succeeds or not. New norms, for instance, do not arrive unchallenged. Norms are often

[47] Martha Finnemore and Kathryn Sikkink, "International Norm Dynamics and Political Change," *International Organization* 52, no. 4 (Autumn 1998).
[48] IBID; and Cass R. Sunstein, "Social Norms and Social Laws," *Columbia Law review* 96 no. 4 (May, 1996), 909. accessed September 14, 2015, http://www.jstor.org/stable/1123430
[49] Martha Finnemore and Kathryn Sikkink, "International Norm Dynamics and Political Change,"

contested and have to compete against the norms proposed actors with different views or those looking out for their own self-interest. As a result, entrepreneurs often use international organizations with similar mandates to the norms they are trying to promote.[50] Even if a norm entrepreneur picks an appropriate platform, it does not guarantee that a norm will be successful even in the emergent stage. This is because past norms shape and limit what kind of norms can be developed and adopted.[51]

This framework of norm entrepreneurs and the norm life cycle has often been used in small state literature. Most often the literature has focused on the ability of small neutral states to act as norm entrepreneurs, but there has also be one case on a small aligned state promoting cyber norms.[52] For instance, Christine Ingebristen suggest that the Scandinavian countries are able to act as 'moral superpowers' giving them increased influence on matters of conflict resolution and equality. The influence of Scandinavian countries is a result of domestic policies of social wealth fare, equality, and neutrality (Finland and Sweden) that has added credibility to their efforts in these areas. This credibility gives them access to prominent positions in international organization which they use to promote new norms that also promote peace and equality.[53] The literature however has not been able to explain why small states promote these norms that have a largely positive effect on international organizations. This is true for both neutral states and small states in general. The reason for

[50] IBID, 897-99.
[51] Laurent Goetschel, "Neutrals as Broker of Peace Building Ideas?" *Cooperation and Conflict* 46 no. 3 (2011): 319.
[52] IBID; Christine Ingebritsen, *Scandinavia in World Politics* (New York: Rowman and Littlefield, 2006).; and Collin Allan and Matthew Crandall, "Small States and Big Ideas: Estonia's Battle for Cybersecurity Norms," *Contemporary Security Policy* 36, no. 2 (July, 2015).
[53] Christine Ingebritsen, *Scandinavia in World Politics.*

this is there are both elements that can be viewed as altruistic and those that can be viewed as strategic.[54] In reality the promotion of norms by small states is probably a mixture of both.

2.4 Cyber Norms and Cultivating Norms in Cyberspace

The study of cyberspace and cyber norms is rapidly developing, but it can still be considered to be in its early stages.[55] Several recent works have attempted to apply existing IR theories to cyber norms or discussed the limitation and differences of creating norms in cyber space compared to those in other areas. However, the vast majority of the literature, in terms of cyber norms, focuses on creating legal norms (or 'binding norms') or on the efforts of large countries in the development of norms. Less work has been conducted on both small states and the private sector.

One notable work on small states and cyber norms is the work of Allan and Crandall which applies Finnemore and Sikkink's theory of norm entrepreneurs and the norm life cycle to cyber space. They argue that in terms of cyber security, Estonia acts as a norm entrepreneur promoting cyber norms. Specifically they look at the efforts of by the Estonian President Thomas Hendrik Ilves and analyze the results in NATO. The findings indicate that Estonia has successfully promoted some norms inside NATO, which have reached the

[54] IBID; and Laurent Goetschel, "Neutrals as Broker of Peace Building Ideas?"314-18.
[55] Tim Maurer, "Cyber Norms Emergence at the United Nations: An Analysis of the Activities at the UN Regarding Cyber Security?" Discussion paper #2011-11, Cambridge, Mass.: *Belfer Center for Science and International Affairs, Harvard Kennedy School* (September 2011).

emergent stage.[56] However, there are some limitations to this study. Although Allan and Crandall argue that there are norms that are currently in the emergent stage, other scholars have suggested that determining which face of the life cycle a norm is in may not be possible for norms relating to cyberspace. This is partially a result of the continuously changing nature of cyberspace. [57] There is also potentially problems with the findings based on what constitutes a norm. For instance, Erskin and Carr have argued that many of norms thought to exist in cyberspace are only 'quasi-norms,' which lack prescriptive and evaluative force, or wide acceptance in a given community.[58]

In the literature covering the private sector and its involvement with cyber norms has largely been influenced by the interest of the private sector. As a result most publications have focused on the technical side or on limiting actions that would undermine the technological integrity of their products or property.[59] Still this does not mean that these efforts are not worth noting, or that the norms they are trying to generate don't have value. After all, the products and services that private companies develop already play a role in norm development.[60]

---

[56] Collin Allan and Matthew Crandall, "Small States and Big Ideas: Estonia's Battle for Cybersecurity Norms," *Contemporary Security Policy* 36, no. 2 (July, 2015).
[57] Madeline Carr and Toni Erskine, "Beyond 'Quasi-Norms': The Challenges and Potential of Engaging with Norms in Cyberspace," in *International Cyber Norms: Legal, Policy and Industry Perspectives,* ed. Anna-Maria Osula and Henry Rõigas. (Tallinn: NATO CCD COE, 2016): 92-96.
[58] IBID, 87-90 and 100.
[59] Maria Osula and Henry Rõigas, "Introduction," 11.; and Scott Charney, "Governments and APTs: The Need for Norms"
[60] Shireen Alam and Ilias Chantzos, "Technological Integrity and The Role of Industry in Emerging Cyber Norms," in *International Cyber Norms: Legal, Policy and Industry Perspectives,* ed. Anna-Maria Osula and Henry Rõigas. (Tallinn: NATO CCD COE, 2016): 205.

Even though the main focus of the private sector is often on integrity of products and services or technical aspects there are still important insights that can be gleaned in regards to how the private sector influences norms and why they should be involved in the creation of norms. The primary reason why the private sector should have a say in norm development is, they have a tremendous stake in the outcomes do to the large amounts of infrastructure and services provided by the private sector. As mentioned earlier (and noted by Finnemore) norms must be achievable to be accepted. If the cost of compliance or the knowledge required to comply with a proposed norm is to high, it will not be accepted.[61] In other words, including the private sector helps to ensure that norms are feasible both economically and technically.

According to the literature the need for the private sector to be involved in the creation of norms is widely accepted. Alam and Chantzos have also noted five ways that the private sector already influences cyber norms. The first way is the development of new technologies and applications for their use, which results in a change to how we behave in cyberspace.[62] For instance, creating an applications that require user to use capital letters and special characters when creating passwords. Second, in an effort to provide customers with effective services and products they seek out and publicize changes in threats. Third, participation in public private partnerships (PPPs) and groups designed for capacity building, which can result in a knowledge transfer or an alignment of ideas. Fourth, by helping law enforcement agencies foil cybercrime. Finally, the private sector develops and provides states with new

[61] Martha Finnemore, "Cultivating International Cyber Norms," 92-3.
[62] Shireen Alam and Ilias Chantzos, "Technological Integrity and The Role of Industry in Emerging Cyber Norms," 205.

technologies and scalability that allows states to put regulations and public policy into effect.[63]

It is clear that the private sector has a stake in norm development and that they already shape the development of norms to a certain degree. There has been some work on how small states act as norm entrepreneurs in cyberspace and promote norms. What is missing is an analysis of how small states with limited resources frame their cooperation with the private sector. As a result one of the aims of this thesis is to suggest how a small frames cooperation with the private in the development of norms by using Estonia as an example. By using Alam and Chantzos's work it is possible to see if Estonia frames cooperation on norms in a way that promotes private sector involvement beyond its traditional level. However, due to the problems mentioned above relating to 'quasi-norms' and the difficulty of determining the stage of a norms development, this thesis avoids the classic example of norm entrepreneurs and the normative life cycle developed by Finnemore and Sikkink. Instead, it will use a framework of norm cultivation, which was developed for cyber norms.

Cyber norm cultivation was developed by Martha Finnemore and takes into account specific challenges of creating norms for cyberspace. Like the norm life cycle, cultivation is conceptualized to have 3 stages; however they vary slightly. These stages are "norm articulation and promulgation," "norm dissemination," and "norm internationalization, institutionalization, and enforcement."[64] Although the norm life cycle is a continuous process, cultivation of cyber norms stresses the continuous nature of the process.[65] This

[63] IBID, 205-210.
[64] Martha Finnemore, "Cultivating International Cyber Norms," 93.
[65] IBID, 90.

continuous nature complicates the creation of cyber norms because they must have 'clearity,' 'utility,' and 'do-ability.' In other words the proposed norm must be understandable, have a valid purpose, and be feasible to implement. To achieve this cooperation between multiple actors is required, including states and the private sector.[66]

Building on the existing literature this thesis will examine how Estonia frames the development and promotion of norms, as well as cooperation with the private sector in throughout the process. Specifically it will look at the advantages, disadvantages that Estonia faces and the perceived benefits it receives from development and promotion of norms in three policy areas: a free and open internet, e-governance, and protection of critical infrastructure. The literature on small states and norms suggests that Estonia's recognized niche capabilities in cyber issues should be framed as an advantage, while disadvantages should include issues relating to resources.

To add additional value, this thesis seeks to show how Estonia frames cooperation with the private sector in the policy areas mentioned above. Once again analysis is focused on the benefits and limitations that Estonia expresses in discourse on cooperation with the private sector. For instance, whether collaboration with the private sector is seen to help cultivate norms that are useful, feasible, and understandable. Additionally how Estonia frames cooperation with the private sector will be compared to Alam and Chantzos five ways that the private sector contributes to cyber norms. This will allow for analysis of whether or

[66] IBID, 89-93.

not Estonia's has framed cooperation with the private sector in a way that goes beyond the level of involvement that the private sector has traditionally fulfilled.

3. Methodology

The aim of this thesis is to determine how Estonian officials view their ability to develop and promote potential cyber norms in regarding three strands of foreign policy: efforts for a free and open internet, promotion of e-Government, and promoting the protection of critical infrastructure. Additionally, this thesis seeks to determine, how Estonia frames the role of the private sector in developing norms in these policy areas. Here cyber norms is used interchangeably with developing, articulated, emerging, emergent norms because the level of analysis here is on the international level. In Estonia some of these norms may be institutionalized, broadly accepted, or even an internalized part of everyday life, but in the international arena that is not the case. In other words, the norms here are seen as being contested at the international level or at the very least have not been widely disseminated.

Because very little has been written on the development of cyber norms by small states or their cooperation with the private sector in developing these cyber norms, this thesis seeks to generate a hypothesis on how small states see their ability to create cyber norms and how they view the role of the private sector in this process. The spars nature of the literature is also the reason a single case study was chosen for this study. As Todd Landman explains, single cases studies are very effective at providing 'contextual description.'[67] The use of a

[67] Todd Landman, "Single-Country Studies as Comparison" in Issues and Methods in Comparative Politics. 3rd edition. (New York: Rutledge, 2008), 86-7.

single case study here will allow for an examination of multiple policy areas and a more detailed view of cooperation between the public and private sector than would be possible with a large-N study. Additionally, because it is difficult to discern the exact level of cooperation and areas of cooperation, it is difficult to select cases that would be suitable for comparing cooperation between the private and public sector.

Estonia was selected as a single case study in an effort to illustrate both how a small state views their ability to develop and promote cyber norms, and how a small state views the role of private sector in throughout the process. The choice of Estonia offers both several advantages and disadvantages. As mentioned earlier, one distinct advantage is that Estonia is internationally recognized as being savvy at cyber issues. This likely helps Estonian decision makers to maintain the 'ideational commitment' that Finnemore and Sikkink suggest is often a hallmark of norm entrepreneurs.[68] Another benefit from the selection of Estonia is that Estonia is involved in many initiatives relating to cyber norms. These include taking part in the GGE and NATO as mentioned earlier, but also efforts such as cyber hygiene in the EU or promoting e-governance through various vectors. Finally, Estonia's work with the private sector on domestic level cyber issues suggests that that cooperation could extend to international initiatives as well.

Although using Estonia as a case study offers several clear advantage, there are also several limitations. First, Estonia's success in carving out a 'cyber niche' means that it is

[68] Martha Finnemore and Kathryn Sikkink, "International Norm Dynamics and Political Change," *International Organization* 52, no. 4 (Autumn 1998).

likely not representative of the typical small state. As a result, some or many of the conclusions may not apply to other small states. However, there is still likely to be some overlap caused by the similar limitations that small states face (such as limited resources). Second, the conclusions for this case study will without a doubt not be applicable to many larger states. Still, some of the descriptions and conclusion may prove useful for comparison in future cases. The final limitation is that due to the large and diverse areas that Estonian cyber policy covers. Because of this, a comprehensive coverage of norm building and cooperation between the private and public sectors is not possible. Taking this case studies limitations into consideration, there remains a significant value to understanding how Estonia frames the development and promotion of cyber norms and how cooperation with the private sector in initiatives is framed.

This thesis seeks to provide insight into how Estonia views its role in the development and promotion of cyber norms and the relationship between the public and private sector in the creation of cyber norms by answering several questions. What role does Estonia have in the creation and promotion of cyber norms? This question is the primary focus of the thesis and is expanded by several sub questions:

- What advantages or disadvantages do officials feel they face as a result of being a small state?
- What benefits does Estonia receive from the promotion of cyber norms?
- In what capacity has there been collaboration with the private sector and how is the cooperation viewed?

- Has Estonia's framed cooperation with the private sector in a way that extends the private sectors involvement beyond what can be viewed as normal?

By answering these questions it is possible to get a general understanding of how a small state views its ability to create and promote cyber norms, as well as to determine how cooperation with the public sector is viewed by officials.

Semi-structured interviews were used in an effort to answer these questions. These interviews were conducted with Estonian officials involved in issues relating to cyber space and were conducted in the spring and summer of 2016. The use of semi-structured interviews was chosen because of the ability to ask follow up questions. Follow up questions were then used in order to clarify information or explore previously unknown information.[69] Because Estonia is involved in many initiatives relating to cyber space, interviews were conducted with personnel from multiple government agencies. Originally, the research plan was to conduct interviews with officials from the Ministry of Defense (MoD), the Ministry of Foreign Affairs (MFA), the State Information System Authority (RIA), and the Ministry of Economic Affairs and Communications (MEAC). In total 5 interviews were conducted with current or past employees of the MFA (1 official), the e-governance Academy of EGA (1 official), RIA (1 official), and two policy experts. No interviews were conducted with the Ministry of Defense.

Although interviews with officials from the MoD would have potential been beneficial, specifically because they could provide a more security focused viewpoint than

[69] Peter Burnham, et al., "Elite Interviewing" in *Research Methods in Politics* (New York: Palgrave, 2008), 213.

the other agencies. However, there proved to be reluctance among MoD officials to conduct interviews, even when the author was referred by colleagues in other agencies. This was likely a result of the nature of the topics that were selected and researched. Both the topic of e-governance and internet freedom are not known to be in the wheelhouse of agencies with a military or defense focus. Because of that fact the only remaining topic that officials might have been able to contribute to was the protection of critical infrastructure. Although, most of the questions were not dealing with what would normally be considered called sensitive issues, this may still have been seen as problematic due to the potentially sensitive nature of the topic. For instance, if officials viewed that the amount of cooperation between the MoD and the private sector to be too sensitive to discuss, it would explain the reluctance of officials to conduct interviews on the subject. Despite the reluctance of officials from the MoD, other agencies proved to be quite open to interviews.

To protect the interviewees' right to anonymity their responses have been anonymized. Each individuals name has been replaced by a code, which is made up of an abbreviation and number. The letters correspond to the interviewee's respective organization so that the letter "PE" represents the policy experts, "EGA" for the e-Governance Academy "F" for the Ministry of Foreign Affairs, and "RIA" for the State Information System Authority. Additionally, a note was made to whether or not the interviewee had previously worked in the private sector. This was only recorded to determine if variations in answer could be related to past work experience. After analysis, there was determined to be no significant difference between the officials that had private sector

experience and those that did not. Both groups were quite supportive of working with the private sector.

Each of the interviews was structured along a predetermined guideline. Prior to the interview all interviewees received a plan language statement, which informed them of the aims of the research and their rights as an interviewee. Each interviewee also received the research questions and a list of themes before the interview. During the interview questions were asked from a standard list of questions that can be found in the appendix. However, due to the differing nature of each agency's respective mission, the questions varied depending on the policy areas that the agency focused. Whenever possible, the interviewees were recorded on a voice recorder in order to ensure a higher level of accuracy in the transcription process. The audio recordings were then transcribed and then patterns in the data were then identified and analyzed using simple discourse analysis.

Discourse analysis modeled off of Henrik Larsen's foreign policy discourse analysis was chosen because allows it for the analysis of how public officials frame the political agenda. The framework created by the discourse by public officials creates both opportunities and restriction on policy.[70] This means that the dominate discourse expressed by public officials in Estonia should provide insight into the challenges and opportunities that Estonia faces when developing and promoting cyber norms. It should also show how these challenges and opportunities relate to cooperation with the private sector.

[70] Henrik Larsen, *Foreign Policy and Discourse Analysis: France, Britain and* Europe (New York: Routledge, 1997), 23; and Peter Burnham, et al., "Discourse Analysis" in *Research Methods in Politics* (New York: Palgrave, 2008), 248.

In this thesis it is assumed that public officials will express the dominate discourse in their interviews, because the language has been internalized. There may still be other discourses present amongst public officials, but the dominate discourse is the one that is most pervasive among the government.[71] Therefore, when the words "Estonia" and "Estonian" are used to describe the views and opinions of public officials, it does not mean that there are no other competing discourses. To ensure the dominate discourse was analyzed, all answers were corroborated by at least one other interviewee, when it was possible. This was done by looking for common themes or wording in the interview transcripts, while also looking for themes that contradicted one another. Additionally triangulation was also strived for by using written sources as support.

One key, but unavoidable, weakness stands out in the research design. Although one of the aims of this thesis is to explore the how the public and private sector cooperate to cultivate cyber norms, interviews with officials representing the private sector actors were not conducted. There are several reasons for this decision. First, the private sector is very large and finding a representative sample of the group would prove unfeasible. Second, the involvement of the private sector actors is not immediately apparent. Meaning that some ground work needs to be done on which actors are involved and in what areas. Third, as mentioned earlier the dominate discourse is argued to be the one that is most pervasive in the government (or public sector). Finally, some of interviewees have previously worked in the private sector, and as a result, their opinions likely informed by their past experience. In

[71] Henrik Larsen, 26 and 31.

other words, those that know the abilities and limitations of the private sector are likely to express those opinions.

4. Estonia and Perceptions on Cyber Norms

This section details the general views of Estonian officials relating cyber norms. In 2007, Estonia came under a coordinated and sustained cyber attack that lasted for days. The attack hit government websites, media outlets, and banks.[72] The Estonian government was rather open about the attack and provided information regarding the attacks to the public and the international community.[73] Although the attacks were not particularly devastating they had a significant impact.

Cyber security and related topics became much more pressing both for Estonia, but also for other countries as well. One reason for this was the attacks showed that certain services that the general public depend on for information and day to day life could be threatened by cyber attacks. It probably also had the effect of making 'cyber savvy' the most defining attribute that Estonia is known for. Since the attack, Estonia has become a prominent part of the debate on issues relating to cyber security. For instance, the current President Thomas Hendrik Ilves has provided numerous speech on the on cyber space, security, and related issues.[74] In addition, Estonia has been a part of the United Nations Group of Governmental experts on Cyber Security (UN GGE) from the second GGE through the fourth GGE. It is also important to note that the GGE has never had more than 20 participating countries selected to participate its meetings. [75] This means that Estonia is one of the few

[72] Piret Pernik and Emmet Tuohy, "Cyberspace in Estonia: Great Security, Greater Challenges," International Center for Defence Studies (August, 2013): (Pages), accessed November 29, 2015, http://www.riso.ee/et/koosvoime/raamistik, 2.
[73] State Information System Authority Official, interviewed by author, Tallinn, July 7, 2016.
[74] Collin Allan and Matthew Crandall, "Small States and Big Ideas: Estonia's Battle for Cybersecurity Norms,"
[75] Marina Kaljurand, "United Nations Group of Governmental Experts: The Estonian Perspective," in International Cyber Norms: Legal, Policy and Industry Perspectives, ed. Anna-Maria Osula and Henry Rõigas. (Tallinn: NATO CCD COE, 2016): 111-27.

countries that is able to provide direct input at the GGE. This is a significant accomplishment for a small state and speaks very highly of their perceived abilities in fields relating to cyber.

So it is clear that Estonia has had been in a position to potentially have an impact on the discussion relating to cyber norms, but what is unclear is how Estonian discourse perceives Estonia's ability to actually promote their initiatives and affect change. Below the perceived capacities of Estonia have been analyzed form the discourse in order to answer a couple of important question. Does Estonia view cyber norms as being necessary for the international system to function properly? Do Estonian officials conceive Estonia as being able to create and/or promote cyber norms through foreign policy?

The question, "Does Estonia view cyber norms as being necessary for the international system to function properly?" may seem like a self-evident question, and in a way it is. What is not self-evident though is how Estonia portrays and justifies the answer to this question in the official discourse. Indeed ever interviewee answered in the affirmative when asked if, Estonia viewed cyber norms as being necessary for the international system to function properly. The prevailing reason proposed by most of the officials was that cyber norms create mutual understanding and clarity. For instance the official from the MFA stated, "The main goal is to create predictability. International norms have been important to the international system for a long time."[76] In other words for Estonia, the cyber norms are not seen as something completely new, they are a way of bringing clarity and predictability to a new domain that is currently lacking those features.

As mentioned before all of the interviewees expressed that norms are important for predictability or clarity; however, there was some debate on why the predictability and clarity are important. For instance, PE2 eluded to the fact that cyber norms are particularly important to insure a small state's survival, saying, "…any international norms, regulations, or order are essential to small states in order to survive. That is the basic theoretical background I guess. So it is only natural that the small states such as Estonia, which is dependent on the actions of bigger states."[77] Although, this is a logical argument and fits with the

[76] Ministry of Foreign Affairs Official, interviewed by the author, Tallinn, July 4, 2016.
[77] Policy Expert Two, interviewed by the author, Tallinn, June 28, 2016.

institutionalist literature on small states, other officials took a slightly different view. The official from the EGA explained, "…I think that every country would probably benefit if there are clear norms regarding cyber space and cyber security…"[78] This was somewhat echoed by the RIA representative who mentioned that in the EU norms are important for creating mutual understanding among its member states.[79] In other words, the dominate discourse reflected among Estonian officials is that cyber norms are important to international order, because they create predictability and mutual understanding for the members of groups, which benefits everyone. In this case the discourse on the promotion of norms is framed in a way that is closer to the thinking of constructivist, which focus on the promotion of norms as a reflection of identity.

The idea that a small state can create and promote norms is not a new idea, as mentioned above the Nordic countries have been successful at promoting norms related to social welfare and neutral countries have succeeded at promoting peacebuilding norms. By looking at speeches and foreign policy outcomes, Crandall and Allen determined that at least in the early phase of a cyber norms lifecycle Estonia is also able to be successful. This does not mean that Estonian discourse is framed in a way that reflects this finding. So does Estonian discourse show that they can influence cyber norms in a similar way? When it comes to promoting norms all the interviewees believed that Estonia is able to promote norms that it finds favorable and see them into the initial part of the dissemination phase. For instance two officials pointed to actual EU regulations, which although they were not created by Estonia, were heavily promoted by Estonia and ultimately passed. The first being the Eelectronic Identification and Authentication Services Regulation (e-IDAS), which "Estonia has worked quite a lot to push through, and that is something that changes the way we do things in the internet environment. It changes it very practically and these are exactly the things that will shape the future of cyber space."[80] Another example was given was Estonia's support for the EU's NIS Directive, which helps to ensure higher standards of information security throughout the entire EU. A representative stressed, "…if you take the European

[78] E-Governance Academy Official, interviewed by the Author, Tallinn, June 28, 2016.
[79] State Information System Authority Official, interviewed by author, Tallinn, July 7, 2016.
[80] E-Governance Academy Official, interviewed by the Author, Tallinn, June 28, 2016.

NIS directive there are a number of elements were Estonia played quite a prominent role and luckily for us we had other countries who were thinking in the same manor so we were not alone."[81] In this respect Estonia is seen as able to influence and help promote norms, but not the sole creator of the norms. Estonia's ability to promote these norms and others was largely portrayed as a result of Estonia's positive image of being a cyber savvy country.

One of the reasons that Estonia is seen as a cyber savvy country is a result of Estonia being seen as a great place to test innovative electronic solutions. For instance, in all of the interviews conducted (and in a few more than once) the idea of Estonia being 'a good test pit' for solutions was mentioned. Because Estonia is a good test pit for ideas, the majority of the respondents, also pointed to the idea that Estonia can share its experiences of what works and doesn't work with others. An example of this was expressed by EGA, "What Estonia can do is to show to the world what can work in practice…. Estonia can show the world that for example the digital identity really works, and Estonia can show how it shapes the society."[82] Somewhat paradoxically, despite having a view that Estonia was a great place to test new ideas and share their experiences, only one official directly stated that Estonia was able to potentially create cyber norms.[83]

The rest of the interviewees were rather skeptical of this idea eluding to the idea that it is theoretically possible, but unlikely. Policy expert two provided a good example of explaining that topics are becoming more specific, which is a problem due to Estonia's limited amount of both personnel and financial resources. He did however, concede that the cyber norm discussion is more of an intellectual discussion, and may not require as many resources.[84] As a result the primary view of Estonian officials is that Estonia is good place to test ideas and that they can share their experience, but to date there is no real proof that Estonia can create its cyber norms on their own.

As mentioned by policy expert two, recourses are a factor when it comes to Estonia's ability to promote norms. This factor was also echoed by all of the other interviewees. A

[81] State Information System Authority Official, interviewed by author, Tallinn, July 7, 2016.
[82] E-Governance Academy Official, interviewed by the Author, Tallinn, June 28, 2016.
[83] Ministry of Foreign Affairs Official, interviewed by the author, Tallinn, July 4, 2016.
[84] Policy Expert Two, interviewed by the author, Tallinn, June 28, 2016.

typical example of the resource limitations that Estonia faces was offered by the representative from the MFA. He explained that, "Our MFA has around 500 people and only a small amount work on a given issue, whereas larger countries like the U.S. have around 50,000 people working in the State Department."[85] This leaves only a few officials for a given topic, and as also requires that Estonia has to pick or prioritize the topics they focus on.[86] An additional problem that was brought up by both policy expert one and the official from RIA, is personnel changes have a huge impact because of the limited number of officials working on a topic. Meaning that losing one very effective member of a two or three person team has a huge effect.[87] This is made worse by the fact that Estonian officials do not conduct right seat left seat rides, or in other words they don't have a transition period were incoming officials can learn about their new position from the outgoing official. Policy expert one mentioned that "…from personal experience it is really a clean slate after an official leaves."[88] On the one hand, this without a doubt contributes to the problems created by having limited resources. While on the other hand, this may be an unfortunate, but unavoidable consequence of being a small state with limited resources. Meaning that a small state may not always be able to spare the financial, personnel, or time resources required to facilitate a training up period. There are ways that Estonia is able to limit the effect of limited resources tough. For instance, by ensuring that all of the officials at the MFA are able to speak on cyber issues at a level that they can answer general questions when needed.[89] This has likely helped advance the image that Estonia is a tech savvy country, and it probably has helped to offset some of the disadvantage that is suffered as a result of having limited personnel to begin with. The reason for this is that if foreign officials always find Estonian personnel to be knowledgeable about cyber issues, it is like to increase the image of be cyber save and to potentially increase Estonia's influence.

The idea that Estonia has to focus its attention and efforts on areas, which Estonia conceives as priorities is an important statement. It illuminates one of the key limitations of

[85] Ministry of Foreign Affairs Official, interviewed by the author, Tallinn, July 4, 2016.
[86] Policy Expert Two, interviewed by the author, Tallinn, June 28, 2016.
[87] State Information System Authority Official, interviewed by author, Tallinn, July 7, 2016.
[88] Policy Expert One, interviewed by the author, Tallinn, June 27, 2016.
[89] Ministry of Foreign Affairs Official, interviewed by the author, Tallinn, July 4, 2016.

small states, which as mentioned earlier has been argued to limit a small states ability to compete in cyber issues. This would appear to add more credence to the Burton's hypothesis on small states having problems keeping up in cyber space. Specifically, the dominate discourse suggests that limited resources of small states such as personnel and financial resources requires Estonia (and most likely other small states) to prioritize resources to the promotion of norms that are deemed the most important. This thesis takes the position that three of these focus or priority areas that Estonia has chosen are the protection of critical infrastructure, e-governance, and a free and open internet. The analysis of these areas is the focus of the remaining chapters.

5. Cyber Norms Relating to Critical Infrastructure

Estonia has been actively promoting and supporting norms that protect a state's critical infrastructure from cyber attacks in various international organizations (IOs) including the UN and NATO.[90] This probably, at least partly, started out as a result of the 2007 cyber attacks, which happened in Estonia, if the attacks do not remain a justification for the continued promotion. One important thing to note is that when Estonia promotes and talks about critical infrastructure, there are distinct types of critical infrastructure. First, there is critical services, which can be thought of as water, power, financial services, etc... Second, is critical information infrastructure protection or (CIIP). CIIP deals with protecting the information that is important for the functioning of governments and services. This could be information that is private or public, such as addresses, which are recorded by the Estonian Population Register.[91] However, drawing a clear line between the two is almost impossible because some of the process that are classified as being under information protection occur on physical hardware. Distinguishing between the two would have required more space than

[90] Marina Kaljurand, "United Nations Group of Governmental Experts: The Estonian Perspective," 116-19.; and Marina Kaljurand, "Estonian Experience at the UN GGE," (speech given at the NATO Convention on Cyber Conflict, May 26, 2015), available at https://ccdcoe.org/cycon/2015/app.html.
[91] E-Governance Academy Official, interviewed by the Author, Tallinn, June 28, 2016.

was available for this paper.[92] For that reason, critical infrastructure has been conceptualized as a generic category comprising both critical service protection and CIIP.

To determine how the promotion of norms relating to the protection of critical infrastructure is portrayed in Estonian discourse, several questions were explored. First, how does Estonia portray norms relating to the protection of critical infrastructure? Second, how is Estonia's efforts viewed by other actors? Third, Has Estonia received benefits or faced any limitations when promoting critical infrastructure? Final, what are the Estonian views on cooperation with the private sector?

It is clear that Estonia views the protection of critical infrastructure as a priority. When asked why Estonia views the protection of critical infrastructure to be so important, all the officials indicated that it is an important topic for everyone. This answer is not surprising after all it is critical infrastructure. Still, there were two additional reasons given by the majority of the respondents. First, all five of the interviewees made references to the 2007 cyber attacks in Estonia, and how it showed the need for norms protecting critical infrastructure. One official put it this way, "I think a big player for us has been the incidents of 2007 and there was a very clear decision by the government not to sugar coat the situation, to say yes we were under coordinated activity, somebody was targeting us, not by random or by coincidence…"[93] Most of the references to the 2007 cyber attack also shared another feature in their discourse, which was the attacks showed Estonia was vulnerable. This vulnerability leads to the other dominate explanation of why the protection of critical infrastructure is so important to Estonia, which is their dependence on ICTs. Policy expert two explained the importance of these norms as such, "Estonia is very dependent on digital services and naturally on the technical level it is important that critical infrastructure wouldn't be attacked. For us especially, because we are so dependent on this technology."[94] In other words besides being an important topic for everyone the discourse shows that there is an

[92] State Information System Authority Official, interviewed by author, Tallinn, July 7, 2016.
[93] IBID.
[94] Policy Expert Two, interviewed by the author, Tallinn, June 28, 2016.

added since of urgency due to Estonia being vulnerable as a result of their dependence on the internet, and their past experience of having been the target of a sophisticated attack.

How other actors view the cyber norms that Estonia promotes is important, because although everyone may agree that protecting critical infrastructure is important, they may not agree with Estonia's onions. However, all of the official explained that Estonia's views are heard without issues. On reason for this may be the influence of the cyber attacks that occurred in 2007. Indeed, all of the officials noted that, the cyber attacks increased Estonia's influence when promoting norms that protect critical infrastructure. An example of this was expressed by the official from the EGA, "Yes, and if you ask did these attacks increase Estonia's influence in norms relating to the protection of critical infrastructure, then of course, that is pretty much all of what we talk about."[95] Part of increased influence may also be due to misconceptions regarding the actual events of the attack. For instance, policy expert two explained that people outside of Estonia don't always have an accurate understanding of what happened. To illustrate this fact he provided an example:

> "[The attacks]…didn't have anything to do with the critical infrastructure, but there is a misconception so it doesn't matter because people think the attacks were very substantial. I remember, somebody asked me in Brussels: "What did you do when you didn't have internet for two weeks?" I was like, I didn't even know we were without internet. So there is this gap and Estonia has benefited from it definitely."[96]

Whether Estonia's increased influence in cyber norms that relate to the protection of critical infrastructure is a product of misconceptions or not is difficult to measure and beyond the scope of this thesis. What is clear is that Estonian discourse reflects that the 2007 attacks had a positive impact on their ability to promote cyber norms in this area.

In terms of benefits, all of the interviewees agreed there were benefits that Estonia receives from promoting cyber norms that protect critical infrastructure. When it comes to what the benefits are there was less consensus. Still four of the five agreed that cyber norms around critical infrastructure reduce the risk of incidents and that they can be seen as

[95] E-Governance Academy Official, interviewed by the Author, Tallinn, June 28, 2016.
[96] Policy Expert Two, interviewed by the author, Tallinn, June 28, 2016.

preventative. For example, the RIA official stated, "I think the benefit has been form the point of view that you have been clear on your level of expectations. That you are rather transparent in what you are saying and why you are saying what you are expecting. So you wouldn't be reactive you would be preventive so you actually articulate what you expect them to do even when nothing has happened yet."[97] In other words, by adding clarity and explaining expectations, cyber norms reduce the risk of incidents." The MFA representative elaborated why Estonia views it as important to prevent cyber incidents relating to the critical infrastructure by saying, "What we believe is this should be something that everyone wants to avoid, which are things that could cause great suffering."[98] As a result Estonia sees the main benefit of promoting cyber norms relating to the protection of critical infrastructure as reducing the risk of incidents that would have widespread negative effects on people.

Although Estonia is able to receive certain benefits from promoting cyber norms that protect critical infrastructure, Estonia still faces challenges. The most visible challenge that arose from the interviews relate to Estonia being a small state. The official from the EGA described the limitations that a small state faces best by explaining:

> "Estonia is a small country and that is logical that internationally we don't have such a big diplomatic capacity. We don't have our embassies in every country. We can't afford to have a cyber officer in our embassies and etc., etc. We cannot take lead in different international formats just because we lack personnel and etc. So it is just logical thinking that if a country is small then it cannot influence international politics too much."[99]

These problems that Estonia faces as a small state were seen to create an additional limitation by the representative from RIA, "That might be that if you say something works is it believable. I think there is a difference when say the Netherlands says it works or if the U.S. says it works, then it has a bit different visibility or weight then when we say different solutions work."[100] It can therefore be said that Estonia's discourse relating to limitations

[97] State Information System Authority Official, interviewed by author, Tallinn, July 7, 2016.
[98] Ministry of Foreign Affairs Official, interviewed by the author, Tallinn, July 4, 2016.
[99] E-Governance Academy Official, interviewed by the Author, Tallinn, June 28, 2016.
[100] State Information System Authority Official, interviewed by author, Tallinn, July 7, 2016.

views the idea of being a small state as a factor that limits their ability to get their ideas heard and when they are heard they may be ridden off do to preconceptions about small states.

With the increased influence that Estonia has in relation to the promotion of critical infrastructure it is not difficult to imagine that Estonia might try to work cooperate with the private sector in this area. However, it is important to understand whether or not Estonia views cooperation with the private sector as important in this area. In every interview the interviewees all agreed that cooperation with the private sector was extremely important. The main reason for this was stated as being that the private sector owns most of the critical infrastructure. For instance when asked if it is necessary to cooperate with the private sector, policy expert one said, "Yes, the states should take the lead, but there must be cooperation because of the ownership of critical infrastructure." This position was echoed very similarly by the rest of the officials.

Estonian discourse paints cooperation with the private sector as a necessary factor for the development and promotion of norms protecting critical infrastructure. It is therefore, logical to assume that cooperation has occurred and that the discourse of officials will highlight the areas that Estonia views as the most critical for cooperation. When asked about where cooperation had occurred, the most propionate example was within public policy. An example was given by policy expert one, which stated that, "The private sector also helped create the cyber security strategy."[101] In addition to their help in drafting Estonia's cyber security strategy, they have also helped with the drafting of legislation. The reason why the private sector has been brought into the process of drafting relevant legislation was described by the EGA representative as follows, "In Estonia we have organized it this way that we include private sector in this legislature development process, because at least in Estonia most of the critical information system operators are outside of the government sector. So they need to protect their systems, but they cannot make the rules. Government has to do that, but they have to do it together with the private sector."[102] In this case Estonia see's it necessary to cooperate with the private sector because they are the owners of the systems, but unable

[101] Policy Expert One, interviewed by the author, Tallinn, June 27, 2016.
[102] E-Governance Academy Official, interviewed by the Author, Tallinn, June 28, 2016.

to make the regulations that the state can. As a result, they are facilitating the protection of critical infrastructure, but there is an additional aspect that Estonia views as important.

One of the benefits that has occurred from cooperating with the private sector is that it increases feasibility. As mentioned earlier, this is considered to be one of the benefits of working with the private sector is that it increases feasibility of norms. Additionally, as Martha Finnemore mentions, feasibility is also important part of norm articulation and promulgation.[103] This feasibility is considered to be very important by Estonia and shows up in the discourses of the majority of the officials. For instance, the EGA representative noted, "[the private sector has to be included]…Otherwise it is going to be either too tight [the regulations] or it is to lose. So there has to be an appropriate balance between security and feasibility. So what they can do, and how they can protect the systems. I would say it is impossible to do it without the private sector."[104] The underlying assumption here is that the government does not understand the sectors well enough to create legislation that balances security with the abilities of the company to comply with the regulation. The official from RIA stated something very similar, but furthered the importance by adding that cooperation helps the private sector with execution. He explained:

> "Plus I think there is also this culture of execution, if they wouldn't understand what we are writing and why we are writing then the execution would be a bit challenged, because they wouldn't understand why we do it, or what was the ultimate meaning of that regulation, what is the goal we are trying to reach and then it might be tricky from the point of executing and acting in accordance with the intent of the legislature."[105]

In other words, not only does Estonia view public and private sector cooperation as important for creating feasibility, it is also important for helping the private sector to comply with regulations that they are trying to make norms.

It is rather easy to overlook the international connect here, since the cooperation on public policy does not appear to have an international element to it. However, a good portion

[103] Martha Finnemore, "Cultivating International Cyber Norms," 92-3.
[104] E-Governance Academy Official, interviewed by the Author, Tallinn, June 28, 2016.
[105] State Information System Authority Official, interviewed by author, Tallinn, July 7, 2016.

of Estonia's critical infrastructure is owned by foreign multinational corporations. For instance, the banks and telecommunication companies are owned by companies from the Nordic countries.[106] This gives the cooperation on public policy a regional aspect and creates a situation where the norms have a great chance to spread. Specifically, the norms that these multinational countries must follow inside Estonia, they may export to other countries where these countries operate. This would make financial sense, in terms of having only one security or protection standard, and is rather logical sense the companies helped to formulate the standards.

In addition to the cooperation that has occurred on public policy multiple officials mentioned cooperation relation to international exercises, specifically the NATO exercise "Locked Shields." According to policy expert one, the Estonian Defense Leagues Cyber Defense League participates in this exercise. The important part being the Cyber Defense League contains members of the private sector.[107] Not only do members of the private sector participate in the exercises they appear to really be interested and enjoy the exercises. The RIA representative explained why the exercises are so appealing to members of the private sector as follows:

> "When you do the cyber security exercises you sooner or later need these companies in the private sector to be involved. My experience is they like to be involved. They are learning and we are learning. It is very interesting for them, because that is the trick in Estonia that working for private sector you get much more money, but it is much more boring. In the public sector you get less money, but it is much more interesting."[108]

In other words, the cooperation between the public and private sector is portrayed as a good learning experience for both sectors. So it builds capacity, but it also portrayed as more than that.

---

[106] IBID.
[107] Policy Expert One, interviewed by the author, Tallinn, June 27, 2016.
[108] State Information System Authority Official, interviewed by author, Tallinn, July 7, 2016.

Although the private sector offers higher pay, the exercises that the Estonian government allows them to join offers excitement that they cannot get from their normal nine to five jobs. The RIA official also gave an example that highlights this effect very well. He stated:

> "So you train them, they get involved and they really want to be involved. So this is pretty much linked to bring the bondage and bring the learning curve – actually my own colleague was here and he said to me, "I really want to be part of Locked Shields again this year." I said okay let's see. Then he emphasized, "If I cannot go during my work hours, I will apply for the vacation and go anyway." So that is the motivation of these guys and that is why we are emphasizing these exercises."[109]

Estonia's involvement of the private sector into exercises is therefore not just portrayed as a way to build capacity, it is seen as a way to encourage further cooperation with the private sector, because it creates an environment where the private sector wants to be active and wants to participate.

Estonian discourse on the protection of critical infrastructure offers some important insights into the reasons why Estonia places so much emphasis on the promotion of norms protecting critical infrastructure. Besides being an important topic in general, the protection of critical infrastructure has increased an importance for Estonia due to the cyber attacks of 2007 and their dependence on internet and telecommunication technologies.

In addition to the importance of this topic Estonian discourse provides valuable insights into the benefits and limitations that Estonia faces when promoting norms in this area. For instance, the most important benefit according to discourse is the fact that cyber norms protecting critical infrastructure are preventative and reduce the risk of cyber incidents in these areas. While the limitations tend to arise from the typical issues facing small states. The limited resources that Estonia is able to muster creates problems for Estonia when they try to promote the protection of critical infrastructure. Not only do the limited resources

[109] State Information System Authority Official, interviewed by author, Tallinn, July 7, 2016.

affect their ability to promote norms, it is conceived that sometimes perceptions on what is believable from a small state can also effect Estonia's ability to promote norms.

Despite these limitations Estonia has been fairly successful in cooperating with the private sector. It is clear from the discourse that Estonia believes it is necessary for there to be public and private sector cooperation in order to successfully create and promote cyber norms that protect critical infrastructure. They also conceive of it being important to include the private sector in order to create feasible norms in public policy. In addition to the feasibility that cooperation offers, Estonia considers it very important to integrate the private sector into exercises including NATO ones. This helps to build the capacity, which as mentioned earlier, is one of the five ways that the private sector already contributes to the development of norms. However, Estonia appears to take this further. Estonia frames their capacity building with the private sector as a very successful form of capacity building. This is because the exercises are conceived as something that is appealing to the private sector and also increases their willingness to participate in the future and for this reason it is not just about capacity building. It is about creating an environment where the public and private sector want to cooperate with each other. So although it does not expand the role of the private sector, it is framed as having perfected what was already there.

6. Internet Governance as a Norm

Estonia has been providing e-services (such as e-taxes, e-customs, and e-school) to its citizens for well over a decade. It has also been active in sharing their success with these services to other countries and their citizens.[110] This includes promotion of X-Road (Estonia's secure data exchange system that provides the foundation for e-services.), the creation and support for the e-Governance Academy, and the newly launched e-Residency program. Perhaps two of the best examples of sharing, which could possibly even be considered as promotion, are speeches by President Ilves regarding the benefits of e-governance and e-services, and the e-Estonia Showroom in Tallinn, Estonia. Both have brought attention to the benefits of e-governance and e-services. This attention that has been

[110] e-Estonia, "The Future is Now," Promotional publication (n.p.: n.d.) also see https://e-estonia.com/

brought to e-governance, by Estonia, has not gone unnoticed by other countries and even their citizens, but can this be considered a cyber norm. If it is a norm then it raises an important question. How does Estonia portray the promotion of e-governance in official discourse?

Although most talk relating to cyber norms has focused on legal, security, or technical norms, this does not mean that e-governance cannot be considered a norm. Norms as mentioned earlier are the expected behaviors for a given identity. A group of countries believing that their governments should provide e-services to their citizens would also fit this definition. This increasingly appears to be the case. Through the EGA many states have been willingly receiving help to create e-services, many of which are Eastern Partnership Countries.[111] Additionally, Estonia has given their X-road platform to Finland and they are currently in the early process of connecting the two countries, which could eventually allow for secure cross border data exchange and services.[112] Finland, also is not the only EU country interested in X-road and providing cross border services. Sweden has shown interest as well and there has been preliminary discussion, about a three way connection between Estonia, Finland, and Sweden.[113] It appears at least in the EU and in countries aspiring to join the EU that e-governance is becoming more of an expected behavior and norm, but as will be shown below, interest extends outside the EU. This matches with what Martha Finnemore described as the first stage of a cyber norm promulgation, but could maybe be argued is in the early phase of dissemination.[114]

Some scholars would doubtless argue that even if e-governance is a norm, it is not worth the discussing. Although this norm may not be as hot of a topic as cyber security norms are, it is worth looking into because of the potential benefits e-governance offers. The

---

[111] E-Governance Academy, "Projects," Last Accessed July 9, 2016, http://ega.ee/projects/.
[112] Personal correspondence with an Official from the Estonian State Information System Authority, May 25, 2016.
[113] The Baltic Course, "Sweden Interested in Estonia's X-Road Platform," Last Modified December 18, 2015, http://www.baltic-course.com/eng/good_for_business/?doc=114572.
[114] Martha Finnemore, "Cultivating International Cyber Norms," in America's Cyber Future: Security and Prosperity in the Information age, ed. Kristin M. Lord and Travis Sharp (Washington, D.C.: Center for a New American Security, 2011), (93-96), https://www.cnas.org/files/documents/publications/CNAS_Cyber_Volume%2011_2.pdf.

ability of citizens to access their government's services digitally from anywhere in the world would positively affect millions of people daily. A security norm may prevent conflict, which also can be seen as a positive effect on people, but it is difficult to argue that it positively affects people on a daily basis, especially taking into account the high amount of cyber attacks that happen regardless of security norms.

Because of the growing use and interest of countries in e-governance, there are naturally interesting questions that relate to how Estonia views the promotion of e-governance in official discourse. In this section those questions have been analyzed to provide a preliminary insight, into the official Estonian discourse on e-governance. Specifically, it has sought to answer the following questions. How is e-governance promoted in official Estonian discourse? Do Estonian officials feel that their efforts are well received by other actors? What are the perceived benefits and/or limitations that Estonia experiences from promoting e-governance? How has cooperation with the private sector worked in relation to the promotion of e-governance?

From the chapter introduction it should be fairly clear that Estonia views e-governance as an important part of foreign policy, and this fact is confirmed in the analysis of Estonian discourse. The officials that were interviewed made it very clear that e-governance is an important part of Estonia's foreign policy for instance, the EGA official naturally summarized why this is the case:

> "I think it is, but it is kind of natural that this topic is part of the foreign policy because we have – I think Estonia is a very good example of a functioning information society. We have … 99% of our government services are online… So it is logical that we talk about that a lot. That is why our President [Ilves] has taken this topic up and he likes to speak about e-governance and cyber security. Logically our different ministries and different ministers are talking about that. Our organization here is established because of that. So we take this knowledge to other countries as well and speak about that. So yes it is a very important part, but is because we have really something to talk about."[115]

[115] E-Governance Academy Official, interviewed by the Author, Tallinn, June 28, 2016.

In other words for Estonia to talk about e-governance is natural, because for them it represents a huge success story and the can claim to be a functioning information society which is perhaps the only one.

Due to Estonia's enthusiasm for e-governance and the fact that the president and various ministries are all talking about e-governance, it would be logical to expect that Estonian discourse portrays e-governance as a new norm that needs to be promoted, but that is simply not the case, at least not outside the context of the EU. How then is the promotion of e-governance portrayed? As an official with the MFA puts it, "With e-governance I think what we can do is explain our experience and the benefits that we have had. Maybe the aim is not to have some international norm, because nobody can dictate how a government should be developed."[116] Again this is a somewhat surprising finding, but it was echoed by others as well including the EGA official who stated, "We talk just about what we have implemented in Estonia about these things that really work in practice."[117] While the official from RIA said,

> "[When speaking about non-EU member states]… I think it has been we are happy to share, but we are not pushing. We have a lot of those international delegations coming whether they are from Africa or Asia, they are coming over here. We are happy to share with them what they have to do, which is okay this is what you can promote. We are happy to be open. If you feel it is good for you than just use it, because our own history is about learning from others. "[118]

In the context of the EU; however, the official from RIA believed that e-governance is more actively promoted as a result of a desire to decrease borders to businesses. In the context of non-member states of the EU, Estonian discourse suggests that e-governance is not promoted but shared out of altruism. Still is worth noting that the amount of attention that is given to e-governance is very high. As mentioned earlier, there is a showroom as well as a website dedicated to e-Estonia. This combined with the large amount of attention given to e-

[116] Ministry of Foreign Affairs Official, interviewed by the author, Tallinn, July 4, 2016.
[117] E-Governance Academy Official, interviewed by the Author, Tallinn, June 28, 2016.
[118] State Information System Authority Official, interviewed by author, Tallinn, July 7, 2016.

governance in the speeches of Estonian officials suggests that although the official discourse may portray it as sharing, e-governance is still in a way promoted.

Within the EU, e-governance was portrayed as being less altruistic and actively being promoted. For instance, the RIA official claimed that:

> "…I think that e-governance is something that towards the European Union we see that okay it has actually opened the internal market and that is why we are doing this project now with Finland, piolet program with Finland. And if it works with Estonia and Finland than in the longer term it could work across the European Union and you would have less barriers in conducting your business life and social life. So the European Union is something where you might find some promotion."[119]

In the context of the EU, Estonian discourse is more promotional and reflects the benefits that it can offer to the entire union like 'less barriers' in conducting business and personal life.

So although it remains difficult to say if e-governance is actively promoted or not, one thing that is clear is what benefits e-governance is portrayed as bring to the countries that adopt it. Specifically, e-governance is portrayed as a way to increase efficiency and to build transparency. When asked if e-governance was conceived to create transparency and efficiency, every interviewee responded with a in the affirmative. The official at the MFA stated, "Of course, what we can see is that transparency and efficiency are the key words." This was also echoed by the rest of the interviewees as well. Specifically, efficiency was referenced as an ability to save time and once in relation to financial efficiency as well. For instance the EGA official explained, "…there are calculations, they are very broad at the moment I think but if every person uses digital signatures effectively, every person can save about one week per year, of working time. If you do that very rough calculation that every person saves one week is about 2% of GDP."[120] In other words, the discourse frames e-governance as a way to create transparency in the government and efficiency that decreases the time required to perform tasks. This was also mentioned by the official from RIA, who explained it similarly, but form the perspective of having a family. In this case he explained,

[119] IBID.
[120] E-Governance Academy Official, interviewed by the Author, Tallinn, June 28, 2016.

"If you have a family of four you save one month."[121] This means that the efficiency can really add up and make a difference not only for people working in the government but for families as well, hence beneficial to everyone.

Despite the benefits of e-governance such as transparency and increased efficiency it appears that Estonia has been most successful, sharing e-governance with other small states. Although this is not exclusively the case, which was made clear by the EGA representative, "…at the end of the day everyone is talking about how to use resources more effectively. It is just simpler to work with smaller countries, but we work with bigger countries as well."[122] Still although Estonia is portrayed as working with all countries on e-governance. Small countries are viewed as being the best place to spend resources. When asked if being a small state was beneficial when Estonia promotes norms to other small states, the majority of interviews agreed that being a small state meant that they were more likely to understand the limitations of other small states. The EGA official explained in the following way,

> "Of course logically it is easier for us to work with smaller countries, because they have the same limitations that we have recourses and population for example. They have bigger pressure to automate the systems and use them efficiently. The bigger countries simply do not have the resources problem, so they don't have the stick that pushes them to take this approach towards e-governance."

Where Estonia is perceived to be able to understand the needs of other small states it is not perceived to be able to predict or understand those of larger states. This was best articulated by the RIA official which explained, "When India was rolling out their ID cards, their speed was one million new users per week. One Estonia per week, and for us to understand their challenge is a bit difficult. I think that might be that if they have a challenge, we might just not relate to the challenge." In other words small states face similar situations understanding their needs comes more natural to Estonia, than say the needs of a large state, which operates under completely different constraints.

[121] State Information System Authority Official, interviewed by author, Tallinn, July 7, 2016.
[122] E-Governance Academy Official, interviewed by the Author, Tallinn, June 28, 2016.

One limitation that is linked to not being able to meet the needs of larger states is the issue of scalability. All five of the interviewees mentioned scalability as a limitation. Four of these saw it as an actual limitation while one argued that it was only perceived as a limitation by larger countries. For example, the official argued that it is perceived that X-road cannot be scaled for larger countries, but that is not really the case.[123] Still the prevailing view is that scalability is an issue. For instance, the RIA official stated, "I think the scalability and the size might be a problem." This was also framed a different way by policy expert one, "Some states have concerns about feasibility." Here as well as in critical infrastructure protection, Estonia views their ability to promote e-governance in the foreign policy as being limited by its size. In this case the limitation relates to large states being skeptical of Estonia's ideas due to the difference in size. Probably the best example of this came from a story the RIA official told:

> "It might work here and we might be very happy with our solutions – there is actually a good example connected to the U.S., we were in Washington D.C. in 2014, and we made a cyber security road show, at George Washington University. There was a forum and we talked about Estonian solutions like e-solutions and security solutions, and there was one guy who was asking – it turned out he was a decedent of Estonians, and he asked, "It is nice that it works there, but even if you were ten times bigger you would be the size of Ohio."[124]

In this story, the question of scalability is eluded to by comparing the size of Estonia to the size of the state of Ohio. The implication being that because Estonia is so small the solution will not work here. Whether it is true or not, it is a limitation that Estonia, articulates as being a limitation in their discourse.

The final limitation that official often mentioned was in relation to trust. The first example deals with the post-Soviet legacy that Estonia is faced with. The EGA official explained:

[123] E-Governance Academy Official, interviewed by the Author, Tallinn, June 28, 2016.
[124] State Information System Authority Official, interviewed by author, Tallinn, July 7, 2016.

> "I mean it is for many countries, it is probably hard to trust an Eastern European country that has been part of the Soviet Union for many years. So it is related to trust and of course these countries who have gathered more information and know how we have done it understand it is based on well-known security systems like public key infrastructure (PKI) and encryption and etc. They know that, but just to overcome what Estonia is or what Estonia is not, I think that being an Eastern European country has a certain connotation that does not work in our favor at the moment at all. That is a limitation, resources and historical background."[125]

This example references that trust can be an issue when promoting internet governance because being a post-soviet country has a relatively negative connotation. There was also references to the general level of trust that people have in the government. For instance, this was considered a limitation for policy expert two who claimed, "And this is a very subjective observation, but I feel that Estonians have a lot more trust towards their government than compared to other states, for some reason, I don't know why. So we are totally okay with our data being in servers and our signatures being digital and our voting being digital."[126] In other words, one limitation that Estonia faces when promoting e-governance is that some countries do not trust the government enough for e-services to actually work and be effective. This was also supported by, the official from RIA, who mentioned that trust is extremely important to the process and that Estonia works hard to build that trust for instance, when speaking on the openness after the cyber attacks:

> "Because we said we failed on some levels it actually increased the trust of the end users, because they realized if something is not good, they will respond, they will tell me. So therefore I [end user] trust the process, there is transparency there, there is an audit process there and there is an improvement process there. So I don't understand but I can trust, because the government is not hiding topics or vulnerabilities they are working on these topics."[127]

In other words, the trust that Estonian's have in their ecosystem was not something that happened overnight. It took time and situations where the state had to concede failure in order to win that trust. It is only logical to assume that this trust will take time to build elsewhere as well. This was also a fact eluded to by the RIA official who explained, "I have to understand other countries, because every country has their own legacy, history, and list

[125] E-Governance Academy Official, interviewed by the Author, Tallinn, June 28, 2016.
[126] Policy Expert Two, interviewed by the author, Tallinn, June 28, 2016.
[127] State Information System Authority Official, interviewed by author, Tallinn, July 7, 2016.

of fears. So I don't want to be condescending or arrogant, but just our experience has been so positive and that is why we are promoting it [e-governance] so actively." [128] This sort of understanding may be Estonia's best bet at helping other countries to overcome issues relating to trust and one day expanding e-services further.

Although there are limitation, the fact that Estonia has been so successful at e-governance at home, the promotion of it offers many benefits to Estonia. One way this has happened or is believed will happen is through business. The majority of the interviewees believed that the promotion of e-governance has or will increase business in Estonia.[129] The most prevalent example of a benefit was increased influence. This was mentioned in several different ways such as visibility mentioned by policy expert one.[130] Additionally, because Estonia is respected in e-governance they can get opportunities to share their views elsewhere. Policy expert two explained it like this, "…the promotion of e-governance is a part of Estonian foreign policy and I think that they have used this to gain in other fields not only governance. People look at us because of e-governance, but we also get this security output out of it. So there is a link because we are so good at e-governance services we also might be able to talk about security issues." So despite the perceived inability to scale solutions to larger countries, Estonia views its success in e-governance has led to concrete benefits, such as an increase in influence when promoting issues including security issues.

Because Estonia is known for e-governance it might be tempting to think that cooperation with the private sector isn't necessary to spread the norm, but the cooperation is very important to e-governance. The interviewees all agreed that cooperation was needed with the private sector. This is a viewed as being critical because the knowledge is centered in the private sector. This does not refer to the knowledge of how e-governance works, but the knowledge required to create services. For instance, policy expert two explained, "these services are actually developed by the private sector and [it is] actually the private sector is selling abroad, it is not the Estonian state selling them abroad so it is very linked to the private

[128] IBID
[129] Policy Expert Two, interviewed by the author, Tallinn, June 28, 2016.
[130] Policy Expert One, interviewed by the author, Tallinn, June 27, 2016.

sector."[131] This means that Estonian officials can share the experiences that Estonia has had as a result of e-governance, but they are not actually building services or providing services for countries that are interested in e-governance. So when a country decides they want to try e-governance Estonian officials turn to the private sector. So as the representative from the EGA puts it, "When it comes to the implementation phase we include the private sector."[132]

Estonia's cooperation with the private sector in relation to the promotion of e-governance norm goes really beyond what could be considered normal involvement by the private sector. Yes, the development of technologies and uses, as well as the associated public private partnership, is already one way that the private sector influences norms.[133] However, the way that the public private partnerships work in relation to this activity is framed differently. The promotion of e-governance does require the cooperation of both the private and public sectors to be achieved, but it is not about building capacity or understanding, it goes beyond that. It creates a sort of cycle where the private sector companies create good services for Estonia. Then Estonia shares its experience with another state. Finally, if that state desires a similar services, Estonia includes the companies into the process. In this since, influencing the norm is not that different when it comes to the development and use of technologies, but a small aspect of the private public partnerships (PPPs) has been expanded. The private sector is dependent on the cooperation between Estonia, other states, and itself. In other words, these companies do not just create technologies that foreign companies later buy. Interest in e-governance is developed by the public sector and then through cooperation the private sector is brought in to help countries realize their goals. So the cooperation goes beyond the normal capacity building measures.

In terms of dominate discourse, e-governance is framed as being something that Estonia does not actively promote outside of the EU. Instead, Estonia portrays it as sharing their experiences relating to e-governance, while not pushing e-governance. Still the way

[131] Policy Expert Two, interviewed by the author, Tallinn, June 28, 2016.
[132] E-Governance Academy Official, interviewed by the Author, Tallinn, June 28, 2016.
[133] Shireen Alam and Ilias Chantzos, "Technological Integrity and The Role of Industry in Emerging Cyber Norms," in International Cyber Norms: Legal, Policy and Industry Perspectives, ed. Anna-Maria Osula and Henry Rõigas. (Tallinn: NATO CCD COE, 2016): 205-210.

these experiences are shown and displayed resembles promotion, and questions whether the discourse is entirely honest. The experience that Estonia shares is framed as increasing transparency and efficiency of the state.

While there are many benefits and limitations to the promotion of e-governance, several standout from the rest. Business possibilities and increased influence being the two most prominent examples of benefits. Although, it is not usually associated with field of security, Estonia's success with E-governance is seen as a something that helps Estonia to exercise increased influence in other areas including security. Despite the benefits that Estonia has received from e-governance it also faces considerable limitations that once again relate to Estonia's size. Specifically, size is framed in the discourse as a problem of scalability. Meaning that e-government solutions that work well for Estonia may be seen as unusable by larger countries do to the size difference between the countries.

An additional limitation is, that not all countries share Estonia's enthusiasm of trusting the government with their personal data. This as the Estonian officials noted is something that is foreign to them as they trust the services and the government. Still, it is recognized that each country has a different history and as a result trust in the government varies. Another variation on the problem of trust comes from other countries ability to trust Estonia. Specifically, some states are perceived to have a lack of Eastern European countries or post-Soviet countries.

The cooperation between Estonia and the private sector once again extends the private sectors involvement beyond what it is normally seen as comprising when it comes to influencing norms. Specifically, it creates a complex relationship where the private sector does not only influence norms through the creation of technology. Instead, the influence becomes partly reliant on the private sectors cooperation with the Estonian public sector, and partially dependent on the relationship between the Estonian state and other countries. This expands PPPs into new territory that goes beyond building capacity building and understanding.

7. Promotion of a Free and Open Internet

The NGO Freedom House has documented an overall trend showing a decrease in internet freedom.[134] Estonia has avoided this trend and is one of the most active countries, if not the most active country, in the promotion and maintaining of a free and open internet. This includes being a member in the Freedom Online Coalition, and the Digital Defenders Partnership (DDP). As a member of these organizations Estonia has supported the initiatives of these organizations. The Freedom Online Coalition helps to monitor internet freedom throughout many countries in the world as well as draws attention to violations to internet freedom.[135] While the DDP is an NGO that is supported by several countries including Estonia. A large part of what the DDP does is provide funding through grants to NGOs, human rights activists, and journalist that face repression due to their work. This can come in several forms, such as purchasing virtual private networks (VPNs) or other secure communication technologies for activists or providing them with training on best practices.[136]

In addition to having supported NGOs that promote internet freedom, Estonia has also supported an open internet at the UN. Specifically at the fourth GGE Estonia supported the inclusion of a reference to the July 2012, general assembly resolution, which they had earlier adopted. This resolution states that rights afforded to people offline must also be afforded online.[137]

---

[134] Freedom House, "Freedom on the Net 2015," accessed May 5, 2016, "https://freedomhouse.org/sites/default/files/FOTN%202015%20Full%20Report.pdf.
[135] Estonian Ministry of Foreign Affairs, "Freedom Online Tallinn," last accessed July 20, 2016, http://www.freedomonline.ee/.; and Freedom Online Coalition, "Freedom Online Coalition," last accessed July 20, 2016, https://www.freedomonlinecoalition.com/.
[136] Digital Defenders Partnership, "Digital Defenders Partnership," last accessed July 28, 2016, https://www.digitaldefenders.org/.
[137] Marina Kaljurand, "United Nations Group of Governmental Experts: The Estonian Perspective," 123.

In light of Estonia's support for a free and open internet, this section has sought to answer several questions by gleaning information from the official discourse. The flowing questions have been considered:

- How does Estonia view the free and open internet and its promotion?
- Does Estonia receive any benefits and/or face any limitations from the promotion of a free and open internet.
- What kind of cooperation has there been between Estonia and the private sector in regards to a free and open internet?

It is clear that Estonia supports organizations that champion a free and open internet and it is also clear that Estonia has supported a free internet in the UN as well. It is reasonable to assume that Estonia would also frame their discourse in a way that emphasizes the need to protect the openness of the internet. When asked how important a free and open internet was to Estonian foreign policy all of the officials agreed that a free and open internet was a priority. Not surprisingly the discourse reflected policy decisions that Estonia has made in the past. However, the reasons portrayed by the discourse provides insight into why this norm is a foreign policy priority for Estonia.

Of the answers given to the question mentioned above the most common justification had to do with identity, and Estonia's position as a Western and liberal democracy. This was portrayed in several different ways, but always with the same theme. For instance, by contrasting Estonia to authoritarian regimes such as, "Another reason [a free and open internet is a priority] is the concern over the actions of authoritarian countries."[138] However, the best summery not surprisingly came from the representative at the MFA that stated:

> "I would say that this is a question about very fundamental issues about what our society is based on and what is the international community based on. You can call them slogans democracy, human rights, and the rule of law. These are the 3 pillars that our way of life is depending on and this is a natural part of our foreign policy. Free internet is a part of free societies and democratic world order. So there is nothing

[138] Policy Expert One, interviewed by the author, Tallinn, June 27, 2016.

> special in this field. What is new with regard to the internet and ICTs in general is that some states see it as a threat to their order and they want to limit it."[139]

The MFA still phrased it as being about identity; however, it is not directly opposed to something, like the statement on authoritarian countries. Policy expert two specifically mentioned identity, "I think this links again with Estonia's larger strategy and aim to be part of the west. It used to be a huge thing in the 90s and before we gained membership in the EU and in NATO. But it is still part of our basic identity, you always have to identify your strong points and go with it." To sum up, Estonia's promotion of a free and open internet is largely framed as a result of their identification as a western country and the values that are associated with that.

Another reason for the promotion of a free and open internet also appeared multiple times throughout the interviews, which was the ability of Estonians to access services anywhere in the world. This was explained in an interview with the RIA official that explained:

> "If we look at the participation of people who are residing outside of Estonia and participating in elections and things like that, they seem to be really active. People are using these opportunities. Before that they would only be able to participate through the letters. I think that getting them involved without the physical barriers is much more engaging. If you are living outside you are still part of Estonia. You don't have to travel to participate."[140]

Estonians can currently vote online, make bank transactions, and open a business from anywhere with an internet connection; however, in places that block internet traffic Estonians may or may not be able to access these services. This point was echoed by the EGA representative who stated, "What is important for us is that if we are abroad we can still access Estonian cyber space, because we have our electronic services. So we don't want someone to create such strong boarders that we cannot even connect to Estonian services

[139] Ministry of Foreign Affairs Official, interviewed by the author, Tallinn, July 4, 2016
[140] State Information System Authority Official, interviewed by author, Tallinn, July 7, 2016.

over the internet."[141] In other words, currently Estonians are able to travel and work where they desire and still be able to participate in government with minimal hassle, but a closed internet could have a very adverse effect on this. Particularly when you remember that Estonia does not have a consulate or embassy in every country, it is easy to see how the ability to vote could be drastically changed if Estonians residing abroad were no longer able to vote online.

The last reason that the interviewees mentioned as being a reason for the prominence of the norm of a free and open internet was that a closed internet is a perceived threat to a small state. The reason for the threat was mostly related to the restriction of information. Policy expert one explained that, "It [a closed internet] is definitely conceived as one [threat]. It restricts information, which a small state relies on. Estonia's position is to allow free access to information…"[142] The official from RIA also eluded to the impact a closed internet has on information:

> "I think it would be the case of having a long term impact on being isolated that would be rather negative whether you are a small or a big country. I would be concerned if part of the international community, one country or a couple of countries are completely isolated from the rest and let's say they get only their internal twisted messages…and that is my worry here is that the end users sooner or later a certain part start to believe it, these twisted messages, and that doesn't help the international society much. It doesn't have a long term benefit for everyone."[143]

Again, the reason is framed as restriction of information; however, this time it is not relating to Estonia. It is referencing how countries can be effected by not having access to outside information. This however can still be very relevant to Estonia as the official explained:

> "I have had these experiences before, even before these escalations with Ukraine and Russia and people are surprised that I am actually speaking Russian with them. Because they have gotten from the media that as a principle Estonians will not speak Russian with them. They forget that the new generation just doesn't learn Russian too much anymore, and they don't have practice, so they just don't know how to

[141] E-Governance Academy Official, interviewed by the Author, Tallinn, June 28, 2016.
[142] Policy Expert One, interviewed by the author, Tallinn, June 27, 2016.
[143] State Information System Authority Official, interviewed by author, Tallinn, July 7, 2016.

> speak it anymore. Then it is presented in a way that we are intentionally hostile to an individual language or culture…"[144]

This example illustrates how a small state, or any state for that matter, can be negatively affected when a country restricts information on the internet and illustrates how it is framed as a threat to Estonia.

One benefit that Estonia has when promoting a free and open internet is the fact they have one of the most free and open internets in the world.[145] This has been framed as giving Estonia increased credibility when promoting norms of a free and open internet. For instance, policy expert one stated "it shows at international meetings. It is an area where Estonia has an image of being experts. Officials are often asked to talk and participate at conferences and others are interested in our views."[146] In this way it is shown to be similar to how e-governance gives Estonia increased influence. In this case influence is increased by being opportunities to be heard and a willingness of others to listen to and potentially learn from the Estonian prospective. The RIA official took a similar position saying, "I think so because we talk the way we act, as I see it … that gives us a certain credibility. That our experience supports what we say, and that we don't act domestically different than when we make the messages outside."[147] So in other words, when Estonia promotes a norm relating to the free and open internet it is more likely to be accepted or at least heard. This follows the same logic as the neutral countries being more successful at creating peace building norms, or Nordic countries being more likely to succeed at promoting norms relating to social welfare. Additionally, when Estonia brings up an abuse of the free internet it is more likely to be heard and harder to reject. For instance, the U.S. has faced problems when bringing up the imprisonment of human rights activists, because the other country needs only point to the

[144] IBID
[145] Freedom House, "Freedom on the Net 2015," accessed May 5, 2016, "https://freedomhouse.org/sites/default/files/FOTN%202015%20Full%20Report.pdf.
[146] Policy Expert One, interviewed by the author, Tallinn, June 27, 2016.
[147] State Information System Authority Official, interviewed by author, Tallinn, July 7, 2016.

Guantanamo Bay Detention Facility. By 'walking the walk,' it is easier for Estonia to avoid similar issues.

When it comes to private sector cooperation on norms relating to the free and open internet, the official discourse is difficult to discern. Most of the officials agreed that cooperation with the private sector was an important, but there were few examples of actual cooperation. One example is that the private sector provides reports on abuses of online freedom, which helps small states like Estonia, because with limited resources they cannot be everywhere.[148] This therefore allows officials to be better informed about the global situation regarding a free and open internet and the threats to that.

This very small and token level cooperation cannot be seen as an improvement to the level of cooperation that the private sector normally provides in relation to influencing norms. This is because the sharing of reports really is an example of capacity building which the private sector already does. One reason for this is again mentioned by the employee of the MFA, who eluded that cooperation on this matter was rather rare.[149] So although Estonia views the cooperation as important, it has yet to fully realize this cooperation and at best has cooperated in a limited manor.

8. Conclusion

[148] Ministry of Foreign Affairs Official, interviewed by the author, Tallinn, July 4, 2016.
[149] IBID.

This thesis sought to glean insights about how Estonia frames discourse relating to three specific policy area that Estonia promotes cyber norms in. Specifically, views on norms relating to the protection of critical infrastructure, e-governance, and the promotion of a free and open internet. For additional value this thesis also examined the cooperation between the Estonian public sector and the private sector as viewed from the official Estonian discourse. To do this interviews were conducted and then analyzed in order to find patterns. Several interesting insights were able to be analyzed from the discourse.

One key finding is that in terms of discourse on norms in general Estonia sees the promotion of cyber norms as an important part of their foreign policy because of the unique ability that they have to add clarity and reduce conflict. This also holds true for the protection of critical infrastructure although, the past experiences that Estonia faced during the 2007 cyber attacks have also played a role. The other two main areas e-governance and a promotion of a free and open internet are more associated with identity. E-governance being portrayed as being example of an Estonian success that other likeminded countries can replicate. The promotion of a free and open internet is something that is also very identity driven in Estonian discourse. Specifically, Estonia's promotion of a free and open internet is seen as upholding the values of liberal democracies and western countries, while an unfree internet is associated with authoritarian states. Additionally, the infringement of the free and open internet is conceptualized as a threat to Estonia.

Estonia's position of being a small state is primarily seen as being a weakness when promoting cyber norms, but this is not exclusively the case. In general, when promoting norms Estonia faces limited resource, which officials believe requires them to prioritize

topics. Even in topics that can be seen as priorities, such as those analyzed here, Estonia faces limitations from being a small state. Throughout the promotion of norms on protection of critical infrastructure and e-governance, Estonia is perceived to face limitations that arise from being a small state. In the case of norms regarding the protection of critical infrastructure, this is seen primarily as an issue arising from the lack of personnel resources. When speaking in terms of e-governance, the issues are more related to scalability, or if a service developed by a small state can work for a larger state. An additional aspect of this relates to if a service is actually believable because Estonia's voice is not perceived to carry the same weight as some other the larger actors, such as the United States. Still, although the size of Estonia was largely perceived as a weakness, it is framed as giving them increased influence when promoting e-governance to other small states due to shared limitations.

The increased influence with small states was not the only benefit that Estonia receives from promoting norms. One commonly mentioned benefit that relates to the promotion of cyber norms is that, Estonia views and portrays its norms as having long term impact and promoting a better future for everyone. This was apparent with the example of e-IDAS regulation and the promotion of all three policy areas that were analyzed. Norms relating to the protection of critical infrastructure were seen as creating clarity and building mutual understanding, which is good for everyone because it reduces the risk of serious cyber incidents occurring. In terms of e-governance, it was framed as a way to create transparency and increase efficiency. The creation of transparency is clearly a benefit that falls into the discourse of a better future, and when speaking about efficiency relating to time saved this is also the case. Promotion of a free and open internet was also in a way portrayed in a way

that promotes a better future because, it facilitates the free flow of information and allows people access.

Another prominent benefit that Estonia is perceived to receive from promoting cyber norms is increased influence in other policy areas including security. Because Estonia has been so successful at e-governance and has been very effective at sharing their success they are portrayed to have increased influence in other areas. So when asked to discuss e-governance Estonian officials get a chance to speak about other issues including security subjects. Something similar also happens in regards to Estonia's promotion of a free and open internet. Although it is not portrayed as offering the same level of benefit as e-governance, this area is still seen as an area where Estonia excels. As a result, Estonian officials are often asked to speak at conferences and are able to get their opinions heard. When promoting norms on the protection of critical infrastructure the increased influence that Estonia receives is not framed as coming from the promotion of norms, but rather the cyber attacks of 2007. This is an interesting difference in how the norms are viewed. Whereas the other areas are seen to contribute to Estonia's influence, with protection of critical infrastructure Estonia is seen as being influential because of another factor.

Despite the increased influence Estonia has received from promotion of norms, cooperation with the private sector varies depending on the area. In terms of the protection of critical infrastructure, Estonian discourse does not frame cooperation as an area where Estonia is expanding or involving the private sector in new ways. Instead it is portrayed as being something that Estonia has been able to perfect, making an environment where the private sector looks forward to cooperating. The most productive area of cooperation with

the private sector is portrayed in matters of e-governance, where the partnership extends past what can be seen as normal capacity building. In comparison, the cooperation on norms relating to a free and open internet has been the least effective, and based on the level of portrayal is rather limited.

In light of these findings this thesis proposes several recommendations on a ways to improve how Estonia promotes cyber norms. First, a train up period for incoming officials could decrease the disruption caused by officials leaving their posts. This would without a doubt make the promotion of cyber norms more effective. Of course, personnel resources have to be taken into account and it may be determined that this is not possible. Second, cooperation with the private sector could be expanded particularly in regards to the promotion of a free and open internet. At this point in time, cooperation is only viewed as information sharing, which can be beneficial to a small state like Estonia, but more cooperation could prove beneficial. For instance working with the private sector on common initiatives could create increased visibility for Estonia in the international arena. Final, the discourse on the promotion of e-governance and scalability may need adjustment. In terms of e-governance, although technically Estonia is sharing their experiences, some methods are extremely close to promotion, and in the case of the EU there is promotion.

The adjustment to the discourse on scalability is also worth looking into. For instance, as mentioned earlier, the EGA official argued that scalability is not always an issue, using the X-road as an example. If made possible by resources availability, key services should be evaluated for their potential to be scaled and discourse should be changed to reflect this. Adjusting the discourse on issues of scalability could be of benefit to Estonia when they are

sharing their experience with e-governance both inside and outside the EU. Specifically, it could decrease the perceptions of foreigners that e-governance isn't scalable for larger states. Without adjustment it is likely that in at least some cases the meetings with foreign officials will continue to face skepticism over scalability.

In light of the research conducted here as well as the findings reported above there are several areas that may prove fruitful for future research. First, research could be conducted with private sector companies in Estonia in order to examine similarities and/or differences in the discourse about cooperation between the public and private sector. Particularly, interviews with officials from Estonia's big banks and telecommunication companies could be of value. Second, small-n studies could be conducted looking at similarities or differences other countries have when promoting norms around protection of critical infrastructure, e-governance, and a free and open internet. Final, and perhaps the best avenue of research might be researching e-governance promulgation and dissemination in the EU. It currently appears that Estonia's promotion of e-governance, as well as the interest of other countries is creating a significant expansion of the use e-governance and e-services. Looking into what role Estonia has played in this could be an interesting topic as could comparing the reasons why countries are promoting and perusing e-governance.

9. Summary of Findings

Estonia and Perceptions on Cyber Norms

Estonia views the promotion of cyber norms as very important to their foreign policy. This is mainly seen as a way to increase predictability. This is not seen as something that is only good for Estonia, but it is seen as something that benefits all the members of different groups, because of the clarity they add. Estonia views that it is able to promote norms, but the official discourse is skeptical as to whether they can create norms. Part of this is due to the limitations that Estonia faces promoting norms, such as limited resources. These limited resources are not helped by the fact that a transition mechanism is not in place to allow for the smooth transition of officials. One thing that may have helped Estonia overcome, this problem is the idea that it is a good test pit for new ideas, which to Estonia is considered to one of the greatest benefits they have when it comes to promoting cyber norms.

Protection of Critical Infrastructure

Cyber norms relating to the protection of critical infrastructure are viewed as being important due to the 2007 cyber attacks that showed that Estonia is vulnerable due to its dependence on ICTs. While promoting cyber norms in this area Estonia perceives itself as benefiting from the decreased risk that comes from adding clarity and explaining expectations relating to the protection of critical infrastructure. Still, Estonia faces the limitations that traditionally effect small states. Even with the limitations, Estonia is portrayed in the discourse as having been able to excel at cooperation with the private sector in this area.

E-Governance as a Norm

For Estonia it is portrayed as natural to promote e-governance, because of their experience is unique and has been quite successful. Despite the successes of e-governance the discourse surrounding the topic clams that it is not actively promoted except for maybe in the context of the EU. However, although it is not considered to be promoted it is portrayed as a way that states can increase transparency and create efficiency. As a small state Estonia believes it is better able to assist other small states in comparison to large states, such as India. Directly linked to this issue is the limitation of scalability, which official believe prevent some service from being adopted by larger countries. Although, there are limitations due to size, the fact that Estonia is good at e-governance is seen as increasing their influence. In the area of e-governance the private sector cooperation increases the participation of the private sector past its normal level. Specifically, the private sector benefits from a more complex relationship between the Estonian State, other countries, and itself, which expands the traditional level of cooperation in PPPs.

Promotion of a Free and Open Internet

For Estonia the promotion of a free and open internet is largely seen as an expression of their identity and values. It is a foreign policy choice that is articulated as being important do to the comment to the values of western states and liberal democracies. In addition to being about Estonia's identity, it is also about the need for a free flow of information. This is because Estonians rely on the free flow of information in order to use e-services and participate in government while they are abroad, but also because isolation of people has had a negative impact on how those people view Estonia. One way that Estonia could likely improve the promotion of a free and open internet is by integrating the private sector more thoroughly into the process. To date the cooperation has been extremely limited.

Bibliography

Aaltola, Mika, et al., "Securing the Global Commons: A Small State Perspective" (working paper, FIIA, 2011), http://www.fiia.fi/en/publication/198/securing_global_commons/.

Aaltola, Mika. et al. "Pushed Together by External Force? The Foreign and Security Policies of Estonia and Finland in the Context of the Ukraine Chrisis" (Briefing Paper, FIIA, 2015), 7, http://www.fiia.fi/en/publication/473/pushed_together_by_external_forces/.

Alam, Shireen and Ilias Chantzos, "Technological Integrity and The Role of Industry in Emerging Cyber Norms," in *International Cyber Norms: Legal, Policy and Industry Perspectives*, ed. Anna-Maria Osula and Henry Rõigas. Tallinn: NATO CCD COE, 2016.

Allan, Collin and Matthew Crandall. "Small States and Big Ideas: Estonia's Battle for Cybersecurity Norms," *Contemporary Security Policy* 36, no. 2 (July, 2015): pg.

Archer, Clive. "Nordic Swans and Baltic Cygnets," *Cooperation and Conflict* 34 no.1 (March, 1999): 48, accessed March 10, 2015, http://cac.sagepub.com/content/34/1/47.full.pdf+html.

Archer, Clive; Bailes, Alyson J.K.; Wivel, Anders. Small States and International Security: Europe and Beyond. (Florence: Taylor and Francis, 2014):54, (accessed March 17, 2016) http://GLA.eblib.com/patron/FullRecord.aspx?p=1683235.

Areng, Liina. "Lilliputian States in Digital Affairs and Cyber Security," in *The Tallinn Papers: Numbers 1-9 (2014-2015)*, ed. Liis Vihul, Tallinn: NATO CCD COE, 2015.

Baehr, Peter R. "Small States: A Tool for Analysis," *World Politics* 27, no. 3 (April, 1975): (Pages), accessed March 17, 2016, http://www.jstor.org/stable/2010129.

Browning, Christopher S. and Pertti Joenniemi. "Regionality Beyond Security? The Baltic Sea Region after Enlargement," *Cooperation and Conflict* 39, no. 3 (2004), accessed March 10, 2015, doi:10.1177/0010836704045202

Browning, Christopher, S. "Small, Smart and Salient? Rethinking Identity in the Small State Literature," *Cambridge Review of International Affairs* 19, no. 4 (December, 2006): (Pages), accessed January 11, 2016, http://dx.doi.org/10.1080/09557570601003536.

Burnham, Peter, et al. "Elite Interviewing" in *Research Methods in Politics.* New York: Palgrave, 2008.

Burton, Joe. “Small states and cyber security: The case of New Zealand,” *Political Science* 65, no. 2 (2013): (Pages), accessed February 3, 2016, DOI: 10.1177/0032318713508491.

Carr ,Madeline and Toni Erskine. “Beyond ‘Quasi-Norms’: The Challenges and Potential of Engaging with Norms in Cyberspace,” in *International Cyber Norms: Legal, Policy and Industry Perspectives,* ed. Anna-Maria Osula and Henry Rõigas. Tallinn: NATO CCD COE, 2016.

Charney, Scott “Governments and APTs: The Need for Norms” in *Cybersecurity Norms: Advancing persistent Security* (n.p., Microsoft, 2014): 12-13.

Crandall, Matthew. “Soft Security Threats and Small States: the Case of Estonia,” *Defence Studies* 14, no. 1 (March, 2014): (Pages), accessed December 14, 2015, http://dx.doi.org/10.1080/14702436.2014.890334.

Digital Defenders Partnership. “Digital Defenders Partnership.” last accessed July 28, 2016. https://www.digitaldefenders.org/

e-Estonia, “The Future is Now,” Promotional publication (n.p.: n.d.)

E-Governance Academy Official, interviewed by the Author, Tallinn, June 28, 2016.

E-Governance Academy. “Projects.” Last Accessed July 9, 2016. http://ega.ee/projects/.

Estonian Ministry of Foreign Affairs, “Freedom Online Tallinn.” last accessed July 20, 2016. http://www.freedomonline.ee/.

Finnemore, Martha and Kathryn Sikkink. “International Norm Dynamics and Political Change,” *International Organization* 52, no. 4 (Autumn 1998): pg.

Finnemore, Martha. “Cultivating International Cyber Norms,” in *America’s Cyber Future: Security and Prosperity in the Information age,* ed. Kristin M. Lord and Travis Sharp (Washington, D.C.: Center for a New American Security, 2011), (Pages), https://www.cnas.org/files/documents/publications/CNAS_Cyber_Volume%2011_2.pdf.

Freedom House. “Freedom on the Net 2015.” accessed May 5, 2016. “https://freedomhouse.org/sites/default/files/FOTN%202015%20Full%20Report.pdf.

Freedom Online Coalition,. “Freedom Online Coalition.” last accessed July 20, 2016. https://www.freedomonlinecoalition.com/.

Goetschel, Laurent. “Neutrals as Broker of Peace Building Ideas?” *Cooperation and Conflict* 46 no. 3 (2011): 312-33.

Goldman, Seymour E., David W. Longhurst, and Stephen J. Lukasik, *Protecting Critical Infrastructures Against Cyber-Attack.* Oxford: Oxford University Press, 2003.

Hansen, Lene and Helen Nissenbaum. "Digital Disaster, 'Cyber Security,' and the Copenhagen School," *International Studies Quarterly* 53, (December, 2009): 1160-1, accessed March 8, 2015, http://www.jstor.org/stable/27735139.

Ingebritsen, Christine. *Scandinavia in World Politics* New York: Rowman and Littlefield, 2006.

Jepperson, Ronald L., Alexander Wendt, and Perter J. Katzenstien. "Norms, Identity, and Culture in National Security," in *Culture of National Security: Norms and Identity in World Politics*, ed. Peter J. Katzenstien, New York: Columbia University Press, 1 996.

Kaljurand, Marina. "United Nations Group of Governmental Experts: The Estonian Perspective." in International Cyber Norms: Legal, Policy and Industry Perspectives, ed. Anna-Maria Osula and Henry Rõigas. Tallinn: NATO CCD COE, 2016, 111-127.

Katzenstien, Perter J. "Introduction: Alternative Perspectives on National Security," in *Culture of National Security: Norms and Identity in World Politics*, ed. Peter J. Katzenstien New York: Columbia University Press, 1996.

Keohane, Robert O. "Lilliputians' Dilemmas: Small States in International Politics," *International Organization* 23, no. 2 (March, 1969): (Pages), accessed December 14, 2015, DOI:10.1017/S002081830003160X.

Keohane, Robert. "The Big Influence of Small Allies," *Foreign Policy* no. 2 (spring, 1971): 168-82.

Larsen, Henrik. *Foreign Policy and Discourse Analysis: France, Britain and* Europe. New York: Routledge, 1997.

March, James G. and Johan P. Olsen. "The International Dynamics of International Political Orders," *International Organization* 52, no. 4 (Autumn 1998): 943-969.

Maurer, Tim. "Cyber Norms Emergence at the United Nations: An Analysis of the Activities at the UN Regarding Cyber Security?" Discussion paper #2011-11, Cambridge, Mass.: *Belfer Center for Science and International Affairs, Harvard Kennedy School* (September 2011): 1-70.

Ministry of Foreign Affairs Official, interviewed by the author, Tallinn, July 4, 2016.

Neumann, Iver B., and Sieglinde Gstöhl. "Lilliputians in Gulliver's World?" in *Small States in International Relations*. Reykjavik: University of Iceland Press, 2006.

Nye, Joseph S., Jr. "Cyber Power," *Belfer Center for Science and International Affairs* (Harvard, 2010), http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf.

Pernik, Piret and Emmet Tuohy, "Cyberspace in Estonia: Great Security, Greater Challenges," *International Center for Defence Studies* (August, 2013): (Pages), accessed November 29, 2015, http://www.riso.ee/et/koosvoime/raamistik.

Policy Expert One, interviewed by the author, Tallinn, June 27, 2016.

Policy Expert Two, interviewed by the author, Tallinn, June 28, 2016.

Rõigas, Henry. "A Small State Utilizing its Niche Capability for Influence in Foreign and Security Policy: The Case of Estonia and Cyber Security." master's thesis, University of Tart, 2015. http://dspace.ut.ee/bitstream/handle/10062 /45179/roigas_henry_ma_ 2015.pdf ?sequence= 1&isAllowed=y.

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

State Information System Authority Official, interviewed by author, Tallinn, July 7, 2016.

Sunstein, Cass R. "Social Norms and Social Laws," *Columbia Law review* 96 no. 4 (May, 1996), accessed September 14, 2015, http://www.jstor.org/stable/1123430

The Baltic Course. "Sweden Interested in Estonia's X-Road Platform." Last Modified December 18, 2015. http://www.baltic-course.com/eng/good_ for_ business/?doc=114572.

Thorhallsson, Baldur. "Small States in the UN Security Council: Means of Influence?" *Hague Journal of Diplomacy* 7, (2012): Pages, accessed February 19, 2016, DOI: 10.1163/187119112X628454.

Thorhallssonn, Buldur and Anders Wivel,."Small States in the European Union: What Do We Know and What Would We Like to Know?" *Cambridge Review of International Affairs* 19, no. 4 (December, 2006): (Pages), accessed January 11, 2016, http://dx.doi.org/10.1080/09557570601003502.

Väyrynen, Raimo. "On the Definition and Measurement of Small Power Status," *Cooperation and Conflict* VI, (1976).

Wivel, Anders. "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, no. 2 (June, 2005).

World Bank, "Gross Domestic Product 2014," *World Development Indicators Database,* (February 17, 2016), http://databank.worldbank.org/data/download/GDP.pdf.

World Bank, "Small States: Meeting Challenges in the Global Economy," *Report of the Commonwealth Secretariat/World Bank Joint Taskforce*, (April 2000), http://siteresources.worldbank.org/PROJECTS/Resources/meetingchallengeinglobal econ omyl.pdf.

Appendix

Interview Themes and Questions

Does Estonia view cyber norms (or agreed upon standards of behavior for states in cyber space) as being necessary for the international system to function properly?

Does Estonia conceive itself as being able to create and promote cyber norms through foreign policy?

Cyber Norms Relating to Critical Infrastructure

Why are cyber norms relating to the protection of critical infrastructure such are prominent part of Estonian foreign policy? Does the promotion of cyber norms protecting critical infrastructure provide Estonia with any benefits (i.e., increasing security or expanded bilateral relations)?

How do other international actors view Estonia's initiatives regarding the protection of critical infrastructure?

As a small state, what limitations does Estonia face when trying to promote norms protecting critical infrastructure (i.e., lack of bilateral relations limited number of officials, etc.…)?

How has the cyber attack of 2007 had an impact on how Estonia's views on protecting critical infrastructure? Is it seen or used as an example to illustrate the need for norms protecting Critical infrastructure? Did the attacks increase Estonia's influence in promoting norms that relate to protection of critical infrastructure?

Is it necessary to cooperate with the private sector to develop and promote cyber norms for critical infrastructure? In what ways has there been cooperation with the private sector in regards to protecting critical infrastructure from cyber attacks? What kind of cooperation has occurred and has it revealed any benefits or limitations?

E-governance as a Norm

Is the promotion of e-governance seen as a crucial part of Estonia's foreign policy? How is e-governance promoted in foreign policy? Is e-governance promoted as a way to help other governments create transparency and/or efficiency?

Does Estonia's experience and success with e-governance give it increased credibility when promoting e-governance to other countries? Does being a small state help to show the value of e-governance.

Has Estonia received any concrete benefits from the promotion of e-governance?

- Has it increased Estonia's influence in areas of governance or cyber issues?
- Has it created an increase in private sector growth? Is e-Residency seen as a way to help Estonia compete for businesses?

What limitations does Estonia face when promoting e-governance to other countries? Does being a small state hinder dialog with larger states?

Is cooperation with the private sector necessary for the promotion of e-governance? How does Estonia cooperate with the private sector when promoting e-governance? Are there any benefits or limitations to cooperation with the private sector?

Promotion of a Free and Open Internet

How important to Estonian foreign policy is the promotion of a free and open internet? Why does Estonia view an open and free internet to be so important? Is the possibility of a closed (or not free) internet a threat to small states?

Does Estonia's position of having one of the most free and open internets provide Estonia with increased credibility when promoting an open internet elsewhere? Does being a small state also add credibility?

Does Estonia work with the private sector to promote and help ensure a free and open internet? Does Estonia view public and private sector cooperation as being necessary for a free and open internet to exist? In what ways have cooperation occurred or should cooperation occur? What benefits or limitations have resulted from cooperation between the public and private sectors?