UNIVERSITY OF TARTU

Faculty of Social Sciences

Johan Skytte Institute of Political Studies

Riin Suuster

COMPARATIVE ANALYSIS OF THE LOCALIZATION OF INTERNATIONAL CYBER SECURITY NORMS: ESTONIA AND ISRAEL

BA thesis

Supervisor: Thomas Michael Linsenmaier, MA

Tartu 2025

Authorship Declaration

I have prepared this thesis independently. All the views of other authors, as well as data from literary sources and elsewhere, have been cited.

Word count of the thesis: 13665

Riin Suuster 19.05. 2025

Abstract

This dissertation presents a comparative analysis of the localization of international cybersecurity norms in Estonia and Israel, focusing in particular on the Budapest Convention on Cybercrime (2001). The main research question of the dissertation is: what explains the variation of implementation of the norms of the Budapest Convention in the Estonian and Israeli contexts? It is explored through a constructivist approach to norms in International Relations theory and operationalizes a theoretical framework that defines conditions for successful norm localization and outlines a spectrum of norm localization outcomes that can be observed in three dimensions: translation in domestic discourse, translation in law, and translation in implementation. To empirically answer the research question, the thesis applies the Small-N Most Similar System Design (MSSD), a comparative method chosen to isolate the factors that cause the variation in norm localization in the two cases. The analysis itself reveals different trajectories in Estonia and Israel. Estonia mostly shows a pattern of full adoption of the provisions of the Budapest Convention. In contrast, Israel has a clear pattern of reinterpretation. Israel has often selectively modified provisions or maintained reservations based on national priorities, whilst Estonia has adopted the provisions with minor changes. The thesis concludes that while both countries have active norm entrepreneurs and capable investigation units, the main reason for the differences in localization types between Estonia (full adoption) and Israel (reinterpretation) in regards to the Convention is due to differences in domestic legislation. This dissertation over all attempts to contribute to the understanding of the localization of international norms as a complex and uneven process, significantly shaped by domestic legislation not just the presence of supporting actors or implementation capacity. Further research could explore the development of norm entrepreneurs' discourse or extend the comparison to other countries.

Table of Contents

Figures, tables graphs

1. Introduction

Since the turn of the century the internet has become a general purpose technology, in 2016 it made for 4 trillion dollars to the global economy and connects millions of people (Nye. 2016: 44). With the emergence of technologies and ever growing use of ICTs the discussion around the norms and standards surrounding these technologies has been evolving. The absence of norm-guided behaviour has become a growing concern to governments and private organisations alike (Huang & Madnick. 2023: 203). Hence some actors have been calling for the development of "cyber norms" to provide security and governance in cyberspace, an example of this would be advocating for non-interference in election processes via the use of ICTs (Huagng & Madnick et al. 2023: 205; Finnmore & Hollins. 2016).

The term "cyber" itself is somewhat ambiguous and used to refer to a variety of wireless, digital and computer-related activities (Nye. 2016: 45). Complicated even more by the nature of cyberspace, which has little resemblance to the physical world that we experience everyday. Unlike the physical world, cyberspace or sometimes referred to as the cyber domain has no borders. This highlights the importance of cooperation in digital governance on an international level. According to Finnemore and Hollis (2016: 436-437) today, norms have become a regulatory tool for advancing stability and safety in cyberspace. Matters are also complicated, as cyberspace is formed by millions of lines of code, making vulnerabilities an inherent feature (Finnemore & Hollis. 2016: 432). These vulnerabilities are what states or cybercriminals look to exploit. Leading to millions of cyber attacks every year, running from threats, espionage, sabotage, disruption to war (Nye. 2016: 47). These attacks can be coordinated by states or non-state actors, most often referred to as hacktivists or cybercriminals, as they organise and form groups either for hire or fighting for a certain cause. Although, these groups do not always operate with impunity and in many states are held accountable (Finnemore & Hollis. 2016: 435). As for states, they have the ability to act in cyber space both directly or by proxy, for example via hired cybercriminals (Finnemore & Hollis. 2016: 436). Both what cybercriminals look to exploit and how states are involved in the cyber domain is important to understand in discussions of how cyber norms work and how we regulate behavior in cyberspace.

The research itself is guided by the central question: What explains variation in the way norms from the Budapest Convention have been implemented in Estonia's and Israel's

national contexts? To answer this question the thesis employs the works of different academics to establish a theoretical framework. Firstly, establishing that norms according to Finnemore and Sikkink (1998: 891) are defined as a standard of appropriate behaviour for a state with a given identity. Therefore, providing us with the knowledge that norm functions have more of a regulative nature. Furthermore, the thesis will be relying on Achyara's (2004: 251) conditions for localization and Zimmermann's (2016: 106) types of localization to provide us with specific understanding on how localization as a concept works and how we can identify the type of localization in a state. My hypothesis is that Estonia has experienced a greater degree of localization that can be deemed full-adoption and Israel's type of localization can be considered reinterpretation.

To answer this research question the thesis operationalizes the theoretical framework by the use of the Most Similar Systems Design (MSSD) which provides us with the necessary complexity to hone in on a specific variable responsible for the variation in localization outcomes. Analysis will be divided into three levels: type of localization, norm entrepreneurs and cybercrime investigation units. Legal documents from the Council of Europe that outline what kind of domestic legislation states have adopted to be in compliance with the Budapest Convention on Cybercrime will be analyzed through a deductive qualitative analysis (Kalmus et al. 2015) through the use of a codebook. While the existence and success of norm entrepreneurs engaging in local discourse will be measured binarly.

The selection of the cases of Estonia and Israel is strategic, as in regards to cyber security they share significant similarities, such as hostile and unfriendly neighbours. Causing them to invest significantly in cyber security both on a civilian and state levels. But they differ in their approach to international cyber norms and conventions, such as the Budapest Convention (2001). Which is referred to by the Council of Europe to be more than a legal document, it is considered to be a framework that permits hundreds of practitioners from Parties to share experience and create relationships facilitating cooperation in specific cases of cybercrime, including in emergency situations, enabling the fight against cybercrime to go beyond the specific provisions foreseen in this Convention. Although this thesis adheres to the specific provisions outlined in the convention, it is important to acknowledge its potential for more than just what it already has outlined.

The thesis will firstly outline the theoretical background in order to create a shared understanding of what norms are, how they function and how we distinguish between diffusion, localization and internalization. As well as tying all of this to the specific features of cyber. Leading us to the methodological section which outlines the research design and specific methods used for extracting data for analysis. The analysis section itself will be divided into three different sections allowing us to analyze how the provisions of the Budapest Convention have been localized in both Estonia and Israel. The section will cover the norm entrepeneurs, law and implementation in accordance with the theoretical and methodological assumptions established beforehand. Next section will outline the findings of the analytical section and discuss the results which analysis provided. Lastly the thesis will end with a conclusion where the most important aspects of this thesis will be summarized.

2. Theoretical Framework: Norms and Norm Localization in World Politics

To answer how localization of the Budapest Convention varies, the framework will explore several key sub-questions: (1) What are norms, and what role do they play in shaping state behavior also in relation to cyber norms; (2) What is norm localization, and how does it function. By addressing these questions, this chapter establishes the theoretical foundation necessary for analyzing variation in norm implementation. The insights gained from this framework will help identify potential causal mechanisms behind these differences, guiding the empirical analysis in the research section of this thesis.

2.1.What are Norms: a Constructivist Approach

Since the study is interested in norms and, more specifically, how norms diffuse and spread, constructivism and literature on norm diffusion and localization provides a fitting framework to study the localization of the Budapest Convention in Estonia and Israel. Constructivism in International Relations is characterized by three defining features: First, Wendt (1992) as well as Finnemore and Skkink (1998: 891) have argued that the constructivist theory rests on the assumption that ideational factors, such as ideals, norms and identities, play an important role in the formation of state behavior. Second, that actors within states are also constructed by shared ideas, not inherently given by nature. Third, that state's actions are linked to much more than material interests or power, but they also follow a "logic of appropriateness" (March & Olsen, 1998; Wendt, 1999). The logic of appropriateness is a term from the field of psychology used to refer to a mode of action where state's are not driven or motivated by self-interest but rather by a socially constructed idea of what is right (March & Olsen. 1989: 160–162). This idea has transferred into the realm of International Relations as the concept of appropriateness captures the constructivist understandings of norms and their dynamics. In the field of International Relations the more appropriate and therefore internalized a norm becomes to a state, both on the domestic and international level the stronger it becomes, as it becomes a part of the *status quo*. Together, these factors result in a perspective on international politics that emphasizes that state behaviour is mostly always norm-guided. The academic debate about what norms are or how to define them has been a significant one.

Although this thesis focuses specifically on international cyber norms, it is important to establish beforehand what the term “norms” even refers to. For example, Finnemore and Sikkink (1998: 891) define norms as “a standard of appropriate behavior for actors with a given identity”.

2.2 Norms and their Roles on the Example of Cyber Norms

Norms are not only something states absorb and internalize, they also have functions and are socially created in order to solve a problem or serve a function. Although there are two different functions to norms–regulative and constitutive. The difference between generative and constitutive norms stems from the fact that regulative norms do not create new rights or actors, but rather limit behaviour such as cybercrime or giving assistance to victims of cyberattacks or threats (Finnemore & Hollis. 2016: 440). This thesis will talk about regulative norms, per Finnemore & Sikkink's (1998: 891) definition of norms, which brings in the logic of appropriateness emphasized, which deems that a type of action is deemed either appropriate or inappropriate.

Norms in cyberspace essentially work like any other norms. Finnemore and Hollis. (2016: 427-428) argue that they should be understood as dynamic processes, rather than fixed “products” as they evolve through interactions among states, companies, civil society and multistakeholder coalitions. We can see this process for example in lobby work where states, companies and civil society all interact with each other in a context of a certain norm. But the action they take can be characterized as regulative as they create duties or obligations that prescribe, prohibit, or permit some activity or inactivity (Finnemore & Hollis. 2016: 440). For example, defining unauthorized access in domestic legislation or ascertaining how it is acceptable to extradite cybercriminals are types of regulative norms.

This leads us to how norms function in relation to cybercrime and cybersecurity. Norm functions, as Wendt (1999:111) mentioned, create a myriad of different actors and actions in the sphere of their interests. One kind of actors who are essential to cyber norm functions are “norm entrepreneurs”, due to the quick technological advancements influencing everything related to cyber. Although cyber norms, like any other norms, ultimately derive from theoretical societal frameworks, they also need to be promoted by entities to stay a subject of discourse in a fastly changing society (Huang & Madnick.. 2023: 206). Zwaolski and Kaunert

(2011) have labeled these entities “norm entrepreneurs”, which means they use various methods of persuasion to essentially “sell” a norm to a population. The success of these organisations is relative by case or case basis (Huang & Madnick. 2023: 206). Entrepreneurs in these cases can be NGOs, companies, lobby organisations; or even countries that can be considered “role models” as Tankard & Paluck (2016) points out. These entrepreneurs are an essential element in the cyber norms three-phase evolution model. The three-phases are, as Huang and Madnick (2023) have argued: (1) trial runs, (2) booming, and (3) decline. This means that cyber norms come and go quickly, strong and capable entrepreneurs help them stay a relevant part of discourse making them more likely to be adopted.

2.3 Norm Diffusion & Localization

Having established what norms are and what they do, the question becomes how they spread. As Huang & Madnick (2023) has noted, norm entrepreneurs play an important role in keeping them a relevant part of a domestic discourse, but to become an international norm, they have to spread - and be adopted/internalized by many states. This process has been called diffusion, which has been previously defined as: “transfer or transmission of objects, processes, ideas and information from one population or region to another" (Checkel. 1999: 85). Norms too can be the subject of diffusion meaning that they have spread from one state to another. But the diffusion of different norms does not inherently mean that these will be adopted into a national context. In order for state’s to adopt certain norms they will need to be adapted to fit the peculiarities of a state’s national context, like culture, religion, domestic practices. The process of this adaptation is called localization.

In any discussion about norm localization, we first need to define what norm localization is. Acharya (2004: 245) defines localization as “the active construction (through discourse, framing, grafting, and pruning) of foreign ideas by local actors, which results in the creation of locally legitimate and functionally appropriate norms.” Arguing with this definition that norm localization happens through the adoption and shaping of foreign ideas, including norms, into local domestic contexts. For example his concepts “grafting” and “pruning” are describing the process of modification of norms where states either add or discard elements of international norms to better align the local traditions and culture (Acharya. 2004: 243-248).

The successful localization of a norm is possible when certain conditions are met. Acharya (2004: 251) outlines a trajectory for localization and defines conditions for progress: (1) resistance and contestation of a norm, (2) willing and credible local actors, (3) grafting, pruning and existing norm hierarchy, (4) borrowing supplements to existing norm hierarchy. The first step of resistance and contestation means that aspects of existing normative order either stay strong or are being discredited which is necessary for localization to happen as an international norm has to be accepted in a domestic context and if there already is a strong norm then localization will not happen. But if the domestic norm is being rejected or contested, for example due to the norm's utility and applicability (Acharya. 2004: 251) it can be replaced by a stronger international norm. This is where willing and credible local actors, also referred to as norm entrepreneurs (Finnemore & Hollis. 2016; Huang & Madnick. 2023) come into play as they ensure that a norm is accepted, but according to Achyara (2004: 251) they must not be seen as outside forces but rather have a strong and reputable role in the state. Achyara (2004: 251) established that they borrow and frame external norms in a way that establishes their value to a local audience. Third condition argues that a norm will have to be adapted/modified or "grafted and pruned" to fit along the already existing norm hierarchy. Lastly, the fourth element of successful localization according to Achyara (2004: 251) is the possibility of incremental change. Meaning that the adoption of international norms should allow for local norms, already established in the hierarchy, to be modified and therefore offer then renewed possibilities for success.

But not all norms always localize, as there are some instances where conditions can not be met and there are exceptions. Acharya (2004: 245-246) also defines exceptions for localization like interplay of cultural congruence, institutional capacity, autonomy from external pressures, and the specific characteristics of the norms in question. These illustrate very well that localization is not always guaranteed and depends on much more than the willingness of local actors, like cultural specifications, political climate, and even the adaptability of the norm itself. To make an example, if a state already has strong norms that allow surveillance of devices and it is conducted on a regular basis, if a norm entrepreneur would start lobbying the ban of this it most likely won't succeeded as the norm that allows surveillance has not been contested and conditions for successful localization have not been met.

Both the conditions and exceptions for localization are important to understand in order to analyze the specific cases of cyber norm localization as it provides us with the necessary framework to understand how localization works and when it does not work. Furthermore, understanding the conditions and exceptions will allow us to uncover the mechanisms of localization at work, for example how domestic actors exercise their agency, how norms are strategically adapted, or how cultural and institutional factors either facilitate or hinder localization. This helps move beyond surface-level policy comparison and allows for a deeper understanding of how and if norms are firstly internalized and therefore localized in each case.

Furthermore, localization as a concept is far from a uniform phenomenon and can result in a range of different outcomes. The concept of norm diffusion has been analyzed based on three variations of outcomes–resistance, full adoption, or a decoupling of rules and practices (Zimmermann. 2016: 99-105). But this doesn't necessarily leave room for analysing the contemporary reality of states–norms are subject to constant part of a negotiating and renegotiating process, therefore the notion that states either commit or comply with a norm doesn't leave room for the complex processes of norm interpretation and translation (Zwingel. 2012: 12; Zimmermann. 2016: 102-104). Hence Zimmermann (2016: 105-106) proposes an approach which inturn should allow to distinguish different types of localization. She proposes three steps which help distinguish different types of localization: "(1) how norms are translated in discourse, (2) how they are translated into law, and (3) how they are translated into implementation" Zimmermann (2016: 105-106).

	Resistance		**Full adoption**
First step: translation into domestic discourse	Domestic frames and practices contest validity of norm set	Re-interpretation of global frames and practices, no contestation of validity	No contestation of validity, understanding of norm set in line with international community
Second step: translation into law	No adoption	Reshaping of norm set during adoption (leaving out /adding on/modifying)	Full adoption of international standards
Third step: translation into implementation	No implementation	Reshaping during implementation (leaving out/ adding on, modifying)	Full implementation

Figure 1: Zimmermann (2016: 106). Category System for Studying Norm Diffusion Results.

Zimmermann (2016: 106) finds localization to be more of a spectrum, seeing it as a three step process: translation into domestic discourse, translation into law, and translation into implementation. But also that each of these steps can have a varied level of adoption, running from resistance to full adoption, dividing it into a table where three possibilities are in direct correlation with one of the three steps. Taking the resistance column, the first step is translation into domestic discourse, Zimmermann (2016: 106) sees that if the norm's validity is contested by the state's frames and practices there will be no adoption and therefore also no implementation leading to a full resistance of the norm. The second column sees that the norm is not contested domestically but rather there is a re-interpretation of global norms which in the second step leads to a modification of the norm in the adoption process and ultimately leads to it also being reshaped during implementation. This leads to a middle ground, where norms are not fully resisted but at the same time fully also not adopted. The third column leads to full adoption of the norms, with there being no contestation of the norm's validity and international standards are fully adopted and implemented. The outcome of localization can differ. More precisely, it is not a dichotomy, but rather a spectrum as in Zimmermann's Figure 1. captures exceptionally well.

Finnemore and Hollis (2016) do not explicitly mention the term "localization", but scholars like Acharya (2004) and Zimmermann (2016) would describe their theory as localization. Finnemore and Hollis (2016: 457) argue that in order for cyber norms to become successful they need to be deeply adopted into local institutional, technical and cultural contexts. Therefore describing very clearly what can be seen in Figure 1 (Zimmermann. 2016: 106) as presented earlier. Zimmermann argued that norm localization takes place on a spectrum. Finnemore and Hollis's (2016: 457) characterization of successful norms requires them to be localized. For example, Zimmermann (2016) argues in her work that the validity of norms should not be contested in the first step of full adoption. Finnemore and Hollis (2016) also agree with this by saying norms should be deeply adopted in local culture. They use different words to essentially describe the me concept–localization. Therefore we can argue that cyber norm localization in principle should work by the same mechanism that regular norm localization does, as the main function of those norms is to solve problems on the local level. Local actors translate cyber norms, such as cyber crime, digital governance, cyber security etc, and adopt them into frameworks fit with local traditions, cultural expectations and

political priorities. Allowing for practical reliance and adherence to a larger international norm while still addressing unique localized challenges. Hence we can combine this knowledge gained from Achyara's (2004) literature, Finnemore and Hollis's (2016) theory on cyber norms with the Zimmermann's (2016: 106) system presented in Figure 1 and form clear-cut theoretical expectations concerning the variation in implementation of international cyber norms:

- Achyara (2004) laid out conditions and exceptions to localization, which is the first theoretical expectation we have: distinguishing if the conditions or expectations for the localization of a norm have been met.
- Which takes us to Zimmermann (2016), who outlines how we can distinguish three different types of localization: resistance, reinterpretation, and full adoption. Setting the second theoretical expectation.
- Thirdly, Finnemore & Hollis (2016) who specify how localization works exactly in regards to cyber norms.

3. Methodology

Research conducted in this thesis will take the form of a small-N comparative design of the Most Similar System Design (MSSD) type, a comparative method that examines two states with significant similarities in all cases except one due to which we can observe a difference in outcome (Anckar. 2007). This thesis focuses specifically on the implementation of the provisions outlined in the Budapest Convention on Cybercrime in the cases of Estonia and Israel, therefore it is a small-N comparative study, as a large-N comparative study would require a larger pool of case studies. This type of research design allows me to isolate the specific factor that varies across the two examples of localization and analyze what drives this variation. For conducting this research via the MSSD method requires that the cases being studied are different in regards to their dependent variable and similar in all potentially relevant independent variables except one. The dependent variable in this case will be norm localization as it is the subject of the research. We can determine this as both the states of Estonia and Israel have the ratified Budapest Convention which means localization of a sort has occurred but the central question of this thesis is to determine the exact degree/type of localization that has occured.

	IV- Discourse and norm entrepreneurs (Zimmermann. 2016)	IV- Harmonization with the convention (Zimmermann. 2016)	IV- Implementation of the norms	CV- Cyber threat amount (RIA. 2020 & INCD. 2020)	CV- Democracy indicator (Freedom House. 2020)	DV- Type of localization of the Budapest convention (Zimmermann. 2016)
Estonia	High	High	High	2722	94	Fully-adopted
Israel	High	Low	High	>9000	76	Reinterpreted

Figure 2. Comparative Research Method MSSD & Norm Localization (Ancker. 2007 & Zimmermann. 2016).

Figure 2. showcases the MSSD research method in terms of studying norm localization in accordance with Achyara's (2004) theoretical framework of necessary conditions for

localization and Zimmermann's (2016) framework on types of localization which formulate the independent variables in studying the variation of localization and what drives the differences in the two cases. The analysis will start with Achyara's condition and establish that they have been met, which means localization has occurred. Then the MSSD table will be operationalized to determine the type of localization.

When it comes to the sources, the thesis draws on a number of different sources that speak to the independent variables listed in Figure 2. The first part of the analysis will be measuring the independent variable "Norm entrepreneurs" and how they affect localization, this will be binary as each state has a lot of different norm entrepreneurs whose success is dependent on a case by case basis and measuring each one is not within the constraints of this thesis. The theoretical expectation is that norm entrepreneurs are "willing and capable" (Achyara. 2004: 251), this thesis will take the stance that if they exist and function they are willing and capable. This section will be reliant on public information on official sites and web pages aiming to outline the role of companies, civil society and NGOs in their role as norm entrepreneurs.

The second part of analysis measuring the independent variable titled "Harmonization with the Convention" which will analyze Zimmermann's (2016: 106) second step in what kind of localization has taken place, as portrayed in Figure 1. This part will rely on Council of Europe (2020a & 2020b) documents outlining how both Estonia's and Israel's specific domestic legislation corresponds with each provision of the Budapest Convention. The aim of this is to analyze how well harmonized are the acts of domestic legislation with the provisions of the Budapest Convention. The data necessary for this research is extracted in the form of deductive content analysis, as described by Kalmus et al. (2015). This method is well suited for testing theoretical concepts and frameworks through the systematic coding of

qualitative textual data based on pre-established categories.

Category of Code	Sub-code	Explanation	Example
Adoption	Full-alignment	The norm has been adopted as seen in the Budapest Convention.	The state is in full compliance or accordance with a provision of the Budapest Convention.
Reinterpretation	Partial adoption	The validity of the norm is not contested, but it has been reinterpreted and reshaped. Something has been left out, modified or added to the norm.	The state reserves the right not to comply with a provision of the Budapest Convention under certain conditions.
Rejection	Contestation of a norm	The validity of the norm is contested in the national context of the country. It's portrayed in a negative light or said to not fit the national contexts of a country.	The state does not comply with a certain provision of the Budapest Convention.

Figure 3. Codebook

To best operationalize this specific method of content analysis a codebook has been formulated based on Zimmermann's (2016) theoretical considerations of types of norm localizations which will allow us to research how each article of domestic legislation correlates with a corresponding article from the Budapest Convention. The codes establish that each article of domestic legislation falls on a spectrum of full-adoption, reinterpretation or rejection. Providing an article by article analysis of how well a convention has been localized in each state.

In regards to the third section of analysis, measuring the independent variable titled "Cybercrime Investigation Units" will be based on the previous analytical section, based on which we understand how the Budapest Convention should be implemented in the country. This section will map out who are the actual units dealing with cyber crime and this again will be binary, as it will measure the presence or absence of cybercrime investigation units. Sources this section draws on will be the Council of Europe (2020a & 2020b) documents as well as public information on official web pages outlining the presence and functions of these units.

Lastly, the control variables provided in the table are seemingly different. The two countries have vastly different amounts of cyber threat levels as demonstrated by incident numbers in 202, where Israel had over 9000 cases and Estonia 2722 cases. Another thing that also differs is their democracy indexes, where Estonia has the score of 94 and Israel 77. Both of these are variables that may affect the localization of the Budapest Convention, portraying its necessity in an environment with acute cyber threats but also motivation to align with international

conventions due to levels of democratic processes. Both of these in this scenario differ and are not capable of explaining the difference in outcome therefore and not supported by the theoretical framework of norm localization.

Today, the Budapest Convention is the only legally binding international convention on cybercrime (Välisministeerium. 2022). The findings from Estonia and Israel will provide insights into how and why states localize international cyber norms differently, contributing to broader discussions on cyber governance, norm diffusion, and security policy.

4. Analysis of the Localization of the Budapest Convention

The analysis will be divided into two sections one analyzing Estonia's case and another Israel's case. Both of these sections will include four smaller sections that will cover both the dependent and independent variables outlined in the methodology section. The Cybercrime Programme Office (C-PROC) of the Council of Europe in 2020 has created reports following the implementation of the Budapest Convention under national legislation. This is under their jurisdiction to follow as the Budapest Convention is under the Council of Europe and therefore subject to their reporting and follow up.

4.1 Estonia

Estonia signed the Budapest Convention on Cybercrime in 2004. In order to analyze the degree of localization we first and foremost need to confirm that localization as a concept has happened in this case. As previously mentioned, Acharya (2004: 251) set conditions for localization. Hence this section will analyze if Estonia has met those conditions. First, resistance and contestation of a norm, Estonia has not made any reservations pursuant to the convention, and method of analysis proved that no norms pertained in the Convention have been fully resisted. There however, have been Articles that are not fully adopted, and parts of them are contested. Such as, Article 7 relating to computer related forgery, which in Estonian legislation has been adopted under the criminalization of forgery overall, and is not explicitly computer related. The second partial contestation regards Article 20 and 21 which outline real-time data traffic, Estonia has not named a state based service provider, given that there are multiple.

Willing and credible local actors are the second important condition of norm localization. Estonia is known for an innovative cyber security industry, with almost all state based services being available online most governmental organizations deal with cybersecurity pertaining to their field (Invest in Estonia. 2025). Third, “grafting and pruning” which means norms from the convention are not adopted as is, but are fitted to the local context. Estonia has adopted the norms in the Budapest Convention almost directly, yet still localization has occurred. For example, Estonia in the cases of Article 7 of the Convention which speaks to computer-related forgery has not adopted legislation that explicitly mentions computer data or digital documents. Except § 344, § 345, and § 347 talk about forgery of documents overall. In Estonia’s case the explicit mention of computer data or digital documents is not needed, as documents in paper format do not exist or are very rare. Hence the norm presented in Article 7 has been pruned to fit into Estonia’s local context. Fourth condition: borrowing supplements to existing norm hierarchy. Estonia has done this in regards to Article 24 outlining extradition conditions for cybercriminals. Estonia made a declaration regarding this article, that if a bilateral treaty does not exist the Budapest Convention will be used as legal basis for extradition. This means placing it in this instance further in norm hierarchy than other existing norms regarding extradition. Hence a supplement to a norm has been established based on this Convention.

Overall this has allowed us to establish that localization of the Budapest Convention has occurred. Norms have been at least partially contested, credible and willing actors exist within the state, some norms have been pruned to fit the local conditions and there are cases of borrowing supplements to existing norm hierarchy.

4.1.1 Type of Localization

First step of the analysis is to measure the degree of localization or the dependent variable; this will be measured as stated in the methodology section by firstly analyzing the Council of Europe document that oversees what kind of domestic legislation a state has adopted and how well it reflects the provisions of the Budapest Convention. This is done via the use of deductive content analysis via the predetermined codes outlined in the codebook.

Article 1 of the Budapest Convention defines terms used in the convention, terms such as “computer system”, “computer data”, “service provider”, “traffic data”, which are directly applicable to Estonia's national legislation, as the terms used in specific provisions of Estonia’s domestic legislation use the exact same terms. Article 2 of the Budapest Convention seeks that states adopt legislation that defines illegal access, states may add a definition of intent, Article 3 regards illegal interception and surveillance, and Article 4 in the Convention targets any kind of unauthorized access. Article 5 and 6 set legislation criteria for system interference and misuse of devices, respectively. Application of the method of analysis showed that Estonia’s domestic legislation provisions outlining illegal access (§ 217), unauthorized surveillance (§ 137), interference with computer data (§ 206), hindering functions of computer systems (§ 207), and preparation of computer related crime (§ 216) meet the criteria for domestic legislation set Budapest Convention for all of the Article 2-6.
Article 7 states that “/…/when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible./…/”

There is a larger question at hand here, as Article 7 states there must be a law speaking specifically to computer data, the subsequent law for Estonia has been marked as § 344, § 345 and § 347 which outline the use of counterfeit documents. Method of analysis shows that these concrete paragraphs do not specifically speak to forgery in the digital space, but rather of documents in a more broad sense. Article 7 explicitly mentions the need for domestic legislation that targets the “alteration, deletion, or suppression of computer data”. Method of analysis finds that Estonia’s corresponding paragraph does not address this explicitly, but due to the nature of documentation and e-governance in Estonia the forgery of documents other than digital is rare, therefore courts or prosecution may argue that these paragraphs apply in this regard. Using the method of analysis we can determine that the norm portrayed in Article 7 has been modified. Zimmermann (2016 :106) referred to the modification of norms in the adopment stage as adding or leaving something out that in the original norm is there. Method of analysis determined that context regarding computer data was left out of Estonia’s domestic legislation yet the making or use of counterfeit documents is still illegal. Hence we can determine that In terms of localization of the Budapest Convention, the norm portrayed in Article 7 has been modified.

Furthermore, Articles 8-13 of the Budapest Convention are fully adopted into Estonian domestic legislation, there's no declarations or reservations made about these Acts and the domestic legislation provided for comparison to the convention, fills all the necessary requirements and criteria. Although for Article 13, that seeks the proper sanctions and measures for cybercrimes, nothing has been mentioned in the subsequent "domestic legislation" section, the method of analysis showed that corresponding legislation has been previously forecasted together with each domestic law as punishment and procedure for these crimes is reflected in the corresponding legislation itself. The method of analysis showed that Estonia in regards to Articles of the convention, such as 2 (illegal access), 4 (data interference), 5 (system interference), 8 (computer-related fraud) make explicit distinctions in punishment of the crime when it is a) committed by a legal person b) a group or c) a repeat offender, in paragraphs § 217 (illegal access), § 137 (unauthorized surveillance), § 206 (interference with computer data), § 207 (hindering functions of computer systems), and § 216 (preparation of computer related crime). Establishing that Articles 12 and 13 are adopted in Estonian legislation.

Section 2 of the Convention outlines procedural law that member states need to follow to comply with the convention. Articles 14 and 15 are about the scope of procedural provisions and safeguards, method of analysis show that Estonia has adopted these articles. Article 14 asks that member states employ legislation that allows for the necessary powers and procedures for the specific criminal investigations or proceedings. Estonia has adopted this norm as demonstrated by § 32 and § 215 which outline the powers of investigative bodies in criminal proceedings and obligations they bear in criminal proceedings, respectively. Secondly, regarding safeguards outlined in Article 15 which is mostly regarded as adherence to the Declaration of Human Rights, which Estonia complies with on an international level by the promotion of Human Rights and on a domestic level by courts, the Chancellor of Justice or the Gender Equality and Equal Treatment Commissioner can also be addressed for the protection of one's rights, as well as through several civil society organisations that work in protection of people's rights and freedoms (Eesti.ee. 2025).

Articles 16-19 seeks that member states have domestic legislation in order to preserve, extract, search and seize computer data for the purposes of criminal proceedings, method of analysis showed that Estonia has outlined these conditions in the following legal acts: § 32, § 215, § 90, ECA § 91, ECA § 102, ECA § 111, ECA § 112. These paragraphs outline the

powers and procedures of respective organs in criminal proceedings involving computer data, extracting data, degree and timeframe of compliance with the authorities that person(s) are required to adhere to, the protection of seized data and its preservation, respectively. As well as the obligation of the state to provide necessary information to the person(s) involved. In regards to Articles 20 and 21 of the convention which specify the member state's ability to real-time collection and interception of data traffic, method of analysis regards that Estonia is in compliance with them, although § 126 providing legal capability for real-time data traffic does not explicitly name a service provider, nor is it done in declarations made during the Budapest Convention. There are several different service providers in Estonia (e.g. Telia, Elisa, Tele 2) and therefore the law must sustain its adaptability to the principle's of the free market. Article 22 the Convention speaks to the jurisdiction of which each member state must operate in, Estonia has defined its jurisdiction it operates in, in §6 (territorial applicability of the penal law), §7 (applicability of penal law by reason of person concerned), §8 (applicability of penal law to acts against internationally protected legal rights), and §9 (applicability of penal law to acts against legal rights of Estonia) which according to the method of analysis is in correlation with the Budapest Convention's Article 22 and therefore we can determine that the norm portrayed has been fully adopted into Estonia's domestic legislation.

Moreover, according to the method of analysis Estonia has fully adopted, implemented and even gone beyond in regards to Article 24 which outlines extradition conditions for cybercriminals. Estonia has declared that when no bilateral extradition treaty exists they will use the Budapest Convention's Article 24 as legal basis for extraditing criminals. (WIPO. 2010). The Budapest Convention seeks that state's adopt domestic legislation in accordance with the criteria each Article of the Convention sets, not necessarily that states need to adhere to every single Article as is written, which is what Estonia has chosen to do in the case of Article 24 provided that no bilateral treaties exist.

Articles 25 and 26 of the Convention outline conditions for mutual assistance and spontaneous information. Analytical approach concludes that Estonia has fully adopted the provisions in the Articles 25 and 26, as the subsequent domestic legislation facilitates a wide range of cooperation, urgency of situations and complies with dual criminality and refusal limitation processes. Regarding Article 27, Estonia has made a declaration that in the absence of an extradition treaty, the authority responsible for making or receiving requests for

provisional arrests is the Ministry of Justice, as well as the central authority responsible for sending, answering and executing requests of mutual assistance (WIPO. 2010). Hence the method of analysis showcases that the conditions set out in the Convention have been met and the Article adopted.

Article 29 and 30 outline the guidelines for member states to expedite the preservation of stored computer data, although Estonia's domestic legislation § 464 does not follow the Budapest Convention word-for-word it has a very similar intention. Key differences between provisions are outlined in the handling of preservation only requests, as Estonia does not have exact legislation regarding this but it belongs under the jurisdiction of the Ministry of Justice as they have the right to act self-executively or it would fall under principles of general international cooperation. Article 30 adds a nuance to this discussion as it does not directly change preservation, but the line of communication needs to be visible if the involvement of another state's service provider is revealed to be involved, as it needs to be in line with international cooperation standards. This is exactly outlined in Article 31 which Estonia's § 464 is in correlation with. Article 33-35 in regards to mutual assistance in collected data traffic, content data and data interception is fully adopted as demonstrated by § 462, § 463 and § 464 in domestic legislation, which outline the criteria for receiving mutual aid from the Estonian government, also applicable for incidents happening in cyberspace. Article 35 is also fully adopted with a law ratifying the convention and with a declaration specifying that 24/7 network support will be provided by the Estonian Police and Border Guard Board.

Overall, the Budapest Convention is very well harmonized with Estonia's domestic legislation, as per the previously established methodological considerations. There are 30 norms adopted out of 35. This illustrates a strong adherence and adoption of the norms outlined in the Budapest Convention. Domestic legislation has been specified to include legal persons or crimes organized by groups, which the Budapest Convention does not explicitly deem as necessary but in this regard the Convention is also vague and does not set a norm on how states should deal with groups or legal persons, instead language such as "states should adopt legislation…" is used. Which leaves room for interpretation but need for specification for conducting domestic legislation. The provisions in the convention and national legislation are in some cases almost comparable word-for-word, for example as seen in Article 1. There are a few minor provisions that according to Zimmermann's (2016) theory count as reinterpretations of a norm as relevant institutions handling a process have been left

out of the legislation, but no Estonia has not used their right to apply reservations in adhering with the convention, instead in cases where bilateral agreements are not in place Article 24 is used as a legal basis for extradition.

4.1.2 Norm Entrepreneurs

As established in the theory section of this thesis, norm localization is highly dependent on the success of a norm in domestic discourse and is driven by entities often referred to as norm entrepreneurs (Acyara. 2004; Huang & Madnick. 2023; Zimmermann. 2016). This analytical section of the thesis attempts to map out the presence of these willing and capable norm entrepreneurs in Estonia, as they are a key element in successful norm localization. This section will try to establish whether or not they exist within the national discourse. The norms presented in the Budapest Convention are very closely tied to the work of these national institutions, hence this is important in the context of this thesis.

The Ministry of Foreign Affairs can be regarded as a "norm entrepreneur" due to diplomacy's inherent nature of promoting the norms mainly involved in a state on an international level. Their focus is in cyber governance through "cyber diplomacy", and according to the Estonian Ministry of Foreign Affairs cyber diplomacy focuses on state behaviour in cyberspace, especially regarding the norms, principles and values that apply there (Välisministeerium. 2024). Moreover, their cyber diplomats are focusing on protecting free and open internet and fighting cybercrime on an international level (Välisministeerium. 2024). Although the direct activities of the Ministry of Foreign Affairs are directed at the international community, it has an indirect effect as a norm entrepreneur also on the domestic community, as Estonia's success and reputation on the international field is something that has inspired domestic actors to form and act in this regard. Method of analysis proved that this norm entrepreneur is relevant as it is responsible for the implementation of Article 23 covering international cooperation, Article 24 covering extradition in regards to diplomatic countries held with other states (although method of analysis proved that the act of extraditing a cybercriminal falls under the Ministry of Justice). As well, as Articles 25-27 as they outline mutual assistance where the Ministry of Foreign Affairs in some instances may play an important role in facilitating diplomatic discussions pertaining to sensitive issues.

Another norm entrepreneur is NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE), which was formed by Estonia's proposal, as they saw a growing need for cooperation regarding cyber threats in the alliance. Although Estonia themselves acted as a norm entrepreneur in creating this institution, the contemporary existence of it is something that not only guides norm localization in Estonia, but in norms in NATO as a whole making it a norm entrepreneur. They have defined their key focus areas to be technology, law, research, training, strategy and operations (NATO CCDCOE. 2025). The existence of this institution in Estonia is important in the context of the Budapest Convention through Articles 25-27 that outline the conditions of mutual assistance in the cases of cybercrime. This is important both in cooperation between the NATO member states as well as their bilateral relations with third countries.

Other norm entrepreneurs in Estonia are mostly companies, most of which combine both technological aspects of cybersecurity and cybersecurity policy within the country. Technological cybersecurity can be understood as companies and research institutions that develop mainly technical solutions in cyberspace, everything from fire-walls, two factor authentication and defence capabilities within the actual cyberspace. When referencing the term "norm entrepreneurs" can talk about specific institutions like Universities and their institutes specifically tuned to cybersecurity research and development (e.g. TalTech, University of Tartu etc), but also companies like Cybernetica, NEVERHACK or SECNORA who amongst research also develop practical and technological solutions for ensuring cybersecurity. In Estonia there are approximately 10 different companies, with physical locations, that deal with providing cybersecurity related services. These norm entrepreneurs however do not only deal with technological aspects of cybersecurity, there are also actors that deal with cybersecurity policy. These entrepreneurs pertain to the provisions of the Budapest Convention indirectly as they can not directly influence their adoption but rather be focus on the lobby and advocacy side of cyber norm implementation. Estonia has a very specific culture and habit of governmental institutions including different interest groups in formulation of legislation, which is referred to as involvement in good faith (*hea kaasamise tava*) (Riigiteataja. 2011). Meaning if and when there is a proposed amendment for a law regarding cybersecurity relevant stakeholders will be invited by the Ministry enacting said change to propose their ideas, issues and positions to ensure the amendment's relevance in a field.

Another norm entrepreneurs are think-tanks that talk about issues related to cyberspace regardless of what changes in legislation are taking place. For example, one of Estonia's leading think-tanks Praxis just published an analysis of Estonians cybersecure behaviour and what kind of effect it has (Praxis. 2025). This is important as these analyses are often referred to in policy or position papers presented to the government or Ministries regarding changes in legislation or current issues surrounding a topic. This is the least direct way of influencing the norms in the Budapest Convention themselves, but still important in mapping the existence of norm entrepreneurs as they offer evidence based analysis of the behaviours in cyber space while also shaping opinions on the topic.

In conclusion, Estonia has willing and capable actors or norm entrepreneurs (Acharya. 2004; Zimmermann. 2016; Huang & Madnick. 2023) within the field of cybersecurity, who keep cybersecurity relevant in the political agenda and formulate different levels of discussions around cyber policy and cybersecurity issues. This helps keep the discourse diverse and relevant which is important in the localization of conventions that involve a number of different norms, such as the Budapest Convention on Cybercrime.

4.1.3 Cybercrime Investigation Units

This analytical section attempts to measure the cybercrime investigation units in Estonia and how their work reflects the Articles of the Budapest Convention. The outcome of this independent variable will be binary. This section will directly speak to how Estonia is implementing the Budapest Convention.

The field of cybersecurity in Estonia mostly belongs under the jurisdiction of the Ministry of Justice and Digital Affairs. In 2009 a cybersecurity council was formed next to the Government's security council, the main job of this newly established council was to increase cooperation among government institutions in terms of cybersecurity, this council is run by the chancellor of the Ministry of Economic Affairs and Communication (Justiits- ja Digiministeerium. 2025). The Ministry of Justice and Digital Affairs is also responsible for enacting domestic legislation that provides frameworks for fighting cybercrime on a national level, they coordinate with international partners and information security partners, ensuring that cybersecurity on a state level is up to standards and capable of responding and dealing

with incidents and create strategy papers that allow for a clear and focused development in the cybersecurity field (Justiits- ja Digiministeerium. 2025). They are directly linked to the Budapest Convention, as the method of analysis shows that Article 24 outlining extradition of cybercriminals is directly in the ministry's jurisdiction. As well as being responsible for the requests of mutual assistance outlined in Article 27.

The Information System Authority (NCSC) is responsible mainly for cybersecurity in the field of critical infrastructure and public domain and is a specific agency under the Ministry of Economic Affairs and Communication. They in most cases of cybercrime or a cyberattack are a person's, companies or institutions second contact (after the police) when there has been a case of hacking, phishing etc; mostly operating through the CERT-EE program, they regularly monitor cyberspace, respond to attacks and mitigate potential risks. NCSC is also responsible for the National Coordination Center (NCC-EE), the goal of this institution is to "promote the development of the Estonian and European cyber security industry, technology, and research" (RIA. 2025). The activities this institution engages in are directly linked to Article 35 per the method of analysis, as this Article facilitates the possibility of a 24/7 network .

The Ministry of Defence mainly works in the field of cybersecurity through their institution CR14 which goal is to advance research and development, international cooperation, cybersecurity training and providing cybersecurity services and consulting (Kaitseministeerium. 2025). What distinguishes them from a "norm entrepreneur" is that they are not as visible and outspoken in the public sphere, but rather focus on providing services and consulting in regards to cybersecurity. Due to the nature of cyberspace and malignant softwares "providing services" more likely than not means that they also detect and protect against cyberattacks or cybercrime. Overall there are three different organizations whose exact job is information security in Estonia, this also includes protection of said information in cyberspace–Estonian Foreign Intelligence Unit, Internal Security Service and the Intelligence Service of the National Defence Forces. They deal with both classified information and not classified information and its security.

4.2 Israel

To answer if localization of the Convention has occurred in Israel, they need to meet Achyara's (2004: 251) four conditions for localization. First, resistance and contestation of a norm, there are many norms in this Convention in regards to which Israel has made reservations to and partially or fully contests them. Such as, Article 6 (misuse of devices), Article 9 (child pornography), (Article 10 (copyright), Article 14 (procedural provisions), Article 22, (jurisdiction), Article 29 (preservation of computer data) are partially contested (WIPO. 2010). Meaning that some norms from these Articles have been adopted, and some have been resisted. Second, willing and credible local actors, according to Startup National Central (2025) Israel has over 500 companies pertaining to the field of cybersecurity, some of which have unionized and have gathered under umbrella organisations. This indicated that there are many willing and credible actors in Israel that drive the discourse around cyber security and cybercrime. As well, there exist state based organisations such as the National Cyber Directorate (2025) who also form strategy and policy papers contributing to discourse. Third, "grafting and pruning", in the case of Israel, "pruning" can be illustrated by Israel's complete ban of any unauthorized access whilst the Convention askes that states that states must adopt legislation that bans unauthorized access with the definition of intent as stated in Article 2, Israel has banned all kind of unauthorized access, regardless of intent. Meaning that this part has been left out of the domestic legislation. Fourth, borrowing supplements to existing norm hierarchy have been mainly used in regards to cooperation between states in fighting cybercrime, as Israel prior to aceeding to the Convention did not have as clear of a framework and in this regard they find it important (UNODC. 2022). Hence, from this we can conclude that Israel has localized the Budapest Convention.

4.2.1 Type of Localization

Article 2 of the Budapest Convention seeks that states adopt legislation that defines illegal access, states may add a definition of intent. While Estonia has in their national legislation clearly defined that criminality is tied to ill intent, Israel on the other hand has taken a much broader approach to this. While both the Budapest Convention and the Israeli Compusters Law are meant to combat unauthorized access, Israeli law criminalized any kind of unauthorized access without regard for security measures or intent (Legal Portal for Internet, Cyber and Information Technologies. 2015).

Article 4 has been compared to Israeli Computer Law (1995), specifically Article 2(2). While article 4 in the Convention targets any kind of unauthorized access, regardless if there are any disruptions or alterations, the Israeli Computer Law Article 2(2) does not target unauthorized access unless alterations or disruptions have occurred (Library of Congress. 2020). Since unauthorized access is criminalized regardless of alterations, this Article 2(2) only makes the domestic legislation stronger as it prevents people from "testing the water" by gaining unauthorized access. The same is with Article 2(1) of the Computer Law (UCI), which has been compared to Article 5 from the Convention, although it is based on the same principle as the Convention's article in practice it goes further, criminalizing any kind of unauthorized interference. Hence the method of analysis tells us that the norm has not been contested on a national level, but in practice it has been modified, specifically in the sense that it has been made stricter than the Convention seeks.

Article 6 of the Budapest Convention outlines that states must adopt legislation that establishes what kind of misuse of a device can be considered criminal offences. Regarding this provision of the Convention, the State of Israel: "has reserved the right not to apply paragraphs 1(a)(i) and 1(a)(ii) when the offence concerns procurement for use or import and paragraph 1(b), regarding the possession of items designated in paragraph (1)(a)(ii)." According to the method of analysis, this essentially means that these norms from the convention are partially adopted because they do not directly align with domestic legislation. Article 6 in the Convention emphasises the importance of establishing passwords and security mechanisms in order to prevent unauthorized access, but Israeli Computers Law (1995) criminalizes any kind of unauthorized access, regardless of the security mechanisms in place. In addition to these reservations, Israel's Computer Act of (1995), specifically provisions 6a-c are compared to Budapest Convention's Article 6.

Moreover, Article 7 of the Budapest Convention requires states to adopt legislation that seriously hinders unauthorized interference, Israel's legislation outright criminalizes it and therefore we can consider this norm to be fully adopted, as criminalizing something is the most serious way to hinder the crime from being committed. Moving on with Article 8 which is a step further from Article 7, and seeks the criminalization of intentional and unauthorized input, alteration, deletion or suppression of computer data. Israel has adopted the norm in this concrete provision of the convention, but does it combining two different laws–Article 2 to the Israeli Computer Act, alongside Article 415 to the Israeli Penal Law (1977). Article 2 to

the Israeli Computers Law bans unauthorized access (WIPO. 1995), while the Israeli Penal Law Article 415 criminalizes obtaining any kind of benefits by means of fraudulent activity (International Commission of Jurists. 2013: 125).

Article 9 of the convention seeks that member states criminalize the production, distribution, distribution and posession of child ponography. Israel has made several reservations to this article while acceding to the convention. The reservations concern provisions 1(d) and 2(b) of Article 9, which attempt to limit the procurement of child pornography through computer systems; and visual depictions of a person appearing to be a minor engaging in sexually explicit acts. The latter reservation is applicable in cases involving the production and possession of sexually explicit material. Israel's reservation in this instance is worded as follows: "The State of Israel has reserved the right not to apply paragraph 2(b) regarding the offences in paragraphs 1(a) and 1(e)." Essentially meaning that Israel is not obligated to criminalize the production or possession of sexually explicit material depicting a person who appears to be a minor, unless they can prove that the person is a minor. Although Israel has criminalized the production of child ponography through Penal Law Article 214 (b1), there is no legal mechanism that addresses specifically offenses committed through computer systems, like distribution or access. Therefore the method of analysis showcases that Israel has not fully adopted the norms in Article 9, as important aspects of said norm have been left out in the domestic legislation.

Furthermore, Article 10 regards copyright infringements which Israel has made reservations to, considering their membership in the TRIPS agreement. Article 10 of the convention attempts to criminalize any online copyright infringements. TRIPS agreement through Article 61, however limits this to only commercial infringements (WTO. 1994). Hence, the method of analysis concludes that Israel has not fully adopted the norm from Article 10, as the scope of the agreements is different. Article 11, establishing that states need to adopt legislation criminalizing aiding and abetting, or attempted aiding and abetting is fully adopted in Israel, as method of analysis showed that this is reflected by Articles 25 (attempt), 31 (accessory), 32 (penalty for accessory) and 34D (accomplices) in the Israeli Penal Law (ICJ. 2013: 9-11). Articles 12 and 13, regarding corporate liability and punishments for criminal activity, respectively, are according to the method of analysis aligned with the Budapest Convention as they are reflected in each domestic legislation. Article 14 outlining the scope of procedural provisions is partially adopted in Israel, as it regards the adoption of powers and procedures

to prosecute crimes layed out in the convention, but as Israel has previously set reservations to certain provisions this article. Therefore the method of analysis shows that it has not not been adopted to its full extent.

Regarding Articles 16-19 which are being compared to the Israeli Criminal Procedure Law 5768-2007, this thesis is unavailable to analyze the harmonization of the law at hand with the convention as full texts of this data are not available online or in person. Article 20 of the convention has been adopted in Israeli domestic legislation via the Communications Law 5742-1982 Article 13(b)(2) which deems that telecommunications data must be made available for national security or public peace reasonings in consultations with the Minister or Prime Minister (WIPO.) Article 21 has been compared to the Israeli Wiretap Law of 1979, which is mostly aligned with the Budapest Convention, as it provides mechanisms for interception of content data for criminal proceedings. Said act has both judicial and governmental oversight and is therefore aligned with the convention. But Article 20 of the Budapest Convention is not fully adopted in Israel, as they have made reservations regarding what constitutes as criminal, in this regard they deffer to Israeli Penal Law (1977), which was aforementioned in discussion around Article 9.

Article 22 outlining the jurisdiction of the previous Articles is adopted into domestic legislation with changes, as Israel requires dual criminality with the approval of the Attorney General, if the crime was committed abroad. Article 24 outlining extradition for cybercrimes is fully-adopted in domestic legislation, as Israeli Extradition Law (1954) states that all crimes punishable with one year or more of imprisonment are subject to extradition according to the analyzed document Article 25 is fully-adopted. Article 26 regarding mutual legal assistance is adopted in Israel's national legislation but it is specified that legal aid will be carried out in accordance with Israeli law (UN Office on Drugs and Crime. 2025). Article 29 is conditionally adopted, as there is a reservation regarding this. The state of Israel has reserved the right to refuse expediting the preservation of computer data in cases where they deem that the criteria for dual criminality can not be fulfilled. Which means the applicability of Article 29 partially contested and is applicable only on a case-by-case basis.

There are a handful of Articles in regards to which Israel has adopted no domestic legislation, nor made any reservations about. Therefore these provisions of the Budapest Convention are not adopted and not localized. Estonia on the other hand has adopted every article from the

convention. Overall, Israel has presented a complex picture of the adopment of the norms in the Convention, where some norms at the same time have partially been rejected and another sub-section of the same norm fully adopted. Of the norms where analysis was possible, the method of analysis showed that 9 Articles have been fully adopted, 7 reinterpreted/modified. 5 Articles present a more complex picture of one norm from the article being adopted, another modified or rejected, or even a combination of all three.

4.2.2 Norm Entrepeneurs

Israel's main norm entrepreneur on the governmental level is the National Cyber Directorate, which also due to their list of tasks doubles as one of their investigation units. The main tasks associated with being a norm entrepreneur within the state are resilience, innovation leadership, institutional posture, strategy and policy formation (Israeli National Cyber Directorate. 2025). On their webpage they keep a section titled "CVE Advisories" which includes a regularly updated list of known code or computer vulnerabilities that cybercriminals may exploit, and recommend that organizations regularly check said list to keep up to date with inorder to avoid falling victim to a cybercrime.

Israel also has an extensive civil society side of cyber norm entrepreneurs. Startup National Central (2025) analyzed the Israeli cybersecurity market and concluded that there are 500+ companies, whom all benefit from Israel's deeply integrated academic, governmental, and industry collaboration. Together these companies raised $3.8 billion dollars in funding (Startup National Central. 2025). Around 200 cybersecurity and defence companies and organisations are gathered under the Israeli Security Business Organisation, whom they advocate for in the Israeli Parliament (Knesset) (ISBU. 2025). According to the ISBU's map of security companies in Israel, there are at least 18 companies who explicitly deal with cybersecurity, but also around 35 organisations that offer intelligence and surveillance services, making them relevant here under norm entrepreneurs as the Budapest Convention attempts to limit the kind of online surveillance methods that are allowed.

Figure 4 & 5 Cybersecurity, Intelligence and Surveillance companies in Israel (ISBU. 2025)

The cyber organizations are divided into two main types–organizations that are strictly related to cybersecurity and companies that offer intelligence and surveillance services and technologies, as seen in Figures 4 and 5. There is a quite large number of service providers.

To conclude, Israel has many companies, institutions and lobby organizations that are focusing on cybersecurity. Hence, through the method of analysis we can say that Zimmermann's (2016), Achyara's (2004) and Mandick et al's (2024) condition of willing and capable actors or otherwise known as norm entrepreneurs is fulfilled. This means that the state has different actors who actively partake in discourse relating to cybersecurity and keep it relevant in policy formation processes, as well as in the local community, helping international norms become successfully localized.

4.2.3 Cybercrime Investigation Units

Similarly to Estonia and other states, Israel also has a Cyber Emergency Response Team (CERT), they are located under the jurisdiction of The Israel National Cyber Directorate, who is responsible for everything related to cyber defence in the civilian sphere (Israeli National Cyber Directorate. 2025). They double as a norm entrepreneur and an investigation unit, due to the tasks listed on their website. In their role as an investigation unit they prevent, detect, identify and respond to cyber attacks, including creating a strategy for effectively achieving these tasks (Israeli National Cyber Directorate. 2025). Which means they both act as a proactive body shaping cyber defence but also act as a rapid-response unit to different incidents in cyberspace. This means they are directly linked to the Budapest Convention

through Article 35 pertaining to 24/7 network, as CERT offers 24/7 support for instances of cybercrime.

Other cybercrime investigation units are for example, Lahav 433, whose role it is to handle complex criminal investigations like hacking, identity theft etc. The organisation is under the jurisdiction of the Israeli Police. Which has a specific sub-unit Police Unit 105 which deals with the protection of children in online spaces (Child Protection Bureau. 2025). This is directly related to the Budapest Convention as firstly, Israel delegates tasks to the Police in regards to obligations stemming from the convention. Like the protection of children in online spaces. As the Budapest Convention in Article 9 has required states to adopt domestic legislation that criminalizes child pornography, Lahav 433 through the work of Police Unit 105 is directly linked to the implementation of the Budapest Convention. They are also explicitly named to be the competent authority in regards to Article 35, as they operate 24/7 (WIPO. 2010).

Unit 8200 has a more militaristic side of a cybercrime investigation unit and is a sub-organisation under the Israeli Defence Forces (IDF), it was established in 1948 and has developed from code interpretation. According to the IDF, the unit is their main intelligence and analysis unit (Israeli Defence Forces. 2021). Most of the work of this unit is classified and activities can range from signals intelligence to data mining and technological attacks and strikes (Reuters. 2024). Subsequently some have believed this unit to be behind the Stuxnet computer virus that was responsible for the physical damage done to an Iranian nuclear facility, the first known cyber attack to have real physical world implications, but this information has not been officially confirmed (Reuters. 2024). According to Tel Aviv they have started using AI technology to select Hamas targets (Reuters. 2024). But as their work is mostly classified there is not sufficient enough evidence to analyze how it pertains to the provisions of the Budapest Convention.

Overall, Israel has cybercrime investigation units that deal with implementing the norms outlined in the Budapest Convention. With CERT and LAHAV 433 investigating cybercrime that affects civilians, state institutions and companies. Hence the methodological condition for the existence of units that investigate cybercrime and therefore implement adopted legislation is fulfilled in Israel.

4.3 Discussion of Findings: Localization of the Budapest Convention on Cybercrime in Estonia and Israel

This comparative study set out to analyze how Estonia and Israel have localized the Budapest Convention on Cybercrime. Offering a theoretical framework that proposes a three dimensional framework for analyzing norm localization (Zimmermann. 2016). The findings reveal two distinct trajectories of norm localization, shaped by institutional, legal and cultural factors in each state.

While both states have adopted a fair share of Articles from the Budapest Convention on Cybercrime. Estonia presents a strong case of full adoption of international norms. The legal analyzis showcased that Estonia adopted 30 out of 35 provisions of the Convention. While the legal analysis showcased the existence of minor modifications in the adoption of Article 7, in computer-related forgery this can be understood in the theoretical context of Achyara's (2004: 251) concept of pruning to fit Estonia's highly digitalized governance structures. Israel in contrast demonstrates a clearcut pattern of reinterpretation (Zimmermann. 2016: 106). Onöy 9 norms from the convention were fully adopted without modifications or reservations, comparing this to Estonia's 32 we see a distinct difference. Importantly as well in several instances, Israel's domestic legislation either predates the Convention or rejects its provisions. Like in the domestic legislation pertaining copyright law or the criminalization of certain forms of child pornography. Hence we can conclude that Israel's accession to the Budapest Convention was rather selectively motivated by national priorities.

The presence of willing and capable norm entrepreneurs is clearly showcased in both states. Estonia's governmental agencies, companies and think-tanks are active in the field of cybersecurity. Israel meanwhile exhibits many different forms of cybersecurity firms, industry alliances and governmental bodies, which in 2025 reached over 500 organisations operating in this regard (Startup National Central. 2025). As such both states fulfill Zimmermann's (2016: 106) condition for the existence of capable and willing norm entrepreneurs who drive the cybersecurity discourse within a state. This gives us a good indication that both states might lean overall towards full-adoption of the convention, as there are entrepreneurs who drive the discourse pertaining that cybercrime and cyber security is important to the states.

Furthermore, Estonia and Israel both also exhibit high implementation capacity as their cyber investigation units actively work in the goal of preventing cybercrime, and in many cases directly deal with the norms outlined in the Budapest Convention. Fulfilling the third dimension of Zimmermann's (2016) localization types theory. This means that there is institutional capacity to implement the norms outlined in the Budapest Convention and adopted into domestic legislation.

Since the states have similar approaches to norm entrepreneurs and cybercrime investigation units, it means the difference in the variation of implementation comes from the translation into domestic legislation stage of Zimmermann's (2016) theory. This means that the main difference of the localization types between Estonia and Israel derive from the harmonization with the convention, as the domestic legislation adopted influences the type of localization a state exhibits. The legal aspect is something that also influences the work of norm entrepreneurs and cybercrime investigation units, as they have to follow the legal acts a state has adopted.

5. Conclusion

This thesis attempted to research what drives the variation of norm implementation of the Budapest Convention on Cybercrime in Estonia and Israel. Drawing on Acyara's (2004) and Zimmermann's (2016) theories on norm localization, establishing conditions and types of localization. Which concluded that there are four conditions that need to be fulfilled in order for localization to be possible: contestation of a norm, willing and credible local actors, grafting and pruning, supplements to local norm hierarchy (Acharya. 2004: 251). When localization has been established, we can go on to determine the type of localization, which according to Zimmermann (2016: 106) can manifest in three types: rejection, reinterpretation and full-adoption.

Th operationalize the theoretical section thesis employed a comparative analysis, specifically the MSSD research design to isolate key differences behind localization outcomes. Data from the documents was extracted using deductive qualitative analysis which preestablished codes for analyzing Council of Europe (2020a & 2020b) documents outlining exact provisions of domestic legislation are reflecting the norms of the Budapest Convention (2001).

The method of analysis showed that Estonia had adopted 30 out of 35 Articles of the Budapest Convention (2001), there is an active sphere of norm entrepreneurs and cybercrime investigation units exist and their work is related to the provisions of the Budapest Convention (2001). In the case of Israel the method of analysis showed that Israel has adopted 9 articles of the convention, the rest being rejected or reinterpreted or a combination of all three norms dependent on the subsection of an Article. There are many active norm entrepreneurs who partake in the discourse on cybersecurity and most cybercrime investigation units work with the provisions of the Convention, if their work is not classified. Hence, we can establish that the primary difference in the variation of implementation of the norms outlined in the Budapest Convention (2001) is dependent on the way states adopt the provisions into their national legislation. The finding based on the theoretical framework and methodological considerations showcased that Estonia demonstrates a type of localization referred to as full adoption, while Israel demonstrates a type called reinterpretation.

Ultimately, this thesis reinforces the idea that norm localization is not a uniform process, but rather involves negotiations which are shaped both by internal actos and legal tradition. The hypothesis proposed at the beginning of this thesis, that Estonia would exhibit a type of localization referred to as “full-adoption” and Israel type referred to “reinterpretation” is according to the result of the empirical section of this thesis true, as the method of analysis proved that is the type of localization they both exhibit. The research question of: what drives the variation of implementation of the norms from the Budapest Convention (2001) can be answered, as the method of analysis proved the variation is dependent on the domestic legislation each state employs. Any future research could expand this comparative analysis by either including additional countries or doing a deeper discourse analysis on norm entrepreneurs in both countries and the change of discourse over time to understand how exactly the internal norm entrepreneurs can influence the localization process.

7. References

Achyara, A. (2004) How Ideas Spread: Whose Norms Matter? Norm Localization and Institutional Change in Asian Regionalism. *International Organization*, Vol. 58, No. 2 (Spring, 2004), pp. 239-275 https://doi.org/10.1017/S0020818304582024

Anckar, C. (2007). On the Applicability of the Most Similar Systems Design and the Most Different Systems Design in Comparative Research. *Int. J. Social Research Methodology* Vol. 11, No. 5, December 2008, 389–40. DOI: 10.1080/13645570701401552

Checkel, JT. (1999) Norms, institutions, and national identity in contemporary Europe. International Studies Quarterly 43(1): 84–114.

Child Protection Bureau. (2025). https://www.gov.il/en/departments/units/operational_unit (retrieved 19th of May 2025).

Council of Europe. (2001) Budapest Convention on Cyber Crime. https://www.coe.int/en/web/cybercrime/the-budapest-convention (retrieved 19th of May 2025).

Council of Europe. (2020a). "Estonia Cybercrime legislation Domestic equivalent to the provisions of the Budapest Convention" https://rm.coe.int/octocom-legal-profile-estonia/16809e5982 (retrieved 19th of May 2025).

Council of Europe. (2020b). "Israel Cybercrime legislation Domestic equivalent to the provisions of the Budapest Convention" https://rm.coe.int/octocom-legal-profile-israel/16809e5783 (retrieved 19th of May 2025).

Communications Technologies for Criminal Purposes. Israel" https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Statements/Israel.pdf (retrieved 19th of May 2025).

Eesti.ee (2025) "Protection of Human Rights" https://www.eesti.ee/eraisik/en/artikkel/republic-of-estonia/human-rights/protection-of-human-rights (retrieved 19th of May 2025).

Even, S. & Siman-Tov, D. (2012) Chapter 4 Israel's Cyber Security Challenge. Cyber Warfare: Concepts and Strategic Trends, May. 1, 2012, pp. 75-84 https://www.jstor.org/stable/resrep08940.7

Finnemore, M., & Hollis, D. B. (2016). Constructing norms for global cybersecurity. The American Journal of International Law, 110(3), 425–479. https://doi.org/10.1017/s0002930000016894

Finnemore, M., & Sikkink, K. (1998). International norm dynamics and political change. International Organization, 52, 887–917. https://doi.org/10.1162/002081898550789

Huang, K., & Madnick, S. (2023). *The evolution of global cybersecurity norms in the digital age: A longitudinal study of the cybersecurity norm development process*. Journal of Cyber Policy, 8(1), 1-23. https://doi.org/10.1080/19393555.2023.2201482

Israeli Defence Forces. (2021). "Military Intelligence Directorate" https://www.idf.il/en/mini-sites/directorates/military-intelligence-directorate/military-intelligence-directorate/ (retrieved 19th of May 2025).

Invest in Estonia. (2025) "cyber security" https://investinestonia.com/business-opportunities/cyber-security/case-studies (retrieved 19th of May 2025).

Israeli National Cyber Directorate. (2025) https://www.gov.il/en/departments/israel_national_cyber_directorate/govil-landing-page (retrieved 19th of May 2025).

Israeli Security Business Organisation. (2025) "Who We Are?" https://www.isbunion.com/ (retrieved 19th of May 2025).

Israeli Security Business Organisation. (2025) "Map of Security Companies in Israel" https://www.isbunion.com/isbu-map (retrieved 19th of May 2025).

International Commission of Jurists. (2013) "Israeli Penal Law 1977" https://www.icj.org/wp-content/uploads/2013/05/Israel-Penal-Law-5737-1977-eng.pdf (retrieved 19th of May 2025).

Justiits- js Digiministeerium. (2025) "Riigi küberturvalisuse tagamine" https://www.justdigi.ee/digi-side-ja-kuber/riigi-kuberturvalisuse-tagamine (retrieved 19th of May 2025).

Kaitseministeerium. (2025) "Sihtasutus CR14" https://kaitseministeerium.ee/et/sihtasutus-cr14 (retrieved 19th of May 2025).

Kalmus et al. (2015) Kvalitatiivne sisuanalüüs. Tartu Ülikool https://samm.ut.ee/kvalitatiivne-sisuanalyys/

Legal Portal for Internet, Cyber and Information Technologies. (2015) "Israeli Supreme Court Determines What Is Considered Unlawful Intrusion to Computers" https://www.law.co.il/en/news/2015/12/18/IL-high-court-defines-unauthorized-access-to-computer/ (retrieved 19th of May 2025).

Library of Congress. (2020) https://maint.loc.gov/law/help/encrypted-communications/israel.php (retrieved 19th of May 2025).

March, J.G. & Olsen, J.P. (1998). "The institutional dynamics of international political order. International Organisations: 52(4): 943-969. DOI:10.1162/002081898550699

Majandus ja Kommunikatsiooni Ministeerium. (2024). "Riigi küberturvalisuse tagamine" https://www.mkm.ee/digiriik-ja-uhenduvus/kuberturvalisus/riigi-kuberturvalisuse-tagamine (retrieved 19th of May 2025).

NATO CCDOCE. (2025) "About Us" https://ccdcoe.org/about-us/ (retrieved 19th of May 2025).

Praxis. (2025) "Küberkäitumine" https://www.praxis.ee/tood/kyberkaitumine/?selected=p_2135 (retrieved 19th of May 2025).

Reuters. (2024). “What is Israel's secretive cyber warfare unit 8200?” https://www.reuters.com/world/middle-east/what-is-israels-secretive-cyber-warfare-unit-8200-2024-09-18/ (retrieved 19th of May 2025).

Riigiteataja. (2011). “Hea õigusloome ja normitehnika eeskiri” https://www.riigiteataja.ee/akt/129122011228 (retrieved 19th of May 2025).

RIA. (2025) https://www.ria.ee/ (retrieved 19th of May 2025).

Startup National Central. (2025) “Israeli Cyber Annual Insights and 2025 Trends” https://startupnationcentral.org/hub/blog/israeli-cyber-annual-insights-and-2025-trends/ (retrieved 19th of May 2025).

Tankard, M. E., & Paluck, E. L. (2016). Norm perception as a vehicle for social change. Social Issues and Policy Review, 10(1), 181–211. https://doi.org/10.1111/sipr.12022

UCI. “Computer Law” https://ics.uci.edu/~kobsa/privacy/israel.htm (retrieved 19th of May 2025).

UN Office on Drugs and Crime. (1998). “International Legal Assistance Law 5758-1998” https://sherloc.unodc.org/cld/document/isr/international_legal_assistance_law_5758-1998.html (retrieved 19th of May 2025).

UN Office on Drugs and Crime. “Computers Law, 1995” https://sherloc.unodc.org/cld/uploads/res/document/computer-law_html/Israel_Computers_Law_5755_1995.pdf (retrieved 19th of May 2025).

UNODC. (2022) “Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes.” https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Statements/Israel.pdf (retrieved 19th of May 2025).

Välisministeerium. 2022. “Fighting Cybercrime” https://vm.ee/en/activity/digital-and-cyber-diplomacy/fighting-cybercrime (retrieved 19th of May 2025).

Wendt A (1999) Social Theory of International Politics. Cambridge: Cambridge University Press.

Wendt, A . (1992). “Anarchy is what states make of it: The social construction of power politics. International Organisations: 46(2): 391-425.

World Bank. (2014) e-Estonia: The Making of An Information Age Society https://www.worldbank.org/en/events/2014/05/20/e-estonia-the-making-of-an-information-age-society (retrieved 19th of May 2025).

WIPO. (2010) “Convention on Cybercrime” https://www.wipo.int/wipolex/en/treaties/actions/952 (retrieved 19th of May 2025).

WTO. (1994) “Agreement on Trade-Related Aspects of Intellectual Property Rights” https://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm (retrieved 19th of May 2025).

WIPO. (1982) “Communications Law (Telecommunications and Broadcasting), 5742-1982, Israel” https://www.wipo.int/wipolex/en/legislation/details/15170 (retrieved 19th of May 2025).

WIPO. (1995) “Computers Law 1995” https://www.wipo.int/wipolex/en/legislation/details/15420 (retrieved 19th of May 2025).

Zimmermann, L. (2016) Same Same or Different? Norm Diffusion Between Resistance, Compliance, and Localization in Post-conflict States, INTERNATIONAL STUDIES PERSPECTIVES; FEB 2016, 17 1, p98-p115, 18p.

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina, Riin Suuster, (isikukood: 60308052715) annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose “Comparative Analysis of the Localization of International Cyber Norms: Estonia and Israel” (Võrdlev analüüs rahvusvaheliste kübernormide kohalikustamisest: Eesti ja Iisrael), mille juhendaja on Thomas Michael Linsenmaier,

1. reprodutseerimiseks säilitamise ja üldsUSele kättesaadavaks tegemise eesmärgil, sealhulgas digitaalarhiivi DSpace’is lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;

2. üldsUSele kättesaadavaks tegemiseks Tartu Ülikooli veebikeskkonna kaudu, sealhulgas digitaalarhiivi DSpace’i kaudu kuni autoriõigUSe kehtivUSe tähtaja lõppemiseni;

3. olen teadlik, et nimetatud õigUsed jäävad alles ka autorile;

4. kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid õigusi.

Riin Suuster

Tartu, 19.05.2025