TALLINN UNIVERSITY OF TECHNOLOGY
School of Business and Governance
Ragnar Nurkse Department of Innovation and Governance

Taavi Turu

The Role of Co-production in National Cyber Security and Cyber Resilience of Critical Infrastructures: the Case of Estonian Defence League's Cyber Unit

Master's Thesis
Programme Public Administration and Innovation

Supervisor: Prof Robert Krimmer. PhD
Co-supervisor: Gerli Aavik-Märtmaa, MA

Tallinn 2021

I hereby declare that I have compiled the thesis/paper (choose one) independently
and all works, important standpoints and data by other authors
have been properly referenced and the same paper
has not been previously presented for grading.
The document length is 17 181 words from the introduction to the end of conclusion.

Taavi Turu ……
(signature, date)
Student code: 132695HAAM
Student e-mail address: taavi.turu@gmail.com

Supervisor: Robert Krimmer, PhD:
The paper conforms to requirements in force

……
(signature, date)

Co-supervisor: Gerli Aavik-Märtmaa, MA:
The paper conforms to requirements in force

……
(signature, date)

Chairman of the Defence Committee:
Permitted to the defence

……
(name, signature, date) “ ..... “ 2021

ABSTRACT

Given the spread of ICT technologies into critical infrastructures and public services formerly isolated vital infrastructure, public services have become vulnerable to cyber threats. Cyber security of interconnected systems owned by private sector and public e-services has become crucial for society's day-to-day functioning and is a growing concern of national security. With the growth of internet users and online services, these threats are becoming more imminent. The purpose of the given master thesis is to explore how citizens can help to improve cyber security through enhancing the resilience of e-services and critical infrastructure vital to society. To answer the research question Four Co's of co-production are used to view different stages of resilience. Through analyzing these different co-production activities in different stages of resilience (plan, respond, recover and adapt), it can be concluded that citizens' role in improving national cyber security and enhancing cyber resilience has thus far been most visibly apparent in co-delivery activities in the resilience stages of respond and recover.

Keywords: critical (information) infrastructure, e-services, national cyber security, co-production, cyber resilience

Table of Contents

Introduction

Over the last three decades, the international community has witnessed an expansion of omnipresent information and communication technology (ICT) solutions. The digitalization of private and public services has allowed businesses and states to be more accessible and efficient. However, better connectivity for service users comes draws parallels vulnerabilities in the cybersphere. As operation systems of most of critical infrastructure heavily rely on ICT, the exploitation of cyber vulnerabilities, whether from accidents, natural disasters, attacks by criminals, terrorists, or foreign nations with malicious intent, poses the risk of considerable damage to countries, their citizens and private business. Although the majority of critical infrastructure is owned by the private sector, it has become evident that governments are responsible in ensuring necessary security precautions as part of the cyber security of their operations and their clients. (Harrop 2015, 166, Warfield 2012, 135)

In addition to natural disasters or systematic errors causing disturbances, developed countries have seen a surge in malicious cyber incidents. There is an urgency to improve protection of citizens, businesses and public institutions against these threats. The European Commission addressed the broad range of cyber security challenges including ransomware attacks, the rise in cyber-criminal activity and the increasing use of cyber tools by state actors to meet their geopolitical goals. (European Commission 2017) Publicly well-known cyber incidents, like cyber attacks against Estonia in 2007[1], Stuxnet[2] in 2010, NotPetya[3] in 2017, were arguably initiated by state actors. More frequently occurring high-profile cyber incidents have only intensified the already on-going trend among nations to invest in cyber capabilities.

There is a rising demand for cyber security specialists and IT technicians. States have shown the initiative in forming stronger ties with cyber security communities to fill the knowledge gap. Although, it is expected that in 2021 there are currently 3.5 million open cyber security positions, more than 2 million of these will be geo-located in the Asia-Pac region, and nearly 400,000 in Europe (Cybersecurity ventures, 2021). It has become increasingly evident that the private sector holds a strong competency and expertise in the sphere of cyber security and private-public partnerships are often used to bridge the knowledge gap and establish efficient

[1] Distributed denial of service (DDoS) attack against the Government of Estonia
[2] Elaborate worm discovered in 2010 that was targeted against Iranian nuclear reactors
[3] Global ransomware malware wave in 2017

co-operation as well as good networks with critical service providers. (Carr 2016, 44) Estonia is a vivid example of how a national cyber security crisis state received much needed help from private-sector cyber security specialists (Mansfield-Devine 2012). Although, this was not achieved solely by relying on public-private partnerships. The help came from informal cyber security community - specialists working in different private companies who volunteered to help. This case demonstrates how government agencies do not always have in-house expertise needed to respond to unexpected incidents in cyber space.

Through the theory of co-production and academic research on the national cyber security, this thesis concentrates on the potential roles that citizens may hold in enhancing national cyber security within critical infrastructure and e-services. This case study focuses on the role of Estonian Defence League's Cyber Unit (EDL CU) in the protection of critical information infrastructure and e-government services by considering two major cyber security crises that took place in Estonia in 2007 and 2017.This thesis looks at the potential of citizens with technical expertise and interest in the security of cyber systems to improve the cyber security of the public services and national security. By analysing the volunteers' role in governments' national cyber security, this thesis seeks to outline the potential threats and benefits of a more diversified national cyber security structure. The research question of this thesis is – **What is the citizens' role in improving the national cyber security for e-government services and critical infrastructures?**

The aim of this thesis is to explore and provide answers to the research question and as such is structured into five chapters. Chapter 1 outlines a short overview of the purpose of this thesis. Chapter 2 provides a theoretical overview of academic research on cyber security of critical infrastructures as a national security issue and co-production as a new way to use citizens' input to improve the quality of services. The theoretical framework described in Chapter 2 gives the structure for the later analysis. Research design and methodology is explained in Chapter 3 as the empirical part of this thesis, Chapter 4 describes the Estonian case including the cyber security policy initiatives aimed at improving co-production in the protection of critical information infrastructure and the e-government. The purpose of the chapter is to describe the implemented changes in response to the national security crises in 2007 and 2017 and developments in the overall cyber security environment. Chapter 5 uses the theoretical framework developed in Chapter 2 in a bid to answer the research question.

1. National cyber security and co-production – citizens' potential role in security of services and critical infrastructure

The following chapter provides an overview of theoretical literature regarding critical (information) infrastructure security, national cyber security management, and co-production. Academic literature highlights the growing importance of online services and critical information systems in modern states' national security (Luiijf 2015, Roege 2017). As more economic activities and services migrate to cyberspace it is assessed as states' responsibilities to protect their citizens from potential cyber threats causing disturbances to day-to-day life. The number of cyber incidents has increased and governments with private sector providers are challenged to keep up with the amounting pressure (Carr 2016). The concept of co-production will be introduced to analyse the potential of improving cyber security by involving citizens.

1.1. Cyber security of the critical infrastructure information systems and e-government and a shift towards enhancing resilience

Critical infrastructure protection (CIP) has been an inseparable part of national security but after the privatization wave in the 1980s and initialisation of globalization processes in the 1990s most of the strategic infrastructure is now owned by the private sector. This has made it more difficult for countries to guarantee national cyber security independently. (Dunn-Cavelty 2009, 179). Nowadays a growing number of sectors vital for the economy and society rely heavily on ICT. The increasing use of ICT in critical infrastructure has given rise to the dependency on an additional cyber layer, which makes the national infrastructure more connected and vulnerable from the outside world, hence increasing the importance of cyber security of critical services and critical service chains. (Luiijf 2015, 17) This has led to a situation wherein governments, to ensure national security, have enforced businesses to take appropriate security measures in critical sectors like energy, transport, water, banking, financial market infrastructures, healthcare, and digital infrastructure. This is often coupled with a responsibility to notify government agencies in the event of cyber incidents relevant to national security. (European Commission 2017)

Development and maintenance of information systems (IS) software is associated with uncertainties that increase vulnerabilities and therefore potential threats (Warfield 2012, 104). Cyber attacks pose a serious threat to ICT infrastructure as malicious actors try to exploit possible security vulnerabilities. This may have severe consequences for individuals, companies, administration, and governments. Threats range from individual identity theft, fraud, and data abuse, to industrial espionage and have the potential to threaten public security. (Wirtz 2017, 1085) Since the beginning of the 21st century, an increasing number of nations have included services providing access to the internet itself into the list of critical infrastructures (Luiijf 2015, 266). A growing number of services rely on the internet connection and so do citizens who need to access the internet to receive services. Formerly independent critical infrastructure systems have become interlinked, interdependent and more vulnerable to cascading effects of cyber incidents. As nation states have become more dependent on cyberspace for its economy, public safety, and even defence, establishing a cyber strategy is considered to be an important element of the overall national and economic security strategy for a government. (Goodwin 2013, 23)

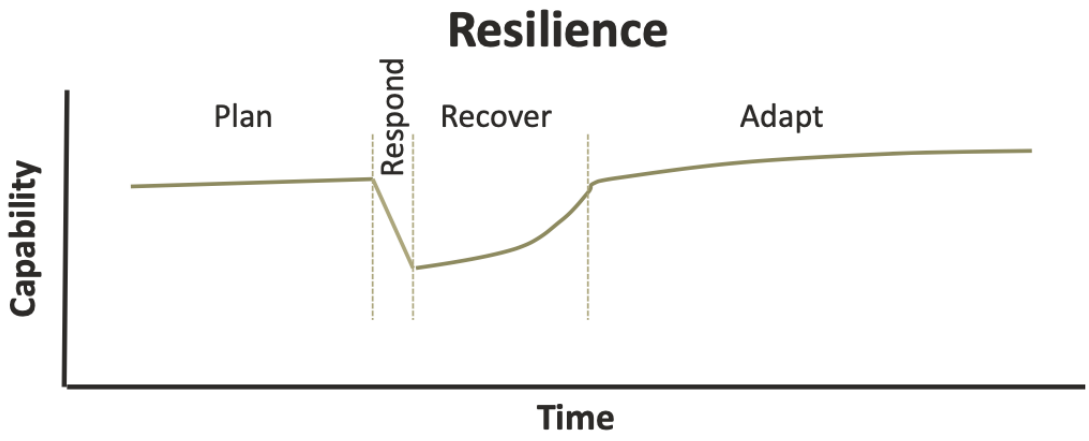
Strategy concentrated solely on the protection of services is not considered to be enough in this challenging cyber environment. The need to introduce resilience in CIP literature is rooted within the idea to be better prepared for rare natural disasters like hurricanes or floods (Boin 2007). It is argued (Setola 2016) that in the sphere of CIP there has been a noticeable shift from a protection-based approach towards a resilience-based approach and some (Coaffee 2021) see it even as a change of paradigm. Although, critical infrastructure risk management, protection, dependency modelling and analysis are still deemed to be necessary and widely used in practice, it is noticeable that resilience has become a wider term to cover different crisis management aspects and stages. (Setola 2016, 19) This shift is becoming more apparent as it is recognized that military and intelligence agencies are devoting considerable resources to successfully intrude on cyber systems (Nye 2017, 68).

While risk management capabilities have improved and continue to do so in the cyber domain, we cannot assume that it is possible to prevent every potential attack or malfunction on infrastructure systems. (Linkov 2013, 471) Instead of concentrating efforts solely on preventive measures, it is equally important to ensure the ability to continue providing vital services without major interruptions after the critical infrastructure ISs are breached. This capacity to predict incidents and limit their damage by being ready to respond to them quickly is known

as cyber resilience which by some authors (Björck 2015, 316) contrasts with the concept of cyber security. One of the most widely used definitions for resilience is termed by the National Academies of Science (NAS). Resilience is the ability to prepare and plan for, absorb, recover from, and more successfully adapt to adverse events (The National Academy of Science 2012).

The plan phase of resilience is an essential aspect to securing the availability of services and assets functioning during an incident. The absorb/respond phase of resilience describes the system's capacity to delay an attack on critical thresholds or immediately reconfigure so that when one part of the system fails, to avoid cascading failures in other systems. (Bostick 2018) It is about ensuring continued services during an attack and taking steps to isolate the incident. (Keys 2019, 70) The goal is to maintain the most critical asset functions and keep the service available. (Rajamäki 2018, 2045) The recover stage composes of restoring all aspects of the service to the same level as before the incident. The adapting stage focuses on implementing the lessons that were learned during the incident to enhance the service resilience. (Keys 2019, 70) Knowledge from the incident is used to change protocols, configuration of the system, personnel training, or other aspects to become more resilient. (Rajamäki 2018, 2045) Figure 1 visualizes these stages on a scale of time and capability helping to understand the resilience processes during a cyber incident.

Figure 1 Conceptual model of the stages of resilience as a function of time



Source: Roege 2017, p. 386

While the traditional risk management approach has depended on only a small number of governmental stakeholders dedicated to the matter, resilience is about expanding the decision-making to individuals, professionals and community groups. (Coaffee 2021, 542) For highly

complex and interconnected systems, it becomes prohibitively difficult to conduct a risk assessment that adequately accounts for the potential cascading effects that could occur through an outage or loss spilling over into other systems. Given the rapid evolution of threats to cyber systems, new management approaches are needed that address risk across all interdependent domains (i.e., physical, information, cognitive, and social) of cyber systems (Linkov et al. 2013a, b). (Linkov 2019, 2)

Ideas and practices of resilience have become a central organising metaphor within policymaking processes and the expanding institutional framework of national security and emergency preparedness. For many, resilience offers an integrated approach for coping with all manner of disruptive events, as well as a new way to engage with future uncertainty. (Coaffee 2021, 542) The concept of resilience has found use and acceptance in many policy areas. The proponents of resilience see unlimited potential, as resilient systems are thought to absorb or bounce back from any shock to the system. Although, there appears to be a problem in signing off on an agreed definition of resilience that would encapsulate its capacity, process, or outcome. It is not always clear how resilience differs from either good governance or crisis management. (Boin 2016, 293)

The academic research on cyber resilience of the critical national infrastructure has thus far been focused mostly on the aspect of government and private sector cooperation. Harrop (2015) focused on how countries have prepared for sustained and targeted attacks on their essential services delivered to the public through national CI and CII concluded the continuing need to improve situational awareness and planning that depends on deepening partnership between industry, commerce, infrastructure owners, infrastructure operators, and government(s). (Harrop 2015, 165)

1.1.1. Integrity of services and information systems

With the wide use of ICT, governments have moved many of their services online. Digital interaction between government and its citizens' enables states to be more accessible, effective, and transparent. This information exchange between the government and citizens forces information databases online. An essential precondition for citizens to use these e-services is a guarantee that information exchanges between government agencies and citizens are safe, private and information could not be accessed by an unauthorized third party. While these

online ISs are not always considered to be economically profitable targets for criminal actors, they might be suitable targets to achieve the geopolitical ambitions of the state actors. Recent years have demonstrated how state actors have used different means to undermine citizens' trust in their government, and by consequence democratic processes have been targeted through attempts to compromise the election systems.

Academic literature shows that cyber security and privacy issues are the major barriers to e-government implementation and may considerably affect the success of e-government (Wirtz 2017, 1086). When ISs are compromised private data may become available for copying, encryption or manipulation. In addition to the economic repercussions, these incidents erode trust in the service providers. For a government, an important aspect is managing the trust tension between citizens' right to receive efficient e-government services and privacy/security concerns that having all this information available. (Dutton 2005, 21) Some argue that while we are witnessing shrinking trust in government, technology in general and e-government, in particular, are often seen as a mechanism that could potentially change this trend (Bannister 2011, 144-145). Efficiency, competence and transparency lead to greater trust in public e-services and by affecting these it is possible to jeopardize trust relationships between government and its citizens.

A key enabler for a working system of e-services is the idea that citizens can identify themselves before accessing the services that entail the use of personal information. To ensure a secure interaction between a citizen and government-provided e-services, states have issued different means of authentication. To provide safer online access, states issue identity cards that in some cases can also entail biometric information and cryptographic credentials. Trust on the internet can be boosted through the use of a chain of certificates that trace back to a root certificate. If the authority responsible for the certificates should have a security breach in the systems or experience problems with providing the services, it will erode all depending trust relationships based on the issued certificates. (Luiijf 2015, 266)

1.1.2. Managing national cyber security

Governments have experienced difficulties with managing the security of IS and assuring private sector's compliance with the enforced cyber security requirements. Private sector ownership poses IT security threats that governments need to address. The private sector is

understandably guided by capitalistic profit/loss analyses when define their commitment and responsibility to invest in infrastructures' ISs. (O'Neill, 2005 referenced in Warfield 2012, 135) It has become more evident that not all industries in the private sector have enough incentives to keep their IS security standards up to date. In banking and telecommunications sectors there is a high demand for service security which creates an incentive to invest in cyber security. While in the energy sector, many industrial control systems that used to be isolated are now interconnected through ICT technologies and open to vulnerabilities (Roege 2017, 399). Without government cyber security regulations there would be no remarkable incentives to invest in cyber security. Cyber security is characterized as a fundamental uncertainty and all actors, government, private sector, and individuals have their role in the continuity and proper functioning of ISs supporting critical infrastructures. (Brechbühl 2010; Dunn-Cavelty 2009; Warfield 2012) However, governments' role is to ensure this is enforced.

The current challenging security environment has pushed CIPs towards industry self-regulation, best practices, and some coordination in terms of information-sharing with the government (Carr 2016, 53). It is not sufficient for governments to regulate by setting standards and enforcing them in a top town hierarchy. This is why national cyber-security strategies avoid suggestions of hierarchy when they refer to the public–private partnership (Carr 2016, 55). Research analysing more than 100 cyber policies of 15 different states concluded that governments tend to delegate authority while developing hierarchical control in case there is a need to react on threatening attacks. However, by creating incentives governments encourage third parties to tackle the risks and vulnerabilities in cyberspace. (Weiss 2019, 259) Governments are searching for new innovative solutions to direct private sector competencies closer to public administration.

In regard to the preservation of national interests or even survival, security considerations generate the need for hierarchical control (Weiss 2019, 261) which in practice may often complicate the use of outside expertise in national cyber security. There is general recognition of the need for a "comprehensive approach" to cyber security, coordination between all stakeholders, and a need for cooperation between all relevant public, private and military entities. (Boeke 2015, 72) Cyber security depends heavily on having an updated overview of the possible threats and making steady improvements in readiness to react to rapid technological changes. Cyber security policies are created to ensure the security of CIISs balance between service providers complying with the standards set by the state and the

authoritative approach of the state. The implementation depends heavily on the willingness of the third parties to comply with the new rules, which is arguably enhanced when they become an integral part of the initial decision-making setting (Scharpf 1997, 11–12; Weiss 2019, 265).

Efficient crisis management and incident response are heavily dependent on the information exchange between government and private actors. Crucial components of national cyber security like situational awareness, threat analysis, and network resilience need to be in place prior to a crisis. On the institutional level, information-sharing between government and private actors is a role of Computer Emergency Response Teams (CERT's). (Boeke 2015, 74) The importance of information sharing through public-private partnerships has become a dominant line of practice articulated in many national cyber security strategies. Information sharing helps to facilitate partners' expectations, face challenges, and bring greater clarity about lines of responsibility and authority. (Carr 2016, 54) Well-defined boundaries improve the government's ability to mobilize intermediaries with beneficial capacities and employ them when incidents occur (Weiss 2019, 269).

1.2. Co-production

The literature overview from the previous section demonstrated how in the sphere of national security the focus has been mainly on the cooperation between the public and private sector while citizens' role in enhancing cyber security and resilience has been limited. The following section introduces the potential role of involving citizens in public service improvement. The concept of co-production has found use in tackling complicated problems. The rising challenge of cyber security and the need to enhance cyber resilience has established itself as another complicated issue where the input of citizens could be tested.

The concept of co-production was introduced in the discipline of public administration by Ostrom in 1972. After a study focusing on cooperation between police and neighbourhood watch found that recipients of public services can have a positive influence on the service quality if they are involved in the service delivery process. (Ostrom 1996, 1073) The theory of co-production has gained prominence after the wave of New Public Management (NPM) theories and in consequence failures of the NPM reforms. There has been a remarkable rise and evolution in the field of co-production studies (Nabatchi 2017, Osborne 2018) which is

related to the rise of New Public Management (NPG). This theory focuses on public service delivery systems that achieve societal goals and public service delivery through emphasizing the interaction between multiple actors (Osborne, 2010).

Finding a comprehensive definition for the concept of co-production is an ongoing process in academic literature. While Voorberg (2015) has found that co-production is in some cases seen as interchangeable with the concept of co-creation, the main objective between the different co-production definitions is quite similar. Table 1 describes the definitions of co-production by different authors. This thesis uses the co-production definition by Brandsen (2016). Co-production is "a relationship between a paid employee of an organization and (groups of) individual citizens that requires a direct and active contribution from these citizens to the work of the organization" (Brandsen 2016, 6). Fugini (2016) has found this definition helpful in highlighting the three main characteristics of co-production. First, the continuous relationship between the organization employees and the citizen(s). Second, the need to have direct and active input from the citizens. Third, the citizens' contribution is voluntary and organization employees are paid for their work. (Fugini 2016, 6) Brandsen's definition was chosen for this thesis because it does not emphasize separating citizens into customers, clients, users, or communities and lets the relationship itself define the nature of it. Also, by defining the co-production relationship as direct and active, it does not include the passive co-production activities and focuses on citizens who are knowingly devoting their time to co-production. Another important aspect of this thesis is also the focus on long-term co-production relationships.

Table 1. Different Authors' definitions of co-production

Author	Definition of co-production
Osborne 2016	"… voluntary or involuntary involvement of public service users in any of the design, management, delivery and/or evaluation of public services." (p. 640)
Loeffler 2016	"Public services, service users and communities making better use of each other's assets and resources to achieve better outcomes or improved efficiency." (p. 1006)
Brandsen 2016	"Coproduction is a relationship between a paid employee of an organization and (groups of) individual citizens that requires a direct and active contribution from these citizens to the work of the organization." (p. 431).
OECD 2011	"… a way of planning, designing, delivering and evaluating public services, drawing directly from citizens and/or civil society organisations." (p. 172)

Boyle 2009	"Delivering public services in an equal and reciprocal relationship between professionals, people using services, their families and their neighbours." (p. 11)
Bovaird 2007	"… the provision of services through regular, long-term relationships between professionalized service providers (in any sector) and service users or other members of the community, where all parties make substantial resource contributions." (p. 847)
Ostrom 1996	"… the process through which inputs used to produce a good or service are contributed by individuals who are not "in" the same organization." (p. 1073)

Source: Author based on the definitions provided by listed authors

1.2.1. Potential of co-production

Academic authors find that co-production should not be treated simply as an "add-on" to services but rather as a core component of public services (Osborne 2016, 641; Loeffler 2021, 396). Ostrom has argued that no market can survive without goods provided by government agencies and governments themselves cannot be efficient without the input from citizens. (Ostrom 1996, 1083) From the perspective of public policy design, it could be said that citizen behaviour is not often taken into consideration, although the very success of the policies is dependent on it (Whitaker 1980, 243). Government agencies need to recognize and encourage the co-production of the citizens and to do that successfully it is essential to understand the complex motivations behind the co-production (Alford 2002, 51).

While the concept of co-production has enjoyed recent academic attention in social sciences (Loeffler 2021, 2), many authors find that collective knowledge about co-production is still incomplete. Further research is needed to distinguish the potential benefits and also the potential shortcomings of co-production (Voorberg 2013, Nabatchi 2017, Brandsen 2018). Loeffler argues that while the level of co-production is evident to a certain extent in all services, the full potential of the concept remains still to be discovered by the service professionals, managers, and politicians. (Loeffler 2016, 1016) Co-production has been recognized as a relevant theoretical concept; however, it has not managed to challenge the discourse of the traditional public service provision where the service provider is solely responsible for the design and provision of public services, and citizens are expected then to demand, consume and evaluate these services. (Osborne 2016, 641)

Authors find that in many cases motivation behind implementing co-production has been a pursuit to overcome the fiscal pressure in public service delivery (Rich 1981, Bovaird 2007, Bovaird 2015; Lember 2017; Nabatchi 2017). The public sector has been subject to the combination of fiscal constraints and citizens' increasing demands and expectations for the higher quality of the services. These trends have caused interest in different forms of cooperation where citizens and private stakeholders would have an opportunity to help to find solutions to the problems and challenges that public services are facing. (Torfing 2019, 799) Loeffler has stated, “For co-production to work, it is essential for citizens and service providers to have something valuable to contribute, be willing to make that contribution, and understand the context in which these contributions can be created efficiently and effectively.” (Loeffler 2016, 1014) This highlights that to implement co-production public service providers need to see and understand the value of co-producing public services with citizens and citizens need to see the value in contributing.

Co-production sees people outside from the public administration as potential resources and the ability to activate this potential could generate innovation in public services (Boyle 2009, 14). Public sector managers are expected to find ways to encourage citizens to be more involved and committed to improving public services by creating a platform for citizens to interact with the state and each other. (Bovaird 2016 b, 254) It is important to go beyond the perspective of a one-way relationship between the state and third sector as principal and agent, or provider and recipient. The concept of co-production emphasizes the shared character of the production process. (Brandsen 2006, 496)

1.2.2. Motivation for co-production

There is a considerable body of public management research elaborating the motivations behind pursuing co-production (Alford 2002, Bovaird 2012, Bovaird 2015, 2016, Surva 2016). Trust between co-producers, personal relationships, and citizens’ intrinsic and extrinsic motivation to contribute their time are all qualities considered to be critical for co-production to take place. All of these can clash with the sometimes inflexible public sector environment. Although co-produced services are praised for their personalized approach, these co-production solutions are still needed to be embedded in the otherwise formalized system of public services, especially when being at least partially funded by the government. (Surva 2016, 1031-1032)

Bovaird (2012) has found that citizens are willing to be more involved in delivering public services if their efforts make them feel like they have a perceptible role in the process. The spectrum of activities where citizens feel the importance to co-produce is limited. For the public sector, it is problematic to find the best way to approach these citizens as it is not used with marketing to specific segments (Bovaird 2012, 1136). This highlights the need to improve the public sector's understanding of citizens' motivations to co-produce and then build an approach focusing on activities where citizen input would be taken into account the most.

Company, fellowship, and esteem of others has been considered as a strong motivational factor for co-production (Alford 2002) Later findings suggest that in most if not all cases citizens might be better engaged individually, on their terms (Alford 2016, 171), especially when the relevant actions are relatively easy and can be carried out individually rather than in groups (Loeffler 2013 cited in Bovaird 2015, 2). Even though individual co-production activities are found to be more popular than group activities (Alford 2016; Bovaird 2012, 2015; Loeffler 2008; Parrado 2013), there are reasons to believe that much of the potential pay-off from co-production, both to the public sector and to citizens, may come from collective activities. (Bovaird 2015, 2) Although it is easier to encourage individual co-production governments should start re-orienting their citizens to collective co-production (Bovaird 2015, 19).

1.2.3. Four Co's of Co-production

This thesis aims to find different ways in which citizens can enhance cyber resilience by highlighting potential co-production opportunities in the sphere of national cyber security. To pursue this goal a decision was made not to limit the co-production concept with the service delivery phase. It has been expressed that co-production activities are visible throughout the full value chain of a service, including planning, design, commissioning, managing, delivering, monitoring, and evaluation. (Bovaird 2007, 847) Many researchers (Pollitt 2007, Bovaird 2012, 2016; Sicilia 2016, Nabatchi 2017) have found useful to study co-production in four phases of the public services production cycle. Theoretical approach chosen for this thesis is Loeffler's which has categorized co-production in Four Co's: **co-commissioning**, **co-design**, **co-delivery** and **co-assessment.** (Loeffler 2016, Loeffler 2021) This approach builds on previous work and avoids further fragmentation of the co-production research. The Four Co's of co-production promises to give a more detailed overview on different co-production activities by using a subcategorised approach.

Co-commissioning concerns public sector organizations working with communities and people who use services to identify, prioritize and finance public outcomes. It covers a wide range of terms like co-governance, co-planning, co-prioritization, co-procurement and co-financing (Loeffler 2016, 1009) which are used as synonyms for co-commissioning or just to highlight more specific activities within the co-commissioning (Nabachi 2017, 771). This approach helps to think through what is needed to be delivered, who is the subject of the service and what outcomes are wished to be achieved by that. The commissioning is about setting the service priorities. Bringing together decisions on which outcomes are priorities and which groups of the public are priorities helps to ensure priority outcomes (Bovaird 2013, 6). This is especially important as it is not always possible to achieve all desired outcomes (Loeffler 2021, 85). Due to the limited resources, however, involving citizens in the process may add a legitimizing aspect for the priorities set. An example of co-commissioning would be interpreting patients who have received care in the hospital as experts by experience. Their experience on the individual or at the collective level has the potential to improve treatment, strategic planning and service provision overall (Brandsen 2018, 301).

Co-design is about service providers and citizens redesigning public services to improve outcomes or reduce cost (Loeffler 2016) or co-developing new pathways to improved outcomes (Loeffler 2021, 82). Co-design activities try to learn from the user experience and then apply these insights into public service planning and design (Bovaird 2013). By using the outside perspective of the service users public sector professionals can see how to provide services in the way that individuals and communities would benefit the most. (Nabatchi 2017, 772) Co-design by users or communities may be related to public spaces, communication, projects, services and improvement plans. (Loeffler 2021, 99) For example, professionals have face-to-face meetings with citizens to frame the problems, elicit expectations, and translate them into viable solutions. But a threat is that these solutions may not necessarily lead to long-term policies which therefore may have a negative influence on the citizens' motivation to further contribute to co-design. (Nesti 2007, 7)

Co-delivery is about citizens, public sector organizations and public service providers engaging in joint activities to directly improve outcomes, for example through behaviour change of service users or other citizens, or which improves services through citizens directly managing or performing some activities in the service delivery process. It includes co-managing, co-influencing behaviour change, co-performing. (Loeffler 2016) Co-delivery

focuses on the ways how service providers and service users provide or improve the quality of public services (Alford 2002). As co-delivery focuses mainly on improving the service efficiency and quality it fits well with the traditional view of co-production (Nabatchi 2017, 772). While co-commissioning, co-design and co-assessment involve citizen's voice, co-delivery is mainly about citizen action to improve public services and/or outcomes, rather than citizen's voice (Loeffler 2021, 79).

Co-assessment is about public service providers working with citizens as monitors and evaluators of public service quality and outcomes (Loeffler 2016). Giving assessments to past activities has the potential to improve services for the better. Co-assessment is a process that helps to learn together with citizens from experiences on how to improve and rethink public services. (Nabatchi 2017, 772) It is about taking a step forward from outcomes of services and highlighting the importance of how services are delivered. By taking into account access, suitability, responsiveness, reassurance, empathy, transparency, participation, collaboration (Bovaird 2013, 11). Loeffler (2021) has also subcategorized three different types of co-assessment: giving feedback to the public service organisations, reviewing public services and outcomes, undertaking joint research with public service organisations (Loeffler 2021, 133). An example of co-assessment is when services are jointly assessed by the professionals and the users through several meetings whereby the activities performed can be modified and potential problems identified (Campanale 2021, 288). Co-assessment may take place in a form of a survey or even a complaint.

By adopting this approach co-production is defined as an overarching concept which helps to capture a wide variety of activities that can occur in any phase of the public service cycle (Nabatchi 2017, 769). While taking account the different roles citizens could have in public services it would be however, unrealistic to be expecting to see Co's represented in every phase of one single public service. Also, it is unlikely that all Four Co's could be equally important in a specific context at a particular time. (Loeffler 2021, 77) However, after dividing co-production activities into four phases of service production it is easier to detect co-production taking place in services even without actors knowingly defining their activities as co-production. The Four Co-s' provide a lens that gives more insight and concreteness in an effort to explain how citizens can improve the quality of the services. This approach helps to understand different aspects of co-production and to be more specific about the otherwise

widely interpreted concept. This thesis uses Four Co-s' to identify different possibilities how citizens could take part in the co-production processes.

1.3 National cyber security and co-production

While co-production has become a relevant concept for academic research in social science, there are far fewer case studies in the sphere of security or national security. This has been previously explained by differentiating "soft" and "hard" services. In "soft" services like education or health care participation of citizens was seen as a requirement to achieve the service improvement. However, in the case of "hard" services like policing and firefighting the service quality was not perceived to be that related to the role of the citizen involvement. Later research findings have suggested that citizen contributions to the "hard" services were often unrecognized and are just as essential to the successful delivery of these services. (Brudney 1983, 60) Long practice of citizen militias, jury systems, and volunteer firefighter commandos demonstrates a strong presence of citizen co-production in the "hard" services (Bovaird 2016a, 48) relevant till this day (Tõnurist 2017).

It has become evident that the co-production of services creates vagueness and mutual dependencies in the authority and control of the resources. These conflicts with the classic public administration approach where transparent and concrete boundaries between the private and public sectors are seen as a precondition for effective policy making. However, it has been argued that in some cases blurring these boundaries may be the key to creating effective service delivery arrangements. (Joshi 2004, 40) Co-production does not offer easy solutions. Even though co-production partnerships between public sector professionals and citizens may seem like more complicated arrangements at the first sight, there is potential to improve public services. The competencies of citizens could be helpful in developing areas related to changing technologies where government agencies have problems in gathering knowledge, know-how and expertise. By establishing appropriate legal, policy and operational frameworks it would be possible to increase national cyber security by engaging volunteers (Czosseck 2011, 63).

1.4 Summary

Section 1.1 provided an overview of the ongoing challenges that governments face in efforts to secure critical infrastructure and e-services from the harm posed by malicious actors and deteriorating cyber security environment. It also highlighted how in the sphere of national cyber security there has been a focus shift from protecting to enhancing the resilience of CIIP. Section 1.2. introduced the concept of co-production and elaborated on the potential of involving citizens to improve the quality and efficiency of the services. Four Co's of co-production were introduced as an approach that could facilitate identifying co-production activities in different service production cycles. Section 1.3 gave an overview of citizens' role in national security and resilience building while also addressing the barriers that the security sphere poses for involving citizens in national cyber security. The next step is to show how introduced theoretical concepts can be tied together in a framework that would help this thesis to analyse the citizens' role in national cyber security by enhancing the resilience of services critical to the day-to-day functioning of modern society.

Traditional public administration and the national security sphere have emphasised a need for strong hierarchical structures while co-production, praised for its potential to improve public services, is recognized for blurring the lines of authority and responsibility. However, the complex nature of the cyber sphere and the growing importance of enhancing national cyber resilience has created a push to innovate and to find new ways to involve citizens in cyber security. While recognizing the conflicting natures and motivations behind stakeholders, this thesis concentrates on citizens' potential to enhance national cyber security. In the age of governance, the input of citizens as service users is seen to have a legitimizing effect and is also valued as a potential improvement to service quality. Even though theoretical literature has tied governments motivations to use co-production for service improvements strongly with monetary reasoning, in the literature on national cyber security the compelling motivation for citizen involvement seems to be the complicated nature of the cyber space.

In the sphere of cyber security, the rising importance of the concept of resilience has changed the basic understanding of security in cyber space. While enhancing resilience may be the desired output in national cyber security policies it is somewhat harder to determine what resiliency actually is and how policy documents could enhance the cyber resilience of vital national infrastructure. In order to have a more structured approach on the concept of resilience

this thesis determines the concept through four stages of resilience: plan, respond, recover, adapt. By doing so it is possible to detect concrete activities targeted to enhance resilience in specific resilience stages. To focus on the citizens' role in resilience, the concept of co-production is introduced to the framework. More specifically, the co-production concept of Four Co's, which defines the wide range of activities characteristic to co-production. The Four Co's (co-commissioning, co-design, co-delivery and co-assessment) help to describe the different potential roles of the citizens - how can citizens enhance national cyber security in different stages of resilience (Table 2) thereby answering the research question - What is the citizens' role in improving the national cyber security for e-government services and critical infrastructures?

Table 2. Co-production opportunities in different stages of CI and CII cyber resilience

Four Co's of co-production	Stages of resilience			
	Plan	**Respond**	**Recover**	**Adapt**
Co-commissioning	Citizens are involved in prioritising the cyber security policies and strategies.	Citizens are involved in setting priorities in CI respond processes and protocols to absorb and respond to the incidents.	Citizens are involved in prioritising the CIs and the aspects of services that need to be restored first.	Citizens are involved in a process where the key lessons from recent incident are drawn.
Co-design	Citizens are involved in policy planning processes to enhance the CI cyber resilience.	Citizens are involved in structuring how CI services could absorb and respond to the incidents.	Citizens are involved in designing CI recovery plans and protocols.	Citizens are involved in redesign security protocols and plans to adapt with previous incidents.
Co-delivery	Citizens are involved in active resiliency planning processes. e.g., attending meetings and workshops.	During an incident, citizens are involved in maintaining the CI service availability.	Citizens are involved in restoring the services to pre-incident level.	Citizens are involved in adapting with possible similar incidents in the future.
Co-assessment	Citizens are involved in monitoring and evaluating the resilience planning activities.	Citizens are involved in monitoring and evaluating CIs incident response protocols.	Citizens are involved in assessing protocols and processes to restore CI services.	Citizens are involved in assessing the adapted post-incident protocols.

Source: Author

The rising prevalence of resilience theory in CI protection emphasizes the involvement of more stakeholders and importance of large networks. Involving citizens in national cyber security would suit with this approach and this is where co-production theory intersects with the resilience. Conjecture of this thesis is that citizens have potential to enhance the resilience of critical national infrastructure and the co-production concept of four Co's enables to explore the citizens' role in more depth. In a pursuit to find the potential roles of citizens in national cyber security and resilience, it is also important to understand the motivations behind these co-production activities. One might have the expertise and potential to co-produce cyber security, but there also needs to be a motivation or an opportunity to use that potential to improve the resilience of CI services. While this thesis uses constructed framework in Table 2. to find the co-production activities, it also brings out the different motivations behind these co-production activities to understand better the motives and circumstances behind these co-production activities.

2. Citizen co-production in Estonian cyber security

2.1. Research design

The empirical analysis is focused on how citizens with cyber security expertise have been involved in the national cyber security policy of Estonia. More specifically how can government professionals and citizens work together to secure public services that improve national cyber security capabilities for critical infrastructure and online services. Section 2.1.1 will elaborate on why the research case study method was chosen for this thesis. Section 2.1.2 describes how data was collected for this research. Section 2.1.3 will give an overview of limitations that are common criticism towards case study as a research method and also highlights the limitations specific to this thesis.

2.1.1. Research design

As this thesis moves from a more general theoretical level to a specific explorative case study it is appropriate to use a deductive approach. This thesis will use a qualitative research approach to analyse the linkages between causally relevant factors in-depth (Mahoney *et al.* 2006, 234). Often when a contemporary phenomenon is studied, in-depth analysis requires some kind of fieldwork, like getting close to the specific case under study (Yin 2003, 24). This thesis uses an explorative single case study to move from general theory to in-depth analysis. Case studies may be based on single or multiple cases; however, to study Estonian cyber security cooperation among various stakeholders, the researcher has decided to take a more profound approach by choosing single case study. While co-production theory has seen widespread popularity in different research fields, there is a limited amount of research conducted in the sphere of national cyber security and this thesis intends to help to bridge that gap. A decision to opt for a single case study is also supported by an argument that single case study tends to be more reliable as it enables more accurate understanding of the circumstances (Mariotto 2014, 363). This case study is holistic rather than embedded as it concentrates on one sub-unit of analysis (Yin 2003).

2.1.2. Data collection

Empirical data for the research was gathered through document analysis and nine semi-structured expert interviews. To achieve a more comprehensive understanding of the cyber security policies different national strategy documents, reports, annual assessments, legislative changes, expert opinions, news articles and academic articles were analysed.

The document analysis was conducted first to establish an initial understanding and overview of the previously published academic and journalistic research on Estonian cyber security incidents and architectural characteristics. Document analysis was focused also on the different legal acts, reports, national policies and strategies on Estonian national cyber security. Policy papers, assessments and strategies like Estonian Information System Authority's Annual Cyber Security Assessment, National Cyber Security Strategy and National Emergency Act were analysed to gain a better understanding of the stakeholders involved and their respective roles in the processes.

In addition to document analysis, semi-structured interviews were conducted with interview questions based on the thesis framework presented in Chapter 1. Document analysis was used to distinguish the organizations that were important from the focus of this research and the experts and former officials who were in key positions during the 2007 and 2017 cyber incidents. In addition to EDL CU members, interviews were conducted with department heads of the state agencies relevant from the thesis research focus. Snowball sampling was used to establish potential names for the next interviews. This helped to identify people who were, according to the experts, in a position to comment occurred incidents, volunteer involvement and motives behind the policy changes. List of interviewees is available in Appendix 1. Interview questions which were adjusted according to the role of interviewees and the list of the interview questions is available in Appendix 2.

Interviews were an important source for in-depth expert knowledge that would not have been otherwise possible to collect from publicly available sources. This is partially related to the national security sphere specifics where published press releases are general with an intent to inform public without revealing any specific information. From that perspective, a decision was made to conduct semi-structured interviews so interviewees from different government agencies responsible for developing cyber security policies and members of EDL CU could bring up matters, subjects, themes and express opinions with importance to understand better Estonian national cyber security processes. Every conducted interview was recorded with the consent of the interviewee and transcribed later for a text analysis.

2.1.3 Limitations

Common criticism towards case study as a research method is the notion that it does not provide basis for scientific generalization. Yin (2003) has answered to critics with acknowledging that even tough case studies are not generalizable to populations nor universes it may be used for theoretical generalizations. (Yin 2003, 10) While one of the limitations of a single case study is that it does not allow to make statistical generalizations, it is countered with an argument that the objective of social research is to gain a deep understanding of one specific case, not to find universal laws (Mariotto *et al.* 2014, 363). Flyvbjerg (2006) however has argued that single cases provide us valuable information and have even led to discoveries in a process to

define universal laws. In some instances, single case studies may be more credible than analysing a large sample of cases. (Flyvbjerg 2006, 225)

To overcome the limitations of the qualitative approach it is necessary to create strong causal paths that can play a key organizing role for general theoretical knowledge. To make the conclusions more generalizable it is prevalent for qualitative research to define scope of theories narrowly. Adopting narrower scope for the research has its roots in a conviction that causal heterogeneity is the norm for large populations. (Mahoney 2006, 237)

A decision was made to focus on two of Estonia's most significant cyber incidents in 2007 and in 2017 to elaborate on the perspective of national cyber resilience. Focusing on the incident response helps to indicate citizens' roles in threats response and enhancing resilience to national cyber security. However, it must be addressed that the 2007 cyber attacks against Estonia did occur 14 years ago and this has an effect on the accuracy of the interviewees' responses. As two incidents took place 10 years apart from each other it gives an opportunity to better understand the structural changes in Estonian cyber security policy and citizens role in it. However, being that far apart from each other on a timescale complicates finding interviewees who were professionally involved with both incidents.

The number of interviews limits also the generalizability of this thesis. This thesis is not able to answer the research question definitely but intends to provide an insight on the potential of co-production in the sphere of national cyber security.

2.2. Cyber security and cyber resilience of critical infrastructure and e-services in Estonia

Estonian case is chosen for the analysis as it is considered to be one of the leading countries in digitalization and moving government services online (Björklund 2016, 915) in particular with regards to public digital infrastructure and e-identity (EISAa 2017). Currently, 99% of Estonian public services are available online (e-Estonia, 2021). Online services have become the most important communication channel between government and citizens making e-services critical for society's day-to-day functioning.

The key to the online interaction between the government and the citizens in Estonia is X-road and national ID-card. Estonian Information System Authority (EISA) launched the X-road in 2001 and started issuing national identification documents providing a unique certificate for the card holder which can be used for accessing online services. X-road is an online environment for services and is designed for a secure data exchange. To ensure secure transfers all outgoing data is digitally signed and encrypted, and all incoming data is authenticated and logged. (e-Estonia, 2019) This environment hosts public and private services. National ID-card that secures a safe login to every user is also used for digital signatures and electronic voting.

High dependency on properly working e-services has made cyber security an important part of the Estonian national security (EISAa 2016, 5). After introducing the e-voting system the steaks were raised, and cyber security was tied directly with the legitimacy of democratic processes. Like most developed countries, the actors behind the cyber threats on Estonia are organized crime and state actors. International trends show that more often malicious groups testing security in cyberspace are supported by hostile governments (EISA 2018, 31).

2.2.1. Cyber Attacks Against Estonia in 2007

In April 2007, the Estonian governments' decision to relocate a Soviet-era statue of Bronze Soldier from the Tallinn city centre to a more remote location in a military cemetery evoked a wave of cyber attacks against the Estonian government. The statue that symbolized Soviet occupation for Estonians had a deep cultural and historical meaning for the Russian-speaking minority. Opposition to the displacement of the statue escalated into a riot that was shortly followed by a politically motivated cyber attack campaign. Simple Denial of Service attacks blocked government websites, online newspapers and disturbed the work of online banking services. This event is considered to be the first known politically motivated cyber attack against a country (Mansfield-Devine 2012, 12) and the only time systems in the Estonian state were interrupted on the national level (Geenius 2019). However, attacks did not halt the further digitalization of the country, on the contrary, Estonia intensified attention in the aspects of cyber security by creating a comprehensive cyber strategy with a strong focus on improving inter-government and private sector cooperation (Mansfield-Devine 2012, EISAa 2017).

The informal communication of cyber experts established beforehand and the existence of a community was the key to resolving the 2007 crisis. The emergence of EDL CU created a new

format of cooperation and provided an opportunity for training, a better understanding of rice protection tasks, etc. (I8)

Estonian reactions to the attacks were described as timely and professional. Estonian government agencies received a great deal of support from an informal small network of Internet security community, which assembled promptly for a co-ordinated response.

In the sense that from 2007 onwards, it was very significant that everyone understood the need for coordination. Because the attack was not only against state structures but against the whole state, including civilian infrastructure like banks, media outlets etc. From there, it just became clear that this was necessary. ... Whether he does it now after he is a citizen or whether he is doing it because he represents his company and the interests of his company, that there is a border like that. I think that this concept of citizen will only come into use from the moment the EDL CU was established. (I9)

The important practical lesson was that there is a need for the improvements in the systems of crisis management and protection plans of the critical structure. To be prepared against similar attacks in the future, there has to be more attention on regular compulsory tests and simulations. (Mansfield-Devine 2012, 15) As a response government adapted a first Cyber Security Strategy already in May 2008. Amended security situation resulted in introducing several new laws and regulations, and several changes in the organisational landscape. (Czosseck 2011, 58) Strong attention on pushing the policy changes and active lobby of the Estonian government resulted in situating the newly established NATO-accredited cyber defence hub in Estonian capital Tallinn. Cooperative Cyber Defence Centre of Excellence (CCDCOE) to support member nations and NATO with cyber defence expertise (CCDCOE, 2019)

The significance of 2007 was not the attacks themselves but the fact that they opened a cyber security debate for politicians. ... With the decision to communicate the 2007 events, Estonia opened the international discussion between diplomats and politicians – cyber security was being talked about publicly. (I7)

2.2.2. Security risk of the Estonian national identity card in 2017

Another more recent significant incident that confirmed the uncertainty of cyber security was the discovery of the national identity card security risk at the end of 2017. An international

group of researchers found a security weakness in an electronic chip technology used also in the Estonian ID-cards (EISA 2018). The government informed the public about the potential security threat that affected almost 750,000 ID-cards issued in the previous three years (ERR 2019). Theoretical vulnerability discovered by researchers affected the digital use of Estonian ID-cards that were issued after October 2014. It appeared that microchip hardware in combination with ID-card software had a potential vulnerability making it possible to break the encryption of the ID-card signature or even forge it. (EISAc 2017) It was a remarkable security concern because the Estonian national identity card was used by the majority of Estonians as a key online identification certificate for making secure payments in e-banking systems, accessing personal information in the e-health portal, signing documents digitally and even e-voting on the parliamentary and local elections.

The Estonian government's decision to disclose the vulnerability publicly was retrospectively seen as a right decision (I1, I3-I5, I7-I9). When experts were asked to name what were the lessons to be learned then the need for an open and clear communication was emphasized to avoid panic and deterioration of public's trust against the IT solutions.

During the ID-card crisis there was a lack in knowledge, skills, physical human resources and technical human resources. However, as private sector understood that the crisis involves very directly their activities then they were offering help voluntarily. To solve the incident number of separate workgroups were assigned by EISA starting with experts on strategical communication to experts with technical knowledge. In every group there were experts who volunteered to help and only thanks to this, ID card crisis was solved that well. (I5)

Compromised day-to-day cyber solutions have great potential to disturb the functioning of modern society. On the one hand, the ID-card crisis demonstrated the uncertainty of cyber security while on the other hand, it proved also that cyber attacks against Estonia in 2007 gave valuable lessons and a strong fundament for future cyber security crisis management. (EISAa 2017, 2) To help avoid similar crises in the future EISA concluded five main lessons by highlighting the importance of alternative solutions, open and flexible architecture, threat responsiveness, extensive cooperation and digital and cyber capable society (EISA 2018, 14-15). In the aftermath, EISA estimated that the expenses caused during the crisis were around 1,8 million euros. Approximately the same amount was spent by the Police and Border Patrol responsible for issuing the new ID-cards. The Head of the EISA emphasized that indirect cost

are much larger and many private sector companies did not ask any fees for the work and assistance they provided during the crisis. (ERR 2019)

Among interviewees there were different opinions on the role of EDL CU during the ID-card crisis. Some found it to not be that significant (I4, I5) or were not just aware of it (I2, I9) while others were confirmed on the importance (I1, I9). Chief of the EDL CU could confirm that citizen volunteers from EDL CU were in fact involved in the 2017 incident to monitor information space with a focus on detecting potential co-ordinated activities to spread misinformation and create false understandings. For example, detected misinformation that could lead panic and overloading government agencies that were involved in giving out the updated ID-cards. Another aspect of the information space monitoring focused on detecting if there were any agitations to start exploiting the potential vulnerability and coordination of attacks. (I1) Citizens have the potential to be involved as a force multiplier and work on incidents if they turn out to be more time consuming, with a larger scale (I1, I4, I5,) or if there is need to do something in a faster pace. (I1)

Estonian ID-card crisis demonstrated that besides having covered the technical side of a cyber security incident it is increasingly important to also have expertise on communication and the legal compliance. It was not a new lesson, but it confirmed an old truth. This means that if the government plans reserves, then it must involve also volunteers with legal expertise, and it is necessary to come out with messages understandable for the public. (I1) This resonates also with the views of other interviewees (I4, I5, I6, I8) that in 2017 incident citizens role was most importantly to stay calm and not to panic. As the ID-card vulnerability was very technical, only number of specialists had the needed expertise to work out the solutions (I1-I9). Most of the help offers were turned down because the very technical nature of the problem and the sheer need to organize the whole process (I6).

2.2.3. Estonian National Cyber Security

Estonia has so far addressed the big picture of cyber security in already three cyber security strategies. Strategy documents will determine the direction and priorities for a longer time period. The first strategy for 2008-2013 focused on establishing national procedural rules and institutions for effective work allocation and inter-governmental cooperation. The second strategy for 2014-2017 was focused mainly on the protection of critical infrastructure, the fight

against cybercrime, information security competency improvement, the legal design needed for cyber security improvements, international cooperation, cyber security notification and development of cyber security industry. The third strategy for 2019-2022 has chosen a closer focus on sustainability of digital society and resilience. (MFA 2019).

In Estonia, the responsibility for ensuring cyber security has been divided between various ministries and government institutions. Responsibility for preventing and stopping cybercrime has been assigned to the Police and Border Guard Board within the administrative area of the Ministry of the Interior (The Ministry of the Interior 2016). The Ministry of Economic Affairs and Communications (MEAC) is operating the EISA, the governmental agency responsible for protecting and advancing digital society in Estonia. EISAs tasks include development and administration of Estonia's state IS and coordination of national cyber security. Cyber security coordination includes also the cyber incident response, emergency preparedness, and management, regulation and supervision. Furthermore, EISA manages also Estonia's e-government platform with national eID infrastructure and the data exchange layer X-Road, which is considered to be the backbone of e-Estonia. (EISAa 2017, 2)

The Section of Critical Information Infrastructure Protection (SCIIP) at the EISA concentrates above all on the protection of ISs that are needed for the proper and continuous operation of critical services. SCIIP is responsible for organizing the protection of the state's critical public and private ISs. The legal framework has made the owners of ISs responsible for ensuring their security. EISA assesses the threat environment and updates relevant stakeholders on the current cyber security situation. If larger incidents should occur, EISA coordinates the response. EISA's main responsibility on the national level is to monitor public and private sector information systems, used to secure the functioning of critical services in Estonia. Herewith are ensured the functioning of many essential aspects of the society – healthcare, security, economic and social well-being, all defined in more detail under the Emergency Act. EISA's responsibility on the strategic level is to protect the field of CIIP. EISA also carries out risk analyses linked to the CII, prepares security measures and supervises these precautionary methods. (EISAb 2017)

On the more operative level, EISA's sub-unit known as the Estonian CERT (CERT-EE) is responsible for the protection of the information systems necessary for providing the critical services. (EISAb 2017) CERT-EE monitors information security, works to prevent cyber incidents and also assists and advises in case of security incidents (EISA 2020). Since 2017

Estonia has successfully developed systems to detect and protect against cyber intrusions, conducted exercises to improve public and private sector cooperation, invested in the user awareness and taken actively part in international cooperation. This has improved remarkably Estonia's capability to handle cyber threats and crises (e-Estonia 2017). CERT-EE has even received a quality certificate by CERT community Trusted Introducer, making CERT-EE one of the six most acknowledged national teams. (EISAd 2021)

In 2018 Cyber command was established in the Estonian Defence Forces (EDF) to address cyber dimension of the conventional war. Former minister of Defence Jüri Luik stressed as a cyber state Estonia needs to protect its systems in the civilian and military fields. The Cyber Command was created to have one organization responsible for and capable of carrying out cyber operations and also to centralize the ICT expertise in the Defence Ministry's (MoD) area of government (EDF 2021). The military side of Cyber Command will be also in charge of the MoD's ICT as well as keeping the EDF's headquarters in proper working order, preparing and organizing the formation of wartime and reserve units, commanding and coordinating the development of cyber and command support capabilities, supporting awareness programs of the EDF, and organizing information operations. (ERR 2018b) The importance of this step is twofold. By unifying the ICT support for the whole Estonian defence structure ensures better quality and safer cyber security environment that can specialize in the security standards of military structures. Another more significant aspect is a step to distinguishing cyber capabilities needed by the defence forces. By this organizational change, Estonia recognizes the changing security environment and a need to allocate resources to build military cyber capabilities.

The approach taken by EISA is that in a case of cyber incident private businesses and citizens would not start hiding their mistakes but rather would report about it and if there would be need the EISA could offer support. (I5) Establishing a trust relationship between government agencies, private sector and citizens is a key aspect for establishing an accurate threat awareness in cyber domain. Engaging EDL CU volunteers as users of e-service who are helping to improve the cyber security environment supports the building of trust between stakeholders. EDL CU members are not officials but rather citizens who contribute their own time to improve the cyber security of other citizens. The fact that EDL CU members are not employed by the state is why it can be seen as co-production.

2.2.4. Current situation

Cyber security is considered to be an important part of national security. This is also well demonstrated by the recently passed laws and acts that put the responsibility of the safety of service users to the service providers. EISA has stated that with each year the critical infrastructure becomes increasingly dependent on e-services meanwhile service providers are not always aware of the risks on continuity of the critical services. Two main reasons causing cyber security risks are low awareness and lack of skills. This is a problem that is seen at all levels of organizations - from specialists to top management. (EISAa 2017, 28) It still remains a great threat that end users violate security protocols and may easily fall for social engineering or phishing. (Kaljurand 2018)

EISA highlighted also threats related to technologies and their probability to increase in frequency. (EISAa 2017, 7-8) Annual Cyber Security Assessment 2017 predicted a possible increase in cyber and information operations against the digital state (and critical infrastructures) as an upcoming challenge. From the start of CERT-EE operations, cyber security incidents have been constantly increasing. (EISAa 2017, 34)

Malicious cyber operations funded by foreign governments differ from other cyber threats because of long-term interests. It is extremely difficult to detect cyber espionage and therefore even harder to evaluate the total number of espionage incidents. After gaining access to the system, intruder's goal is to collect and transmit data over a longer period of time. In case of partial success, intruders are willing to wait patiently in the system for further opportunities to access more sensitive information. (EISAa 2017, 32) Malware incident with the Estonian group of oil shale, power, and public utility companies, Viru Keemia Grupp, is considered to be one vivid example of state-organized cyber operation against CISPs (EISAa 2017, 24) It is not seen exceptional that malicious actors are searching for vulnerabilities in the IS of critical infrastructure to support geopolitical ambitions of hostile states. (EISA 2018). Cyber attacks have become a common tool for state actors.

Estonia's state digital architecture has two categories of risks. First, since the expectations on the digital state are always changing then digital services are expected to operate smoothly and, in a way, society has been forced to adapt to. Therefore, the digital state has to be able to protect its services from imminent threats. Second, if risks connected to technological innovations become realized, then it is not only that some specific systems become vulnerable but instead,

the whole national security may become affected. (EISAa 2017, 35-36) This was highlighted also in the expert interviews who stressed that ID-card crisis changed the understanding of how e-services have physical alternatives.

> *Previously there was an understanding that every digital service has a physical alternative. Then it turned out that this is not really the case anymore. Some (services) may be on paper, but for example if a judge is not able to digitally sign or a doctor cannot open patient's digital health history and then prescribe a digital prescription... It was thought that the service could be somewhat disrupted, and you could go back to the paper alternative. However, in reality, it is so inefficient that much of the service will be not received.* (I4)

Increasingly growing complex systems of e-services need updates and are becoming more interconnected. Government agencies are not capable of having all the capabilities to respond to all the potential crises. (I5) Every private sector institution and private business is responsible for ensuring their cyber security.

All the interviewees recognized that citizens' role in enhancing critical infrastructure cyber security and resilience would be in creating a reserve of capable specialists for a large-scale incident.

My personal opinion is that the EDL should say what kind of reserve they need. What skills would they need to cover and if these are not covered then specific trainings would be conducted to meet the needs which then would be tested during an exercise. This would apply also to EISA and CERT – they would say what kind of skill sets they need for incident response. (I2)

Interviewees (I1, I2, I5, I7, I8) agreed that reserves of citizen volunteers would be helpful in case of larger cyber incidents; however, maintaining a reserve of citizens with skills to respond to certain incidents is resource intensive. Another aspect is that in case of a widespread incident, citizens who work as cyber security experts may be needed at their every-day job post (I3) and if a crisis situation is declared then EDL CU members would be assigned on their crisis positions in the Defence Force crisis structure (I1). However, the lack of cyber security specialists is emphasized by every interviewee. Think tank Parxis has estimated that by 2023, Estonian cyber security sector will need an additional 270-870 specialists with skills and

knowledge in the field. Compared to 2017, this is an increase of 32-86% in labour force (Praxis 2019).

2.2.5. Estonian Defence League's Cyber Unit

The cyber attacks against Estonia in 2007 demonstrated how effectively voluntary citizen networks of cyber security specialist mobilised to protect the Estonian IT infrastructure. Small group of information security experts from different companies and organisations worked together informally. (EDL) This incident influenced Estonian cyber security policy with valuable lessons that are embedded in cyber security strategies until today. One of the key lessons after creating the Cyber security policy was the need for cooperation and multi-stakeholder approach which led to the formation of EDL CU. It became clear that patriotism and volunteering helped to gather together specialist like government could never afford. (Kaljurand 2018)

An informal group of cyber specialists formed already in the 1990s through the Estonian ID-card system developing process. Over time this network of professionals worked together to protect critical infrastructures against criminally motivated cyber attacks. (Czosseck 2011, 61) Need to materialize informal networks of cyber security specialists, that proved to be extremely valuable during the moment of crisis, to something more formal and tangible. Even though an informal network of cyber security specialist was starting to form in EDL already after the cyber attacks in 2007, it was not until 2010 when the MoD proposed a change in regulation to create a formal unit of cyber security specialist inside the EDL. EDL CU was purposely formed to become the unit responsible for coordinating and advising volunteer cyber security professionals and citizens interested in protecting the Estonian e-society. (MoD, 2010)

Former Commander of the Estonian Defence Forces, Riho Terras has highlighted the importance of creating EDL CU in two aspects. On the one hand, it improves the informal network of cyber specialists and on the other hand, it gives government recognition to the activities of volunteer IT security specialists (MoD 2010). This aspect is heavily based on the notion that for government agencies in the sphere of national security it is vital to have clearly regulated relations, tasks and a line of command. Being embedded in EDL creates the preconditions to be involved in cooperation and partnership agreements with power structures and facilitates the processes in crisis management. To become a member in EDL CU

recommendation from a member is needed and background check is carried out before a new member is admitted (EDL 2021). This is not ordinary for a volunteer organization relevant from the national security perspective and an important aspect also for gaining the trust from CISP's.

EDL CU is assigned to assemble voluntary cyber security competence and in case of cyber attacks against Estonia, it cannot take initiative in organizing countermeasures instead EDL CU has an advisory role. (MOD 2010) EDL CU supports the Estonian Cyber Security Strategy in three main areas: raising awareness about cyber threats in society, sharing cyber security-related knowledge among IT specialists and participating in the protection of critical infrastructure if there is a crisis. During the crisis EDL CU has exactly the same role as EDL - to aid and support civil structures and protection of the critical infrastructure. (EDL) Commander of CU, Andrus Padar, has commented that volunteer's role in EDL is to provide support to public officials in a crisis situation when government officials are overwhelmed. Commander Padar finds that EDL is well involved in national defence and highlighted the importance of showing initiative to be involved and active participation in exercises with the EDF. (Delfi 2016)

CU gives an output for patriotically minded cyber security specialists while not emphazising overly on the traditional military service aspects. Besides from providing an opportunity to fulfil the patriotic call, MoD has promoted EDL CU as a way to provide volunteer information security specialists with additional value through extracting new knowledge from trainings, upskilling and training environment which would benefit also the volunteers' employers whose specialists are gaining new knowledge and experience on their field. (EPL 2010) This approach might be attractive to specialists as Estonia is known for hosting many highly recognized international cyber defence exercises and yearly national cyber security exercises. For example, EDL CU volunteers have been involved with organizing the NATO Cyber Security Centre their high-level exercise Lock Shields since 2010. This partnership was officially formalized with a cooperation agreement in 2014 which stated the continuing support of EDL CU in the planning and carrying out phase of the exercise. (ERR, 2014)

The National Cyber Security Strategies have highlighted the role of the EDL CU in ensuring national security. It has been served as an effort of co-operation between a public, private and third sector that led to establishing the EDL CU. EDL CU unites a wide range of experts with various backgrounds and thus provides very different insights and perspectives that could be a

valuable input during exercises, testing new solutions, and in other coordinated activities to improve cyber security in government agencies or private enterprises. The importance of EDL CU in national security stands in the fact that during a crisis situation it is possible to involve EDL CU in the activities to support civil structures and to protect critical infrastructure. (MFA 2014, 10) The Emergency "Act provides for the legal bases for crisis management, including preparing for and resolving an emergency as well as ensuring the continuity of vital services. This Act also governs the declaration, resolution and termination of an emergency situation, the involvement of the Defence Forces and the Defence League in resolving an emergency that has led to the declaration of an emergency situation, and state supervision and liability." (Emergency Act, 2017).

2.2.5.1. Potential of co-commissioning

Many interviewees pointed out that while the 2007 cyber attacks caught state agencies by surprise, the private sector experts had already experienced a number of larger DDoS attacks against businesses and established networks to respond cyber attacks (I1, I5, I7, I9). It became evident that private sector experts were needed to develop a comprehensive national cyber security strategy that would address the threats and vulnerabilities revealed in 2007. Taking this into consideration, it would be expected that the same cyber security experts who voluntarily helped to resolve the 2007 incident were also involved in developing the Estonian first cyber security published already in 2008.

A more concrete and better-documented example of co-commissioning comes out from the second Estonian cyber security strategy where the important role of national and international cyber defence exercises was emphasised in developing and accessing cyber security capabilities. One exercise highlighted is the government level cyber defence staff exercise "Cyber Fever" held in 2012 (Cyber security strategy 2014-2017, 3). The elaborate scenario of large-scale exercise included power outage in Estonia's second most populous city Tartu, interruptions in external internet connections causing significant disruptions to the availability of cash and the operation of payments and settlements, as well as compromise of data in national databases and much more. (EDL 2021)

A 16-member group from EDL CU Union team was in office to develop the right messages, and all ministries were involved. EDL CU Lieutenant Meiel considers the exercise a success

and is most pleased to see the real impact of Cyber Fever. According to Lt. Meiel several ministries changed their protocols before and after the exercise (Kaitse Kodu 2012, 5) Meiel pointed out that one of the political decisions that was made as a consequence of this exercise was that the big banks were not given the permission to move their server farms outside from Estonia, even though it would have been more cost-effective solution for the banks. (EDL 2021) This is an example of co-production in resilience stages of plan and adapt.

EDL CU improved their methodology in the US Department of Homeland Security, but the foundations of the tactical-level staff exercise they received had to be thoroughly redesigned for the government level. The methodology had to be changed and the factors that deliver the right messages to the government had to be found.

In interviews with experts no concrete examples of recent official requests to EDL CU would have received an official request to be involved in co-commissioning activities. However, the wide network of EDL CU connects members from different private sector companies, Individual contacts with the members and between the members may be the source for informal advice. Co-commissioning activities focused on setting goals or priorities are rather gathered through informal channels or through using individual contacts facilitated through the network (I7, I9). Setting goals and priorities and overall policy design is a time-consuming task this is rather seen as a work of a paid professional and could conflict with the volunteer motivations. One of the values of having EDL CU is the mediation of an informal network. This creates an access to individuals with certain expertise.

2.2.5.2. Potential of co-design

While the 2007 cyber incident did highlight the importance of cyber security for Estonian society, there is currently not a single educational program that trains cyber security specialists. Even though the Estonian Cyber Security Strategy 2019-2022 has addressed the need to develop a training system for cyber security specialists in the field, at the moment there is no coherent approach on how to educate public sector security specialists on the field of cyber security. Today cyber security education is provided as an elective by a Masters' program in the Estonian Academy of Security Sciences (CSS 2019-2022, 39). Even though there is a growing demand for cyber security specialists on the field, it seems like EDL CU has been offering an opportunity for interested specialists to learn and develop problem-solving

mentality. Practical experiences from the exercises and the opportunity to work with real incidents have been an alternative filling the gap of missing training systems for cyber security specialists. This accompanied by a potential motivational factor why is EDL CU attractive for cyber security professionals. The simple fact that the state has the monopoly of developing offensive cyber capabilities (I1). EDL CU is providing an opportunity for cyber security related IT specialists to complement their knowledge and experience with practical assignments.

The members of EDL CU were closely tied with initiating the International Cyber Defence Exercise Locked Shields and one of the organizers. Exercise tests the defence skills of IT experts under real-life conditions and provides an invaluable opportunity to practise cooperation with cyber defence experts from different nations. (CCDCOE 2013) Collaboration with the community of cyber experts to test cyber security processes gives ideas and improves the overall design of service security protocols. Exercises are showing in what areas co-production can be improved and essential for planning. If already involved in exercises, then organizers need also take into considerations the feedback from EDL CU.

2.2.5.3. Potential of co-delivery

Events in 2007 led to concrete legal steps to find a way how government agencies could involve cyber expert citizens in large-scale cyber incident response. In 2013 a change in the EDL statute was made to enable EISA to involve EDL CU members for CIP assistance in case of incidents. The explanatory memorandum to the bill provided an example of how in the case of cyber attacks in 2007, at one point the online banking services were not available due to the volume of electronic information requests. The procedure provided in this Regulation was updated to enable EISA to involve EDL CU in a similar situation to restore access to the service faster. To this end, EDL CU can, for example, perform network monitoring to identify the electronic communication channels used for attacks, the closure of which by the RIA allows the service to be restored. (MoD 2013, 1)

One of the most recent examples of co-delivery in national cyber security improving service efficiency and quality through co-delivery is from April 2020. Estonian Health Board crisis team made a request to the EDL CU for volunteer analysts and ICT specialists to assist creating a dynamic and rapid picture of the fight against COVID-19 using various data sources. They had identified that COVID-19 related data was processed in different non-compatible systems,

that slowed the organizations work processes remarkably and a more efficient tool was needed for information processing. The volunteers of the EDL CU were supported in their activities by conscripts from the Cyber Defence Command of the Defence Forces together with active members of the Cyber Defence Command. (Lõunaeestlane 2020)

Among four Co's of co-production co-delivery seems to have the most potential for government officials and co-producers to find common ground and work together without being affected by the limitations otherwise common to the sphere of national security. Most connected to the citizens motivation

If interviewees were asked in which areas there is potential for citizens to become more involved in national cyber security, then government officials (I5) pointed out the need to raise awareness of the wider public. Uncertainty characteristic to the cyber sphere creates a never-ending need to raise the public awareness on the dangers posed by malicious actors and consequences of poor cyber hygiene. Even if the information systems and databases are not that easily penetrable there is always room for the human error. No matter how good technical solutions are applied to protect the e-services there is no guarantee that this would not be bypassed by exploiting the poor cyber hygiene of the users or the active work of malicious actors phishing for information form the users. While on elaborating on citizens role in cyber security all interviewees agreed that the first thing that citizens can do for cyber security is to be informed and aware of the dangers in cyber environment.

Joint activities to co-influence behaviour change of the citizens or specific service users are actually one key aspects in improving the cyber security environment. In the Cyber security Strategy for 2019-2022, it is addressed that more in-depth training and cyber-security training has mostly been up to this day project-based and in cooperation with the CDL and TalTech. (MEAC 2019). However, the project-based solution does not support educating specialists with regularity and at the same time it is difficult to measure the impact of these kind of campaigns, it is a one possible solution how to respond to the emerging threats. It is vital to address the need for this kind of lower-level trainings that EDL CU has conducted in smaller communities for schools and hospitals.

At the moment there are no joint initiatives tackling citizen's digital literacy and awareness. Government agencies have their policy planning processes and EDL CU joins these kind initiatives usually if there is a direct request from government agency or local authority (I1).

But one of the lessons from the 2017 ID-card crisis was that there is an ongoing need to invest in improving the digital literacy and awareness of the citizens. As state agency professionals cannot and maybe also should not reach to every citizen, EDL CU has established itself as a trustworthy partner in raising public awareness. EDL CU is a valuable project-based partner in raising awareness and training the other public service providers in the health sector and educational sector. (I1)

The government agencies and volunteers themselves agreed that the main role of the EDL CU is to be the force multiplier during the time of need and the co-production of public services is often seen as too time demanding and motivation draining for volunteers. For example, during the ID-card crisis, EDL CU was requested to help with media space monitoring to detect if there are any hidden information campaigns. (I1) The citizens' "insider view" is not given then in a form of redesigning the services or strategies in a long-term view but more in the form of real-time trend monitoring and threat detection. These are more time-consuming background processes of the incident that could change the threat environment remarkably if materialized. However, the accumulation of this kind of reporting, data or information collection can be seen as a considerable input to the materials that may be a basis for decision making processes.

Opportunities have been created for the use of EDL CU in crisis situations, where the unit can be used to support civilian structures and protect critical infrastructure. (KJS 2014)

2.2.5.4. Potential of co-assessment

Outside perspective can be helpful in detecting aspects that people working in a same organization or a system otherwise may overlook. Just before the ID-card crisis became evident government agencies had filled a survey asking to assess how much do they think they depend on ID-card in their everyday work. The majority of the respondents answered that they did not recognize being dependent on the ID-card solution. The realization of how many government agencies were actually depending on this technical solution came after a few months when the ID-card crisis took place. (I6) This demonstrates clearly how everyday users of these technical solutions have a hard time to understand the real implications of not being able to use these systems.

A common way how to enhance resiliency is to improve readiness for emergencies through joint exercises. Cyber exercises are an opportunity to practice for situations where co-delivery is needed to absorb and respond to cyber incident disrupting provision of critical services. On the other hand these exercises also provide an opportunity to assess the existing capabilities, information exchange and protocols already in place. In 2018 EISA organized an exercise "Kübersiil" (*cyber hedgehog*) focusing on securing the continuity of the vital services of different sectors. This involved MoD, EDL CU, CIPs like two main hospitals of Estonia, Pärnu and Central Hospital of Ida Viru, the port of Pärnu and Alexela and Tax and Customs Board of Estonia. Aim of exercise was to prepare public authorities and businesses responsible for providing to practice operating vital services in the event of a real cyber attack. (ERR 2018) Meanwhile introducing the action plan and logic of the vital service systems to citizen volunteers who have the professional expertise to support the same system in a crisis. As information on these exercises is usually limited to the public statements, it is difficult to estimate the citizens role in planning and assessment activities. While cyber security and resilience depends how well we can use our collective brain (I6, EISA 2021), the potential of co-assessing the joint exercises is evident and a small step to improve the exercise quality.

For example, the Baltic Ghost exercise where the scenario envisaged hackers' attack posing a threat to the supply of electricity different companies providing vital services (energy company Elering), state agencies (MoD, EISA) and EDL CU volunteers exercised joint incident response. Exercise took place simultaneously in three Baltic states and involved vital service providers, critical infrastructure owners, state institutions and volunteers from EDL CU (Elering, 2016). Exercises with CIPs help to test inter-organizational information exchange during cyber incidents and also to practice and improve the procedures in place to provide the needed external support for service providers. This prepares EDL CU volunteers to enhance respond and recover stages of resilience.

In times of crisis, things will not work on their own. There is no point to assume that we still act calmly as every day. And when there is a crisis, we can suddenly do everything. Training is also important. This same triangle of companies, the state and volunteers are constantly practicing together. Collaborative systems, are about getting to know each other, understanding each other's headaches and what are the actual problems. (I9)

3. Discussion

While co-production is evident in most of the public services, it has often not been the case in the sphere of national security. The cyber attacks against Estonia in 2007 led politicians and public managers to understand the importance of cyber security from the perspective of national security and the potential of having citizens involved in co-producing cyber resilience. As the citizen supported response to cyber incident has been often characterised as "õhinapõhine" (led by volunteer vigour) there is reason to believe that citizens with cyber security expertise are motivated to contribute their time and skills if CIs and CIIs are under threat. Theoretical framework was created to focus on four co-production activities in four stages of resilience. Based on that different opportunities were proposed where citizen involvement could contribute in cyber security and enhance CI's and CII's cyber resilience. In discussion this table is filled with examples of EDL CU co-production activities (see Table 3).

Estonia is one of the most digitalized countries and as the ID-card crisis in 2017 demonstrated increasing number of e-services do have no physical alternatives (I4, I5). This is also why the Estonian Cyber Security Strategy has highlighted enhancing the cyber resiliency as one of the main goals. Even though there is no clear roadmap established and there is a need for more detailed mapping to define the potential roles of the citizens in cyber security of infrastructure and e-services, stakeholders (I1, I3, I5) find that citizens have an important role in enhancing the cyber security of critical infrastructure and e-services. Citizens' more active contribution to the national cyber security can be related with the shift from risk management principles to a more stakeholder inclusive cyber resilience.

Table 3. EDL CU co-production opportunities in different stages of CI and CII cyber resilience

Four Co's of co-production	Stages of resilience			
	Plan	**Respond**	**Recover**	**Adapt**
Co-commissioning	EDL CU members may be involved in prioritising the cyber security policies and strategies.	EDL CU members may be involved in setting priorities in CI respond processes and protocols.	EDL CU members may be involved in prioritising the CIs and the aspects of services that need to be restored first.	EDL CU members may be involved in joint task forces or asked input informally on adapting priorities.
Co-design	EDL CU members may be asked informally for input on policy planning processes.	During an exercise EDL CU members may come up with a suggestion how to improve an incident respond protocol.	EDL CU members are involved in designing CI recovery plans and protocols.	Input from the exercise organised by EDL CU redesigns security protocols in banking.
Co-delivery	EDL CU organise an exercise for decision makers and public sector professionals to enhance resiliency protocols.	EDL CU is helping to monitor networks in order to detect threats that could realize during the ongoing incident.	EDL CU members with required expertise help to find solutions on how to restore services to pre-incident level.	EDL CU helps to adapt by delivering a program for the Estonian Health Board Cyber related to COVID-19 crisis.
Co-assessment	EDL CU takes part in exercises that assess the readiness of stakeholders and the resilience of CI's.	EDL CU organized an exercise Cyber Fever assessed CI's incident response protocols.	EDL CU organized an exercise Cyber Fever that assessed processes to restore CI's services.	EDL CU members are involved in testing the updated e-voting software.

Source: Author

In the **plan** stage of resilience phase, public sector professionals have the leading role and an opportunity to involve different stakeholders and citizens through exercises. Some interviewees (I1, I2, I5) suggested that the coordination of further activities should be initiated by professionals from government agencies managing the coordinated activities to enhance cyber security of critical infrastructures and e-services. Volunteers are motivated to contribute as long as they feel they can do something meaningful. Co-producing activities in the plan stage of resilience lay the foundation for the stages respond and recover of the resilience. Interviews revealed that co-production may take in a plan stage on an informal level (I7, I9). Public sector professionals who are EDL CU members or have good contacts with EDL CU

may ask input informally. So far there has not been a clear indication from EISA on what competencies are most likely needed from the citizens to support the critical infrastructures in crisis situations (I1, I2, I3, I5).

In the **respond** stage of resilience, citizens' contribution to cyber security has the greatest impact in example of the 2007 and 2017 events. Continued functioning of the vital services or e-services may depend on the manpower available for tasks that require specific expertise. Citizens are seen as force multipliers who can help through tackling the incident to co-deliver the responding and absorbing phases of resilience. In some cases, they may be the second shift for incident response (I2). EDL CU volunteers and citizens not affiliated with EDL CU have demonstrated readiness in both crises and have helped government professionals with their expertise to protect Estonia's national cyber security. In the 2007 example, cyber security specialists who had experiences with solving similar incidents in private sector became an invaluable resource during the stage of respond (I7).

Both cyber security incidents, which have been covered in this thesis, demonstrated how citizens were motivated to provide help to the government professionals. However, to enhance resilience in the stages of respond and recover it would be wise not to necessarily depend on coincidences and instead map and plan these resources available for crises. It would also be a stretch to name these coincidental acts of citizens contributing to cyber security as co-production while this thesis uses the Loeffler's definition of co-production that emphasizes the importance of long-term nature of the relationship between professionals and citizens. Long-term aspect of co-production comes into play with the aftermath of 2007 cyber attacks when EDL CU was established.

One aspect why the **recover** stage of resilience was in both incidents enhanced by citizens and private sector firms was the sense of mission and the wish to protect the environment where we operate in our day-to-day activities. There was an understanding that the business environment in which firms operate was under threat. (I7, I9) The banks that were targeted by the attacks were clearly motivated to restore their online services just like public sector's motivation was to not lose citizens' trust in the security and availability of their services.

The 2007 cyber attacks against Estonia showed that **adapting** with the new situation needed the support from the citizens who had cyber security expertise. After the incident cyber security came to political awareness on national and on the international level. Citizens who had worked

on cyber security matters in private sector and had encountered attacks like these before and were helping government organizations during the crisis and later helped to form strategies, start institutions and shape regulations. Exercise “Cyber Fever” that was co-delivered in 2012 by EDL CU and government professionals from different ministries resulted in renewed protocols for ministries and led to adapting a policy where banks could not take their server farms outside from Estonia.

In Estonian case public sector’s motivations to involve citizens have been quite clearly communicated and written in the legal framework. Volunteer cyber security experts are valued partners in co-delivering respond and recover stages of resilience. Citizen cyber security experts have proved that they are motivated to protect Estonian e-way of life. There is a mutal understanding that complex and large-scale incidents cannot be resolved without the help of private sector and volunteering citizens (I1-I9).

Public sector professionals and EDL CU members voiced caution on burdening volunteer citizen input in national cyber security services. There is some healthy scepticism about the potential of using volunteer workforce in services provision on a regular basis. Any potential initiatives increasing the role of EDL CU seems to be analysed from the perspective as if government agencies try to find a cost-effective solution and how to source out time-consuming and repetitive tasks that could hurt the voluntary motivation. When asked how volunteer citizens could help to improve the national cyber security services, the same concern is also reflected in the answers of the experts from the government agencies. The citizen's motivation to contribute to the national cyber security is recognized as a valuable asset and there is a precaution to not overuse it.

In the legal framework during a crisis EDL CU volunteers are defined as reserves to ensure CI protection and therefore the citizens’ role in national cyber security is mainly seen as a force multiplier. Based on the framework this means that the citizens help to co-deliver in the stages of respond and recover of CI resilience. As the 2007 and 2017 incidents demonstrated, citizens are motivated to co-deliver if they feel that the threats cause disturbances in normal day-to-day life and affect the normal functioning of the Estonian society. This citizen motivation to protect Estonia and it’s e-way of life is combined with the private sector businesses’ incentive to protect their business environment in the cyberspace (I1, I5, 17, I9).

It appears that the government agencies apprehend very well that co-production with citizens is not a way to save money in their budgets. On the contrary, there is an understanding that it takes a considerable amount of resources to assure that volunteers could acquire and maintain a certain level of expertise necessary to support vital services. These skills are very specific and may not be related to the daily work of the volunteers. The information systems are constantly updating and changing which means that there are no one-time investments in this sphere (I1, I2, I3, I5). The readiness of the reserve can only be guaranteed by making sure that necessary exercises are held regularly.

Besides stressing the importance of annual exercises with volunteer cyber security experts, professionals working in the government agencies (I4, I5, I6, I8, I9) have emphasized that one of the main pillars of national cyber security is citizen awareness. While it is important to have access to trained specialists who can help to respond if/when complex critical infrastructures and e-services have large-scale incidents, citizen awareness and elemental cyber hygiene is an important pillar of resilience in national cyber security. Project-based awareness campaigns are easily achievable co-production activities that could be co-delivered to improve cyber resilience. It is important to emphasise the project-based aspect of awareness campaigns as interviewees stressed the effect of routine work having on the volunteer motivation. There is a fine line between the activities EDL CU volunteers are motivated to participate in and activities that are considered to be repetitive or too time-consuming and therefore non-meaningful.

CONCLUSION

The widespread use of ICT technologies in almost every aspect of our lives and in our interconnected economies has created vulnerabilities in the critical infrastructures and e-services vital for countries' national security. We recognize how our dependence on ICT solutions is growing while the number and complexity of cyber incidents increases. Effective national cyber security is dependent on stakeholder cooperation and is not limited anymore only to taking protective measures. The focus in crisis management and cyber security has moved towards understanding the need to enhance resilience, which provides for an expansion of those responsible for cyber security.

This thesis focused on the role of Estonian citizens in the EDL CU volunteers in the cyber security of critical infrastructure and e-services. A framework in combination of co-production and resilience was created to assess the potential roles that citizens have in national cyber security and in enhancing cyber resiliency. To answer the research question, key aspects of citizen co-production in cyber security were mapped through analysing Estonian cyber security policy processes and developments that took place after the cyber incidents in 2007 and 2017.

What is the citizens' role in improving the national cyber security for e-government services and critical infrastructures?

When co-production is categorized in Four Co's then it is evident that in certain aspects the sphere national security has posed barriers for co-production. This is addressed however with a strong institutional and legal framework so the government agencies responsible for national cyber security could form relations with trusted citizen partners.

The 2007 cyber attacks demonstrated how large-scale incidents create potential for co-production between citizens and public sector professionals. Citizens and government agencies are motivated to work together to tackle large-scale incidents threatening the CI's and CII's.

There is an evident need to have better structures in place to use potential of volunteer cyber specialists. Over the years, the role of EDL CU in national cyber security has been formalized in policy documents and cooperation agreements. Having a legal framework in place was an essential step to establish regular relationship of cooperation in aspects important for national cyber security. The situations where there is a need for quick support from "outside experts"

to assure everyday work of vital services demands trustworthy experts. EDL CU is a platform for that and gives an opportunity to exercise the cooperation between volunteer cyber security experts and vital services providers from different sectors in an environment of trust. Making it possible to create social connections between the vital service providers and cyber security experts who could provide assistance in a time of need. EDL CU has made society more resilient by creating a reserve of citizens with specific skills to help private sector specialists with a training, know-how and experience on how to react in case of certain incidents. Personal contacts between EDL CU members and vital service providers are necessary to reduce the learning curve during the crisis (I1, I2, I4, I5).

EDL CU involves citizens with a wide range of specific skills. As it was indicated by the interviewed experts, during the ID-card crisis EDL CU was not tasked with a specific role. Instead of being involved in the incident as a volunteer organization there were volunteer specialists of which some are members of CU. The importance of informal networks of cyber security specialists is still relevant to find a faster access to pool of experts during large-scale incidents. As systems of systems are becoming increasingly complicated it is impossible for government agencies to have sufficient sector-based knowledge to offer support for vital service providers.

There is an understanding among the experts that with the growing digitalization of services and cyber threats accompanying these processes the potential role of EDL CU in national cyber security should grow. To be able to act successfully as the force multiplier in a crisis situation, EDL CU is involved in cyber security exercises with the agencies responsible for cyber security and critical infrastructure providers who are potential targets in the crisis. There is no support to involve EDL CU to the "provision of services" of national cyber security that were provided by professional earlier. The potential role of EDL CU in securing the national cyber security has been defined in the Emergency Act, however, there is room to improve also through bilateral cooperation agreements between EDL CU and governmental agencies.

Acknowledgements

Soovin tänada enda juhendajaid Robert Krimmerit ja Gerli Aavik-Märtmaad. Robert, aitäh Sulle sinu kannatlikkuse ja eluterve suhtumise eest. Gerli, aitäh Sulle, et oled olnud äärmiselt suureks toeks enda väsimatu positiivsusega. Paremat kaasjuhendajat ei oleks ette kujutanud.

Sooviksin veel tänada Ragnar Nurkse Instituudi töötajaid. Eriliselt suured tänud Margit Kirsile ja Piretile Kährile julgustavate sõnade ja lõputu abivalmiduse eest.

Lõpuks soovin tänada enda peret ja kallist elukaaslast Kristiinet, kelle tagalatoeta poleks see võimalik olnud.

Toetust saadi H2020 teadus- ja innovatsiooniprogrammi kaudu toetuslepingu nr 857622 alusel.

Summary in Estonian

Elutähtsate teenuste küberjulgeoleku ja -kerksuse koosloome Eesti Kaitseliidu Küberkaitseüksuse juhtumi näitel

Taavi Turu

Resümee

Informatsiooni ja kommunikatsioonitehnoloogia lahenduste kiire levik kriitiliste infrastruktuuride juhtimissüsteemidesse ning avaliku sektori teenustesse on endaga kaasa toonud teenuste tõhususe ning kvaliteedi kasvu. Viimase kahe aastakümne jooksul on suurenenud ühiskonna sõltuvus IT-lahendustest, kuid samuti on kasvanud ka küberohud. Lisaks tehnilistele riketele ohustavad IT süsteemidel tuginevaid eluliselt tähtsaid teenuseid ja e-teenuseid järjest rohkem küberrünnakud. Suuresti erasektorile kuuluvad eluliselt tähtsate teenuste turvalisus on saanud rahvusliku julgeoleku seisukohast oluliseks küsimuseks.

Käesolev magistritöö analüüsib, kas ja kuidas on võimalik kodanikel aidata parandada Eesti eluliselt tähtsate teenuste ja e-teenuste küberturvalisust. Eestit peetakse üheks enim digitaliseerunud riigiks ja suunanäitajaks e-teenuste kasutuselevõtul (RIA 2019) ning seetõttu on küberturvalisus rahvusliku julgeoleku seisukohalt äärmiselt oluline. Eesti on heaks juhtumiks, mida küberturvalisuse kontekstis uurida ka tänu kodanike ja vabatahtlike panusele küberjulgeolekusse suuremate küberintsidentide ajal aasta 2007 ja 2017. Töö annab hinnangu Eesti küberjulgeoleku poliitika edule kodanike kaasamisele küberkerksuse aspektist.

Magistritöö jaguneb kolmeks suuremaks osaks. Töö teoreetiline osa tutvustab kriitilise infrastruktuuri- ja informatsioonisüsteemide küberturvalisusele keskendunud akadeemilist kirjandust ning toob esile kuidas küberjulgeoleku diskussioonis on hakanud nihkuma fookus küberkaitselt küberkerksusele. Lisaks tutvustatakse koosloome (co-production) teooriat, mis rõhutab avalike teenuste planeerimisel (co-commissioning), kujundamisel (co-design), osutamisel (co-planning), ja hindamisel (co-assessment) teenuseid osutavate professionaalide ja kodanike koostöö olulisust teenuste kvaliteedile ja mõjule. Eesti näite põhjal kaardistab empiiriline osa kodanike potensiaalsed rollid rahvuslikus küberjulgeolekus. Keskenduses kahele suuremale küberjulgeolekut ohustanud sündmusele 2007. a küberrünnak ja 2017. a ID-kaardi kriis kaardistab töö kodanike rolli neljas kerksuse faasis planeerimine (plan),

reageerimine (respond), taastumine (recover) ja kohanemine (adapt). Magistritöö diskussiooni osa arutleb juhtumianalüüsi leidude üle ja vastab töö alguses püstitatud uurimusküsimusele. Magistritöö kasutab kvalitatiivset üksikjuhtumianalüüsi ning empiirilised andmed on kogutud läbi dokumendianalüüsi ning autori poolt läbi viidud poolstruktureeritud intervjuudega.

Tuginedes empiirilistele andmetele saab antud töö analüüsist järeldada, et Eestil juhtumi näitel on kodanikel olnud arvestatav roll rahvusliku küberjulgeoleku parandamisel. Magistritöös vaatluse all olnud 2007. a ja 2017. a toimunud intsidentide näitel on kodanikel olnud arvestatav roll e-teenuste turvalisuse tagamisel. Kodanike võimalikku rolli nähakse eeskätt Eestis küberturvalisuse võimendajatena, mis on määravaks mahukate või ajakriitiliste ülesannete täitmisel. Selle üleval hoidmiseks korraldatavad õppused annavad kodanikele võimaluse rääkida kaasa rahvusliku küberturvalisuse tagamisel. Arenguruumi on end vabatahtliku küberjulgeolekuga sidunud kodanike ekspertiisi potenstisaali sihipärasel kaardistamisel ning kriisiaja ülesannete planeerimisel.

REFERENCES

Academic literature

Alford, J. (2002) “Why Do Public-Sector Clients Coproduce? Toward a Contingency Theory”, *Administration & Society*, 34(1): 32-56.

Alford, J., Yates, S. (2016) “Co-Production of public services in Australia: The roles of government organisations and Co-Producers”, *Australian Journal of Public Administration*, 75(2): 159-175.

Bannister, F., Connolly, R. (2011) "Trust and transformational government: A proposed framework for research", *Government Information Quarterly*, 28(2): 137-147.

Björklund, F. (2016) “E-Government and Moral Citizenship: The Case of Estonia.” *Citizenship Studies,* 20(6–7): 914-931.

Boeke, S., Heinl, C. H., Veenendaal, M. A. (2015) “Civil-military relations and international military cooperation in cyber security: Common challenges & state practices across Asia and Europe”, *7th International Conference on Cyber Conflict: Architectures in Cyberspace*, Tallinn, 69-80.

Boin, A., McConnell, A. (2007) “Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience". Journal of Contingencies and Crisis Management, 15(1): 50-59.

Boin, A., Lodge, M. (2016) “Designing Resilient Institutions for Transboundary Crisis Management: A Time for Public Administration.” *Public Administration*, 94(2): 289-298.

Bovaird, T. (2007) “Beyond engagement and participation: User and community coproduction of public services.”, *Public administration review*, 67(5): 846-860.

Bovaird, T., Loeffler, E., (2012) “From engagement to co-production: The contribution of users and communities to outcomes and public value”, *Voluntas: International Journal of Voluntary and Nonprofit Organizations*, 23(4):1119-1138.

Bovaird, T. and Loeffler, E., (2013) “We’re all in this together: harnessing user and community co-production of public outcomes.” Birmingham: Institute of Local Government Studies: University of Birmingham, 1(2013): 15.

Bovaird, T., Van Ryzin, G.G., Loeffler, E., Parrado, S., (2015) “Activating citizens to participate in collective co-production of public services”, *Journal of Social Policy*, 44(1): 1-23.

Bovaird, T., Stoker, G., Jones, T., Loeffler, E., Pinilla Roncancio, M., (2016a) “Activating collective co-production of public services: influencing citizens to participate in complex governance mechanisms in the UK”, *International Review of Administrative Sciences*, 82(1):47-68.

Bovaird, T., Loeffler, E., (2016b) “What has co-production ever done for interactive governance?” In J. Edelenbos, & I. van Meerkerk (Eds.), Critical reflections on interactive governance. Cheltenham, UK: Edward Elgar.

Boyle, D., Harris, M., (2009) “The challenge of co-production”, London: new economics foundation, 185-194.

Brandsen, T., Pestoff, V., (2006) “Co-production, the third sector and the delivery of public services: An introduction.”, *Public management review*, 8(4), 493-501.

Brandsen, T., Honingh, M., (2016) “Distinguishing different types of coproduction: A conceptual analysis based on the classical definitions.” *Public Administration Review*, 76(3): 427-435.

Brandsen, T., Steen, T., Verschuere, B., (2018) “Co-production and co-creation: Engaging citizens in public services” (p. 322). Taylor & Francis.

Bostick, T.P., Connelly E.B., Lambert, J.H., Linkov I., 2018) “Resilience Science, Policy and Investment for Civil Infrastructure.”, *Reliability Engineering and System Safety*

Brechbühl, H., Bruce, R., Dynes, S., Johnson, M. E. (2010) “Protecting Critical Information Infrastructure: Developing Cybersecurity Policy.” *Information Technology for Development*, 16(1): 83-91.

Brudney, J.L., England, R. E., (1983) “Toward a definition of the coproduction concept”, *Public Administration Review*, 43(1): 59-65.

Carr, M., (2016) “Public–private partnerships in national cyber-security strategies”, *International Affairs*, 92(1): 43–62.

Coaffee, J., de Albuquerque, J.P. and Pitidis, V., (2021) “Risk and Resilience Management in Co-production“, In *The Palgrave Handbook of Co-Production of Public Services and Outcomes* (pp. 541-558). Palgrave Macmillan, Cham.

Czosseck, C., Ottis, R., Talihärm, A. (2011) “Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security” *International Journal of Cyber Warfare and Terrorism (IJCWT)*, 1(1): 24-34.

Dunn-Cavelty, M., Suter, M., (2009) “Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection.” *International Journal of Critical Infrastructure Protection*, 2(4): 179-187.

Dutton, W., Guerra, G. A., Zizzo D. J., Peltu, M., (2005) “The Cyber Trust Tension in E-Government: Balancing Identity, Privacy, Security.” *Information Policy,* 10(1, 2): 13-23.

Flyvbjerg, B., (2006) “Five misunderstandings about case-study research.“ *Qualitative inquiry*, *12*(2): 219-245.

Fugini, Maria Grazia, Enrico Bracci, and Mariafrancesca Sicilia, eds. (2016) “Coproduction in the Public Sector: Experiences and Challenges”, Milan: Springer.

Goodwin, C.F., Nicholas, J.P., (2013) “Developing a National Strategy for Cybersecurity”

Harrop, W., Matteson, A., (2015) “Cyber resilience: A review of critical national infrastructure and cyber-security protection measures applied in the UK and USA.“ *Current and emerging trends in cyber operations*, 149-166.

Joshi, A., Moore, M. (2004) “Institutionalised co-production: unorthodox public service delivery in challenging environments”, *Journal of Development Studies*, 40(4): 31-49.

Keys, B., Shapiro, S. (2019) Frameworks and Best Practices

Lember, V. (2017) “The increasing role of digital technologies in co-production.” The other canon foundation and Tallinn university of technology working papers in technology governance and economic dynamics.

Linkov, I., Eisenberg, D.A., Plourde, K., Seager, T.P., Allen, J., Kott, A. (2013) “Resilience metrics for cyber systems.” *Environment Systems and Decisions*, 33(4): 471-476.

Linkov, I., Kott, A. (2019) “Fundamental concepts of cyber resilience: Introduction and overview. ” In *Cyber resilience of systems and networks* (pp. 1-25). Springer, Cham.

Löffler, E., Parrado, S., Bovaird, T. and Van Ryzin, G. (2008), “If you want to go fast, walk alone; if you want to go far, walk together”: Citizens and the co-production of public services’, French Ministry of the Treasury, Public Accounts and Civil Service, on behalf of the Presidency of the EU, Paris.

Loeffler, E., Bovaird, T. (2016) “User and Community Co-Production of Public Services: What Does the Evidence Tell Us?”, *International Journal of Public Administration*, 39(13): 1006-1019.

Loeffler, E., (2021) “Co-Production of Public Services and Outcomes.” Palgrave Macmillan. 1-444

Luiijf, E., and Marieke Klaver. (2015) “Governing Critical ICT: Elements That Require Attention.” *European Journal of Risk Regulation,* 6(2): 263-70.

Mahoney, J., Goertz, G. (2006) “A Tale of Two Cultures: Contrasting Quantitative and Qualitative Research.” *Political Analysis,* 14(2): 227-249.

Mansfield-Devine, S. (2012) “Estonia: what doesn't kill you makes you stronger.” *Network security*, (7): 12-20.

Nabatchi, T. (2017) “Varieties of Participation in Public Services: The Who, When, and What of Coproduction” *Public Administration Review*, 77(5): 766-776.

Nesti, G., (2018) “Co-production for innovation: the urban living lab experience.” *Policy and Society*, 37(3): 310-325.

Nye Jr, J.S., 2017. “Deterrence and dissuasion in cyberspace”, *International Security*, 41(3): 44-71.

OECD (2011). “Government at a Glance 2011” OECD Publishing 268

Osborne, S. P. (2010) “Delivering public services: time for a new theory?”, 1-10.

Osborne, S. P. (2018) “From public service-dominant logic to public service logic: are public service organizations capable of co-production and value co-creation?”, *Public Management Review*, 20(2): 225-231.

Osborne, S.P., Radnor, Z., Strokosch, K. (2016) “Co-production and the co-creation of value in public services: a suitable case for treatment?” *Public Management Review*, 18(5): 639-653.

Ostrom, E. (1996) “Crossing the Great Divide: Coproduction, Synergy, and Development.” *World Development*, 24(6): 1073-1087.

Rajamäki, J., Nevmerzhitskaya, J., Virág, C. (2018) “Cybersecurity education and training in hospitals: Proactive resilience educational framework (Prosilience EF). ” In 2018 IEEE Global Engineering Education Conference (EDUCON) (pp. 2042-2046). IEEE.

Rich, R. C. (1981) “Interaction of the Voluntary and Governmental Sectors: Toward an Understanding of the Co-Production of Municipal Services”, *Administration & Society,* 13(1): 59-75.

Roege (2017) Bridging the Gap from Cyber Security to Resilience

Setola, R., Luiijf, E., Theocharidou, M., (2016) “Critical infrastructures, protection and resilience”, In Managing the Complexity of Critical Infrastructures (pp. 1-18). Springer, Cham.

Sicilia, M., Enrico G., Alessandro S., Martino A., Renato R. (2016) “Public Services Management and Co-Production in Multi-Level Governance Settings” *International Review of Administrative Sciences*, 82(1): 8-27.

Surva, L., Tõnurist, P., Lember, V. (2016) “Co-production in a network setting: providing an alternative to the national probation service”, *International Journal of Public Administration*, 39(13): 1031-1043.

Torfing, J., Sørensen, E., Røiseland, A. (2019) “Transforming the public sector into an arena for co-creation: Barriers, drivers, benefits, and ways forward”, *Administration & Society,* 51(5): 795-825.

Tõnurist, P., Surva, L., (2017) “Is volunteering always voluntary? Between compulsion and coercion in co-production”, *VOLUNTAS: International Journal of Voluntary and Nonprofit Organizations*, 28(1): 223-247.

Voorberg, W., Bekkers, V.J.J.M., Tummers, L. (2013) “Co-creation and co-production in social innovation: A systematic review and future research agenda” In Proceedings of the EGPA Conference, pp. 11-13.

Voorberg, W. H., Bekkers, V. J. J. M., Tummers, L. G. (2015) “A Systematic Review of Co-Creation and Co-Production: Embarking on the social innovation journey”, *Public Management Review*, 17(9): 1333-1357.

Warfield, D. (2012) “Critical Infrastructures: IT Security and Threats from Private Sector Ownership”, *Information Security Journal: A Global Perspective*, 21(3): 127-136.

Weiss, M., Jankauskas, V. (2019) “Securing cyberspace: How states design governance arrangements”, *Governance*, 32: 259–275.

Whitaker, G. P. (1980) "Citizen Participation in Service Delivery", *Public Administration Review*, 40(3): 240-246.

Wirtz, B. W., Weyerer, J. C. (2017) “Cyberterrorism and Cyber Attacks in the Public Sector: How Public Administration Copes with Digital Threats”, *International Journal of Public Administration,* 40 (13): 1085–1100.

Yin, R. K. (2003) The Role of Theory in Doing Case Studies. In Applications of Case Study

Other literature

Delfi (2018) “Kaitseliidu küberkaitseüksuse pealik: oleme kokku tulnud meie e-eluviisi kaitseks” Available: https://www.delfi.ee/news/paevauudised/eesti/delfi-video-kaitseliidu-kuberkaitseuksuse-pealik-oleme-kokku-tulnud-meie-e-eluviisi-kaitseks?id=74891991, accessed 10.04.2021

E-Estonia (2017) “How Estonia became a global heavyweight in cyber security” Available: https://e-estonia.com/how-estonia-became-a-global-heavyweight-in-cyber-security/, accessed 11.04.2021

E-Estonia (2021) Available: https://e-estonia.com/, accessed 12.04.2021

Elering (2016) “Küberkaitseõppus Baltic Ghost harjutab elektrivarustuse tagamist küberrünnakute korral” Available: https://elering.ee/node/116, accessed 08.05.2021

Emergency Act (2017) Available: https://www.riigiteataja.ee/en/eli/516052020003/consolide, accessed 11.04.2021

Estonian Cyber Defence League (CDL) “Frequently Asked Questions” Available: http://www.kaitseliit.ee/en/frequently-asked-questions, accessed 11.04.2021

Estonian Information System Authority (EISAa) (2016) “Annual Cyber Security Assessment 2017 Estonian Information System Authority” Available: https://www.ria.ee/public/Kuberturvalisus/RIA_CSA_2017.PDF, accessed 08.05.2021

Estonian Information System Authority (EISAb) (2016) “Critical Information Infrastructure Protection” Available: https://www.ria.ee/en/ciip.html, accessed 28.03.2019

Estonian Information System Authority (EISAc) (2017) “Possible Security Vulnerability Detected in the Estonian ID-card Chip” Available: https://www.ria.ee/en/possible-security-vulnerability-detected-in-the-estonian-id-card-chip.html, accessed 09.05.2021

Estonian Information System Authority (EISAd) (2021) "Riiklik küberüksus CERT-EE on jätkuvalt maailma parimate hulgas" Available: https://www.ria.ee/et/uudised/riiklik-kuberuksus-cert-ee-jatkuvalt-maailma-parimate-hulgas.html, accessed 09.05.2021

ERR (2014) “Küberkaitsekeskus ja Kaitseliit valmistuvad koos õppuseks Locked Shields” Available: https://www.err.ee/506144/kuberkaitsekeskus-ja-kaitseliit-valmistuvad-koos-oppuseks-locked-shields, accessed 09.05.2021

ERR (2017) “Cracking of one ID card would require Estonia to deactivate 750,000 cards” Available: https://news.err.ee/634222/cracking-of-one-id-card-would-require-estonia-to-deactivate-750-000-cards, accessed 09.05.2021

ERR (2018) “Kübersiili korraldajate sõnul tulid kõik osalejad õppusest auga välja” Available: https://www.err.ee/829768/kubersiili-korraldajate-sonul-tulid-koik-osalejad-oppusest-auga-valja, accessed 09.05.2021

ERR (2018) “Defence Forces cyber command takes up operations” Available: https://news.err.ee/850719/defence-forces-cyber-command-takes-up-operations, accessed 09.05.2021

ERR (2018) “ID-kaardi kriis maksis ametitele miljoneid” Available: https://www.err.ee/693331/id-kaardi-kriis-maksis-ametitele-miljoneid, accessed 09.05.2021

CCDCOE (2013) Available: https://ccdcoe.org/news/2013/nato-team-wins-the-locked-shields-cyber-defence-exercise/, accessed 07.05.2021

Geenius (2019) “ID-kaart lisati riiklikku küberintsidendi hädaolukorra plaani” Available: https://digi.geenius.ee/rubriik/uudis/id-kaart-lisati-riiklikku-kuberintsidendi-hadaolukorra-plaani/, accessed 09.05.2021

Kaitse Kodu (2012) “Kaitseliitlased treenisid vabariigi valitsust” Available: https://issuu.com/kaitse_kodu/docs/kaitse_kodu_marts_2012/5, accessed 11.05.2021

Lõunaeestlane (2020) “Küberväelased valmistasid terviseametile viiruseandmete infosüsteemi” Available: https://lounaeestlane.ee/kubervaelased-valmistasid-terviseametile-viiruseandmete-infosusteemi/, accessed 03.05.2021

Kaljurand, M. 2018 “How to Protect Critical Infrastructure?” Nordic-Baltic Security Summit. Available: https://summit.confent.com/summary18/, accessed 14.03.2019

Praxis (2019) “Labour force and skills needs in cyber security in Estonia Available: http://www.praxis.ee/wp-content/uploads/2018/04/Küberturbe-uuring.-Lühikokkuvõte_eng.pdf, accessed 09.05.2021

The Ministry of Defence of the Republic of Estonia (MoD) (2010) “Kaitseliidu koosseisus luuakse küberkaitseüksus” Available: www.kmin.ee/et/uudised/kaitseliidu-koosseisus-luuakse-kuberkaitseuksus, accessed 08.05.2021

The Ministry of Defence of the Republic of Estonia (MoD) (2013) Available: https://eelnoud.valitsus.ee/main#hpu0oqdF, accessed 08.05.2021

The NATO Cooperative Cyber Defence Centre of Excellence Available: https://ccdcoe.org/about-us/, accessed 08.05.2021

The Ministry of Economic Affairs and Communications (MEAC) (2019) “KÜBERTURVALISUSESTRATEEGIA2019-2022” Available: https://www.mkm.ee/sites/default/files/kuberturvalisuse_strateegia_2019-2022.pdf, accessed 08.05.2021

The Ministry of Economic Affairs and Communications (MEAC) (2014) National Cybersecurity Strategy 2014-2017 Available: https://www.mkm.ee/sites/default/files/kuberjulgeoleku_strateegia_2014-2017.pdf, accessed 08.05.2021

The Ministry of Interior Affairs Available: https://www.siseministeerium.ee/et/eesmark-tegevused/kriisireguleerimine/elutahtsad-teenused, accessed 08.05.2021

The list of abbreviations

CCDCOE - Cooperative Cyber Defence Centre of Excellence

CERT - Computer Emergency Response Team

CI - Critical Infrastructure

CII - Critical Information Infrastructure

DoS – Denial of Service

EDF - Estonian Defence Forces

EDL - Estonian Defence League

EDL CU - Cyber Unit

EISA – (the) Estonian Information System Authority

ICT – information and communication technology

IS – information systems

MEAC – (the) Ministry of Economic Affairs and Communications

MFA - (the) Ministry of Foreign Affairs

MoD – (the) Ministry of Defence

NCSS - National Cyber Security Strategy

Appendix 1 – List of Interviewees

1. **Andrus Padar**, Chief of Estonian Defence League's Cyber Unit
2. **N/A**, volunteer of the Estonian Cyber Defence League
3. **Rain Ottis**, Estonian cyber-security expert, founding member of the EDL CU researcher in NATO CCDCOE
4. **Lauri Luht**, Head of Cyber Exercises NATO Cooperative Cyber Defence Centre of Excellence
5. **Ragnar Õun**, Head of Department, Head of Critical Information Infrastructure Protection, EISA
6. **Margus Arm**, EISA Head of Department, Electronic Identity, EISA
7. **Jaan Priisalu**, cyber security expert, former Deputy Director General in EISA
8. **Toomas Vaks**, cyber security expert, former Deputy Director General in EISA
9. **Mikk Tikk**, Deputy Commander, Estonian Defence Forces Cyber Command

Appendix 2 – Interview questions

1. How did the cyber attacks against the Estonian government in 2007 change the cyber security environment and what was the role of the citizens in responding to the crisis? How did this crisis change the role of involving citizens?
2. How did the national ID-card crisis in 2017 change cyber security environment? Who were the key stakeholders in handling the crisis? (What was the role of the citizens/ EDL's Cyber Unit during the crisis?)
3. What have been the main changes in involving citizens in national cyber security from 2007 till now? How has the role of EDL CU changed during a more than 10-year period of existence? Besides EDL CU are there any other noticeable forms of citizen participation in national cyber security?
4. What are the states' motivations to use citizens' input in national cyber security? Did the financial pressure and cutbacks play any role in involving the citizens?
5. What are the risks and barriers of using volunteers in improving the national cyber security services?
6. What is the importance of having citizens in national cyber security? In which areas there is potential for citizens to become more involved in national cyber security?
7. What are the motivations of the volunteering cyber specialists and what are the potential gains they get from volunteering?
8. What is the role of citizens in protecting the critical infrastructure?
9. If and how has EDL CU contributed in solving the problem of lack of specialists in national cyber security?
10. Is there a distinction between military and civil responsibilities/services? How does the newly created Defence Force Cybercommand change the role and responsibilities of the EDL CU?