DISSERTATIONES
RERUM
POLITICARUM
UNIVERSITATIS
TARTUENSIS
31

LOGAN CARMICHAEL

Cybersecurity Governance Responses in the Estonian Digital Governance Model, 2007–2023

DISSERTATIONES RERUM POLITICARUM UNIVERSITATIS TARTUENSIS
31

DISSERTATIONES RERUM POLITICARUM UNIVERSITATIS TARTUENSIS
31

LOGAN CARMICHAEL

Cybersecurity Governance Responses in the Estonian Digital Governance Model, 2007–2023

UNIVERSITY OF TARTU
Press
1632

Johan Skytte Institute of Political Studies, University of Tartu

This dissertation has been accepted for the commencement of the degree of Doctor of Philosophy (in Political Science) on 2 February 2026 by the Council of the Johan Skytte Institute of Political Studies.

Supervisor:	Mihkel Solvak, Associate Professor of Technology Research, Johan Skytte Institute of Political Studies, University of Tartu, Estonia
Opponent:	Miguel Alberto Gomez, Senior Research Fellow, Lee Kuan Yew School of Public Policy, National University of Singapore, Singapore
Commencement:	17 March 2026 at 14:30, University of Tartu Senate Hall (Ülikooli 18)

The research work of this dissertation and the included publications were supported by ECePS ERA Chair of e-governance and digital public services, funded by the European Union's Horizon 2020 research and innovation programme under grant agreement No. 857622. Views and opinions expressed are, however, those of the author only.

Funded by
the European Union

ISSN 1736-4205 (print)
ISBN 978-9908-57-139-3 (print)
ISSN 2806-2558 (pdf)
ISBN 978-9908-57-140-9 (pdf)

University of Tartu Press
www.tyk.ee

TABLE OF CONTENTS

LIST OF ORIGINAL PUBLICATIONS

This dissertation is based on the following three original publications referred to by Roman numerals:

I **Carmichael, Logan** (2021). "Exploring Estonian e-Government Before, During, and Beyond COVID-19," *New Zealand Journal of Research on Europe.* **ETIS 1.2.**

II **Carmichael, Logan** (2025). "Crafting a Cybersecurity Governance Ecosystem: Two Decades of Learning in Estonia," *European Policy Analysis*. https://doi.org/10.1002/epa2.70017. **ETIS 1.1.**

III **Carmichael, Logan** (2025). "Lessons from Small and Highly-Digitalised Estonia: Decision-Making in the Aftermath of Cybersecurity Crises," *Internet Policy Review*, 14(3). https://doi.org/10.14763/2025.3.2028. **ETIS 1.1.**

The author of this dissertation is the sole author of all three publications.

ACKNOWLEDGEMENTS

When I committed to doing a PhD, I knew there would be challenges, but I anticipated that these would come from the academic rigour required to carry out an in-depth, multi-year study worthy of this degree. I was prepared to tackle these challenges. What I didn't anticipate were the immense challenges of being a young woman in the male-dominated tech space, which actually posed the greatest challenge of all to me as I completed the PhD you are now reading. My PhD journey was full of both thinly-veiled and outright blatant misogynistic comments, highly inappropriate and unsolicited advances from men, and comments about my appearance and my body, all overshadowing my extensive knowledge of cybersecurity governance and digitalisation. There is a reason why it is still an uphill battle for women in STEM: this field is neither friendly nor safe for young women in its current form, and that needs to change in the future.

I am, therefore, immensely grateful for the people I have in both my professional and personal life who supported me through this journey, valuing my expertise and my humanity along the way.

First and foremost, I would like to thank my supervisor, Mihkel Solvak, for his unwavering support – with thoughtful feedback, sound advice, and much-needed reminders to generalise my findings beyond the Estonian case – from start to finish of this PhD project.

Thank you to Vincent Homburg, Kerli Klock, and Varje Kuut for the immense support they provided throughout the duration of the ECePS project and beyond. Thanks also to Kristel Vits, Maili Vilson, and Piret Ehin for their support at various stages of this PhD project.

I started this journey with four fellow PhD students, all of whom were initially colleagues but have become dear friends: Art Alishani, Bogdan Romanov, Stefan Dedovic, and Biao He – thank you for being such a wonderful support system while navigating this roller coaster! I would also like to thank PhD friends, in Estonia and abroad, who have shared in this journey: Butrint Berisha, Mike Cole, Colin van Noordt, Petros Petrikkos, and Amelie Tolvin.

My friends have truly supported me through this process and I owe them an incredible amount of gratitude: Anastasiia Turusinova (we even built an entire MOOC on cybersecurity together in a ridiculous amount of time!), Vika Lukashova, Maria Urbel, Lindsay Wojtula, Salina Castle, Emma Groombridge, Emily Stadder, Sarah Da Silva-Sharma, Meg Morrow, Leah Johnson, Karmen Konnapere, Sass Adojaan, Anna Mykkänen, Masha Dudareva, Fidan Vali, and Marii-Liis Tulk. Thank you for being there through this entire journey to laugh, cry, and cheer me on.

Throughout my academic journey, I have been fortunate to have professors and mentors who have believed wholeheartedly in my potential. I am so grateful for the opportunities that they have given to me and their continued support. In Windsor: Stephen Brooks, Jamey Essex, and John Sutcliffe. In Auckland: Bernadette Luciano, Thomas Gregory, and Stephen Noakes. In Estonia: Gary McQueen and Sigurdur Palsson.

Thank you, as well, to the Estonian government officials who took the time to share their valuable insights for this project. They were all incredibly generous with their time and expertise, and this dissertation would simply not exist in its current form without their willingness to speak and share their experiences with me.

I am grateful to my team in the Data Exchange Technologies Department at Cybernetica for their patience and support as I completed the final stages of this PhD while also starting my new role in the company.

A very big thank you to my family in Canada, Ruth (and Mark), Jesse, and Reid Carmichael for cheering me on throughout this entire process. Thank you also to the extended McNae family in New Zealand for all of your support as I've embarked on this PhD. To Mitch McNae: thank you isn't big enough. You made the first trip to Estonia happen back in 2017 and have spent every day since encouraging me and believing in me on this journey.

Finally, I owe the most immense gratitude to my grandparents – Robert (Bobby) and Helen Carmichael – who believed endlessly in the opportunities that an education could bring and supported me wholeheartedly as I pursued my education and adventured, quite literally, across the globe. I am so honoured to carry on the Carmichael name, and I hope that through this PhD and the journey that I have been on, from Canada to New Zealand to Estonia, I am making them proud. This entire PhD is for them.

1. INTRODUCTION

Cybersecurity has emerged as a pre-eminent threat facing governments across the world in the 21st century. As a topic, cybersecurity traces its roots back more than half a century; without explicitly naming it as such, 'cybersecurity' or 'computer security' owes its origins to the US National Security Agency's (NSA) innovations surrounding ARPANET (the online network predecessor to the World Wide Web) in the 1960s, for "the development of practical cybersecurity methodologies," in response to a fear that, "as networks increasingly connected to one another, the risk of information becoming compromised increased."[1] Cybersecurity governance, the institutional structures and decision-making related to cybersecurity, emerged comparatively later than the technological side of the topic. Only more recently did governments begin to realise the significance and magnitude of cybersecurity and how they broached it in an organisational context; while some of the earliest instances of cybersecurity governance amongst governments began in earnest in the early 2000s, some governments are only in the earliest stages of developing cybersecurity governance processes today.[2] Cybersecurity is a concern surrounding a myriad of government functions, which includes the digitalisation of governmental service provisions. It is particularly with this scope that this project is concerned.

As countries around the world become increasingly digitalised, both predating and coinciding with the COVID-19 pandemic, so too does the 'surface area' or possibility for cyberattacks and other nefarious activities in cyberspace increase.[3] The COVID-19 pandemic saw governments increasingly digitalise and move their provisions online, in line with lockdown efforts to curb the spread of the virus. The UN noted that while "the emergence of COVID-19 revealed just how unprepared most governments were to deal with an extended global crisis," it also proved an opportunity, driving "efforts to achieve a real digital government transformation in support of building a sustainable and digitally resilient society."[4] Such sentiment has been echoed by the OECD: "most governments intensified their efforts to digitalise the public sector during the COVID-19 pandemic, with the expectation that it would enhance their resilience and responsiveness."[5] Various global metrics have tracked this increased digitalisation of public service provisions in countries across the world, developed and developing alike: between 2017–2022, the Digital Economy and Society Index (DESI) tracked EU member states relative progress in digital development as between 5% and 12% growth per year.[6] Similarly, the OECD tracked developments in the digitalisation

1 Berg, Crawford, and Seymour, 2016, p. 208.

2 Urgessa, 2020; Von Solms and Von Solms, 2018; see, for example, Hankewitz, 2020.

3 For example, Härmand, 2021; Tasheva, 2021; Praggono and Arabo, 2020.

4 United Nations, 2022, p. 170.

5 OECD, 2023.

6 European Commission, 2022.

of the public sectors of its member states between 1 January 2020 and 31 October 2022, coinciding with the onset of the COVID-19 pandemic, ultimately finding that – using a scale of 0 to 1, where 1 is the highest level of effort in forming the foundations for digital transformation – almost all of its member states reached the 0.5 threshold to "[situate] themselves in the upper half of the index."[7] While finding significant disparities in the levels of e-governance across regions of the world, especially between Europe as the most digitalised and Africa as the least digitalised, the United Nations Development Programme (UNDP) has indicated that "digitalisation is considered a key enabler and is identified as a priority for strategic programming investment" in developing countries.[8] Both the UNDP and the World Bank are extensively supporting ongoing public sector digital transformation initiatives across the developing world,[9] illuminating the reach of digitalisation processes globally.

Many newer players in the digitalisation game also experienced cyberattacks in more recent years. Examples include Costa Rica, where the government declared a state of emergency in April 2022, after ransomware attacks targeted numerous government sites;[10] Albania, which saw attacks on its fledgling e-governance structure in July 2022 by the Iranian state-sponsored group "Home-Land Justice";[11] and Moldova, whose parliament came under cyberattack in the leadup to elections and a referendum on EU membership in October 2024, with some agency information compromised by an unidentified cyber threat actor.[12] Thus, with increased digitalisation having become a trend globally, the question emerges of how to configure and carry out cybersecurity governance in a manner that secures these various digitalised initiatives. Common amongst the global reporting from international organisations or bodies outlined above, is a concern for cybersecurity surrounding digitalised governmental provisions: indeed, one particular survey has indicated that, amongst European adults, the priority in the future of digital technologies should be to "protect users from cyberattacks," with 30% of respondents expressing this concern.[13]

However, this conundrum is one that Estonia has been grappling with for longer than most of its global counterparts, having both undergone digital transformation and experienced a major cyberattack far earlier than many other states. Thus, this research project examines the ways that cybersecurity practices, policies, and governance structures aimed at securing e-governance provisions have evolved in Estonia, addressing the core research questions: *in what ways have the cybersecurity governance models aimed at securing e-governance provisions in*

---

7 OECD, 2023.

8 United Nations Development Programme, 2023.

9 World Bank, 2022; United National Development Programme, 2023.

10 Datta and Acton, 2024, p. 57–58.

11 Biberaj, et al., 2022, p. 342; CISA, 2022.

12 Antoniuk, 2024.

13 Statista, 2023.

Estonian evolved over the period of 2007 to 2023, and whether and in what ways do critical events or changed circumstances explain the changes in these cybersecurity governance models over time? Using the critical and mature Estonian case, this project aims to derive more widely applicable findings on cybersecurity governance practices, and specifically how they can be deployed to protect various digitalisation provisions. To address this overarching research question, three studies broach the topic from more specific perspectives: 1) the evolution of the Estonian e-governance model over time, 2) the evolution of the Estonian cybersecurity governance ecosystem over time and the reasons for this ecosystem's configuration, and 3) how crisis management and decision-making have unfolded in response to cybersecurity crises affecting e-governance.

These research questions have been addressed through three individual but interconnected papers. The first paper (Study I) explores the evolution of the Estonian e-governance model, from its origins to the COVID-19 pandemic, examining how pandemic-related realities prompted shifts and additions to this model. This article provides context for how cybersecurity can be governed and what potential cybersecurity concerns can emerge, as examined in subsequent papers. The second paper (Study II) examines the Estonian cybersecurity governance ecosystem, that is, how the purview for cybersecurity governance is divided within the ministries, agencies, and other entities of the Estonian government. Furthermore, this paper looks at how this cybersecurity ecosystem has been formed and shaped over time, and how the term 'cybersecurity governance' is understood across the government, particularly looking at the practical realities resulting from this. The third paper (Study III) analyses governmental responses to four key cybersecurity crises that befell Estonia, particularly those that pertain to e-governance. These crises are 1) the 2007 DDoS cyberattacks, which targeted government, news media, and banking sites amidst political violence resulting from the relocation of a controversial Soviet-era monument; 2) the 2017 'eID crisis,' whereby a vulnerability in 800,000 electronic identification cards risked exploitation; 3) the COVID-19 pandemic, which forced practically all in-person interactions online and prompted new cybersecurity risks; and 4) Russia's full-scale invasion of Ukraine in 2022, which saw cyberattacks target Ukraine's allies, including Estonia. Using these crises, this paper looks at how the government can undertake decision-making in times of crisis to bolster future cybersecurity.

Collectively, these studies broach the core research question of this PhD project, as they contribute new scholarship on cybersecurity governance and its evolution over time, especially shaped by institutional learning and adaptation, and decision-making in times of crisis and non-crisis, all within a highly-digitalised context. Together, these studies demonstrate that, in the mature, multi-faceted, and multi-stakeholder context of digitalisation, cybersecurity needs will be higher. The result of this is a need for an appropriate and tailored cybersecurity governance system, which responds to cybersecurity needs themselves, as well as the localised context of governance, security, culture, or other considerations. A highly-digitalised context also presents the need for preparedness within this cybersecurity governance ecosystem in dealing with crises, should they unfold,

with technical, policy, and communications measures in place. Furthermore, these studies collectively provide a mid-level examination of cybersecurity governance that is broadly valuable both theoretically and practically, as outlined below. Theoretically, these studies contribute to domain-specific cybersecurity governance with collaborative governance and historical institutionalism serving as theoretical frameworks. Additionally, these studies, while utilising the Estonian case, provide lessons that are adaptable for settings beyond Estonia, where a set of circumstances surrounding digitalisation may be similar.

This project employs novel theoretical approaches to these studies, using a collaborative governance theoretical approach to examine how policy change unfolded, crafting an ecosystem for cybersecurity governance that has formed and evolved over time, and historical institutionalism to examine responses to cybersecurity crises impacting e-governance. The methodological approach includes document analysis for Study I, and expert interviews of responsible government cybersecurity decision-makers in the Estonian government in Studies II and III. The more specific conceptual, theoretical, and methodological approaches to this research project, and each of these studies are outlined in further detail in subsequent sections.

1.1. Selection and Background of the Estonian Case

Flyvberg notes that case studies are "intensive" and "comprise more detail, richness, completeness, and variance – that is, depth – for the unit of study than does cross-unit analysis."[14] Furthermore, Annamalah emphasises the benefits of case studies as "powerful qualitative methodology, allowing researchers to delve deeply into the intricacies of social phenomena in their natural settings," providing "invaluable tools for examining diverse contexts and generating rich qualitative data."[15] Within the broader case study approach to qualitative research is the critical case, which "usually refers to a single case under investigation that provides so much detail in a context with such great relevance that new theoretical propositions can be created, developed, revised, or debunked."[16] Thus, Estonia has been chosen as the critical case study for the in-depth study of the phenomena of cybersecurity governance and e-governance, for a number of key reasons.

The relevance of the Estonian case in the fields of cybersecurity and digitalisation is based on both the maturity and valuable lessons that can be derived from the country's experience in these two domains. As a pioneer in both spaces, this maturity has been gained through multiple capacities. Firstly, through the early and pervasive adoption of e-governance provisions in Estonia, with its digitalisation experience occurring much earlier than most of its national counterparts globally. Secondly, the 2007 DDoS cyberattacks on the Estonian government,

[14] Flyvberg, 2011, p. 301.

[15] Annamalah, 2024, p. 485–486.

[16] Hysa, 2022, p. 355.

banking, and news media – an event outlined in further detail below – are largely believed to be among the first publicly-acknowledged instances of a cyberattack. Though other cyberattacks certainly predated this instance, the 2007 DDoS attacks occurred earlier than many international counterparts and prompted the Estonian government to craft a new range of governance responses, rather than follow precedent, which did not exist at the time. Given that this research project examines these phenomena over a decade and a half, a time period that is significant in the overall history of cybersecurity governance as a relatively young field, the maturity of the Estonian case is valuable and unique. Examining these phenomena in the Estonian case over a longer period allows for the observation of changes in the cybersecurity governance ecosystem over time. Facilitating the examination of the resilience of these structures to cybersecurity threats and crises, particularly as context and the overall cybersecurity landscape change over time.

Thus, there is immense benefit, both theoretically and practically, to studying the experiences, growth, and processes that Estonia has undergone in these domains. The use of Estonia as a critical case offers "depth and authenticity that enhance the understanding of the phenomena under study," in this case, cybersecurity governance and digitalisation, while providing novel theoretical contributions in the study of cybersecurity vis-à-vis collaborative governance (Study II) and historical institutionalist (Study III) frameworks.[17] Furthermore, there is a limited body of scholarship that has devoted itself specifically to these topics, and thus, this project represents a novel contribution; the more detailed theoretical underpinnings of the project are outlined in the following section. More practically, this project delivers potential lessons in cybersecurity and digitalisation practices that could be adapted to localised settings in other governments across the world. Though Estonia was an early adopter of both e-governance and cybersecurity practices, the ensuing decades have seen other countries 'catch up', especially with digitalisation and, similarly, the cybersecurity mechanisms needed to protect such provisions. As other governments carry out digitalisation initiatives, and consider cybersecurity approaches they can undertake, there is immense value in studying the Estonian case, where government officials have been grappling with these topics for over two decades. Indeed, section 5 of this dissertation outlines some of the specific lessons from the Estonian case, related to crafting a cybersecurity governance ecosystem, as well as policy and communications responses to cyber crises, that could be usefully adapted to other governmental contexts. Arguably, the result is a knowledge creation and sharing that could lead to enhanced cybersecurity of e-governance systems over time.

The origins of Estonian digitalisation date back to the country's restoration of independence in August 1991, after half a century of occupation by the Soviet Union. Upon restored nation-statehood, the new Estonian government sought possibilities for the country's fledgling economy; one such emerging opportunity was in the information technology (IT) sector, which offered an equal playing

[17] Annamalah, 2024, p. 486

field with Estonia's counterparts with larger and more established economies. In this regard, innovation in technology-related fields was actually comparatively easier for Estonia, as the "legacy costs and path dependencies" of older, more analogue Soviet systems, provided a "blank slate" upon which to craft entirely new systems.[18] A pre-cursor to the establishment of e-governance provisions was the Tiger Leap programme, launched in Estonian classrooms in 1997, in order to "prepare the education system and the whole society for the Information Age," providing Estonian students with IT literacy and computer skills.[19] The Tiger Leap programme received a budget of €10 million from the national-level government and €9 million from municipalities to install computers in 560 Estonian schools, provide internet access in 75% of schools, and train over 10,000 teachers in technological education over a four-year period.[20] Coinciding with the Tiger Leap era, access to both computers and the internet "took off"; between 1997 and 1999, Estonian computer ownership rose from 5% to 14%, divergent even from its Baltic neighbours in Latvia and Lithuania, where the same figure remained at 6%.[21]

The 1990s saw a rapid and sophisticated development of technologies in the banking sector, even vis-à-vis many Western countries. Digitalised services, including authentication methods, saw early and widespread adoption by Estonian banking customers, to such an extent that Estonia's two largest banks at the time, Hansapank and Ühispank, offered their banking portal platforms to the Estonian government for use for e-governance purposes.[22] The government data exchange layer, X-Road, was initially launched in 2001, the same year as Estonia's first public Wi-Fi space. The first global instance of internet voting in nation-wide elections was held in Estonian local elections in 2005, and has been utilised in all subsequent local, parliamentary, and European Parliament elections since, reaching its twentieth anniversary in 2025. All the while, the offering of digitalised e-services from the government continued to expand.

At the onset of the time period examined in this project, 2007, Estonia had already begun forming a sophisticated e-governance system. However, the repercussions of the 2007 cyberattacks likely would have been far worse if the level of digitalisation in Estonia had been as it is today, coupled with the safeguards for cybersecurity in place then. While there were some cybersecurity mechanisms in place prior to 2007, cybersecurity governance processes were lacking and the DDoS cyberattacks themselves were precedent-setting, shaping future experiences with cybersecurity governance. Both e-governance and cybersecurity have remained core parts of the Estonian governance agenda, domestically and on the international stage.[23] By late 2024, Estonia saw the expansion of

[18] Kitsing, 2018, p. 63.

[19] Aru-Chabilan, 2020, p. 63

[20] Toots and Laanpere, 2004, p. 8.

[21] Runnel, Pruulmann-Vengerfeldt, and Reinsalu, 2009, p. 31.

[22] Kitsing, 2018, p. 63–64.

[23] ERR News, 2020.

its digitalised services finally reach 100%; although this development has occurred after the time period examined in this project, it is an interesting extension of the topics examined in these studies and a possible pathway for continued research.

Thus, Estonia remains a critical case in both the domains of cybersecurity governance and e-governance. As an early adopter, a pioneer, and a mature case, studying the Estonian case is valuable for observing the phenomena of cybersecurity and e-governance, with the immense benefit of examining how these phenomena have evolved and been shaped over time, as the cybersecurity threat landscape and broader political context have shifted. This allows for practical learnings in addition to the theoretical propositions outlined by Hysa. While the Estonian case is unique for its smallness and agility, lessons can be derived from its experience with cybersecurity governance and digitalisation, with applicability in a variety of settings. Estonia's government has also continued to learn and reshape its cybersecurity approaches over time, as current President Alar Karis noted, when it comes to cybersecurity, Estonia cannot be complacent. He has indicated, "in peace and wartime alike, cybersecurity must be a collaborative effort, from the entirety of society," involving cooperation between the private and public sectors and internationally.[24] As was aptly pointed out to me by a fellow academic in a research seminar where I presented an earlier version of the third paper of this project, in actuality, more governments across the world resemble the Estonian case than they do, for example, the American case, whether they be local governments, federated governments, or the national-level governments of small states. By this logic, large governments like the United States are somewhat anomalous, as there are myriad smaller states or governments more closely resembling the Estonian case that could potentially adapt the learnings of this research project to their own contexts. Furthermore, there is the possibility for lessons from the Estonian case to be scalable to larger contexts. This project does not necessarily advocate for a direct replication of Estonian practices in other settings; this idea has similarly been dispelled by Estonian government officials throughout the years.[25] What this project does aim to do, however, is derive broader lessons from the Estonian case, which could have applicability in other contexts for the purpose of improving cybersecurity governance measures aimed at protecting digitalised provisions. As a result, this project has both theoretical and practical contributions. In the former, it makes novel theoretical contributions, applying collaborative governance theory to examine policy change in the establishment of a cybersecurity governance ecosystem in Study II, and applying historical institutionalism to examine cybersecurity crises in Study III. In the latter, it offers practical insights into how to carry out cybersecurity governance in a highly digitalised context, from a mature and illuminating case study.

---

[24] ERR News, 2023.

[25] For example, former National Cybersecurity Director Liisa Past and former President Kersti Kaljulaid.

1.2. Structure of Introduction Chapter

The structure of this introduction chapter is as follows: beyond this introductory section, section 2 looks at the conceptual approaches and theoretical frameworks underpinning this project, and each of the studies that comprise it. This section firstly articulates the core concepts employed across this project and in each of its respective papers. It then provides the current literature landscape, both for the broader topic of the research and for the specific focuses of the papers, identifying gaps in the current literature and situating this research in the broader body of existing literature. Finally, this section identifies the theoretical frameworks applied in each paper. Section 3 looks at the methodological approaches undertaken in this research project, outlining the approach to each paper and justifying these methodological decisions. It also identifies the potential limitations and how these were mitigated while undertaking this research. Section 4 outlines the overall findings of the research project, as well as the findings of the papers, showing how these findings are interconnected to one another, but also how this all contributes to the gaps in the current body of research. Section 5 is a discussion of the overarching research implications of this project and its studies, while also outlining some prospective avenues for future research, which stem from the findings of this research project. Lastly, the conclusion provides final remarks on this research project.

2. THEORETICAL BACKGROUND

This section looks at the theoretical approach to both the PhD project itself and the papers that comprise it, providing an overview and justification of the conceptual approaches that have been used, alongside the theoretical frameworks that have been applied to this research. Firstly, it outlines the core concepts and definitions used in this project, followed by a review of relevant literature and the situation of this research project and its papers within the landscape of this existing scholarship. Finally, it provides an overview of the theoretical approaches employed in each of the papers comprising this research project. An overview of the conceptual approaches and theoretical frameworks employed within and across Studies I, II, and III can be seen in Table 1 below.

Table 1: Conceptual/Theoretical Outline of Studies

Core concepts across Studies I, II, and III		**Study II**	**Study III**
– Cybersecurity – Cybersecurity Governance – e-Governance/Digital Governance	**Conceptual Approach**	Policy change and policy learning	Crisis management
	Theoretical Framework	Collaborative governance	Historical institutionalism

2.1. Defining Core Concepts

The definitions employed in this project, and similarly, in each of the papers, are as follows. Derived from the work of Craigen, Diakun-Thibault, and Purse, cybersecurity is *the security of technological systems and software, free of manipulation or disruption, and the protection of the information contained in these systems from alteration, corruption, deletion, unauthorised access, or dissemination*.[26] Cybersecurity governance, then, is *the institutional structure and decision-making related to cybersecurity*, as defined above. This definition has been intentionally defined in a broader manner, in order to accommodate the understandings of the topic globally, and to allow for nuance within the topic of cybersecurity governance examined in this project – this is connected with the theoretical underpinnings outlined later in this section. As the work of Urgessa and others has shown, there are myriad different definitions of cybersecurity offered across the governments of the world, organisations such as the UN, and even private sector entities. While this breadth is reflected in some literature and

[26] Craigen, Diakun-Thibault, and Purse, 2014.

governmental or international organisations' definitions,[27] conversely, other scholarship does not define cybersecurity and its governance so broadly. For example, Schiliro has written that "the term 'cybersecurity' is commonly used to refer to a set of circumstances or events related to improving the integrity of a given information management system or infrastructure," a definition which does not specifically refer to the information contained in the systems themselves.[28] Given the significance of information, in addition to the systems themselves, especially when studying e-governance systems, such a broad approach to defining cybersecurity, as well as cybersecurity governance, is crucial for this research project. Furthermore, this broad terminological approach aligns with the theoretical and methodological approaches undertaken in this project; as outlined below, the multitude of actors involved with cybersecurity governance, as the range of interviewees involved from across the Estonian government demonstrates, are well-suited to this broad conceptualisation.

Next, the definition of e-governance, or digital governance (used interchangeably, though not the same as e-government or digital government), employed in this project has been derived from the work of D'Agostino, Schwester, Carrizales, and Melitski, and Bannister and Connoly, as *the digitalisation of provisions offered by the government, assuming an "interactive dynamic" between the government and its citizenry, which fundamentally or substantively differs from the analogue provisions offered prior to this digitalisation process*.[29] While acknowledging that these provisions can, and do, extend beyond the public sector exclusively, the focus of e-governance in the context of this research project is primarily in a governmental setting. Study II employs Weible et al.'s definition of policy change: "*the creation or modification of an existing public policy,*" with a particular emphasis on "*how government can adapt through public policies to signal their responsiveness to societal needs and wants*."[30] An inter-related subset of policy change is policy learning, whereby policies can change by "adjusting understandings and beliefs related to public policy" particularly by learning.[31] Study III employs Coombs' definition of a crisis as a "broad term related to disruptions of some kind," while using Boin et al.'s criteria for a crisis, as an incident with elements of *threat, urgency,* and *uncertainty*, as outlined in greater detail vis-à-vis the Estonian crises examined in Study III.[32] Therefore, crisis management is "a set of factors designed to combat crises and to lessen the actual damage inflicted by" them.[33]

---

[27] See, for example, Ferdousi, 2024, p. 152, who derives a definition of cybersecurity from the National Security Presidential Directive.

[28] Schiliro, 2023, p. 2.

[29] D'Agostino, Schwester, Carrizales, and Melitski, 2011; Bannister and Conolly, 2012.

[30] Weible, 2011, p. 1.

[31] Moyson, Scholton, and Weible, 2017, p. 162; Bennett and Howlett, 1992; Hall, 1993.

[32] Coombs, Holladay, and Tachkova, 2019, p. 31; Boin, 't Hart, Stern, and Sundelius, 2016, p. 3–7.

[33] Coombs, Holladay, and Tachkova, 2019, p. 31; Coombs, 2018, p. 1.

2.2. Review of Literature

By the nature of its topic, this research project is inherently interdisciplinary and is situated at the nexus of cybersecurity, e-governance, broader governance, public policy, and crisis management literature. Thus, there are multiple clusters of scholarship that already exist on topics related to this research project, both broadly and more specifically. In specific strands of literature, there are gaps that this project and its studies aim to contribute to. Most broadly, this research project is situated in the field of cybersecurity research.

In practice, cybersecurity's origins can be traced back to the 1960s, whereby "cybersecurity [was] the pursuit of the technology industry (particularly that of the industrial military complex) for more than half a century," especially through National Security Agency (NSA) initiatives.[34] However, earlier scholarship termed these practical processes 'computer security,' while the term 'cybersecurity' came into use much later, around the start of the 1990s.[35] Fidler notes that "scholarship on the early history of network security and cybersecurity is more recent than that on computer networks."[36] Indeed, a great deal of literature in the cybersecurity domain, dating back to these origins and continuing to the present day, is highly technical; the earliest scientific experiments related to cybersecurity, undertaken in the 1970s, were inherently technical. In 1971, Thomas's "Creeper" experiment presented the message "I'M THE CREEPER : CATCH ME IF YOU CAN" across 28 systems connected to ARPANET, a precursor to the modern internet; subsequently, Tomlinson wrote a similar experimental mobile programme later that same year called "Reaper," which removed copies of the previous "Creeper" from ARPANET.[37] Shortly thereafter, Cohen was believed to have created the first computer virus at the University of Southern California.[38] Together, these early technical experiments in the fledgling field of cybersecurity formed the earliest foundations of cyber threats that have continued to evolve. This PhD project does not claim to be technical in such a manner, instead its focus is on the governance side of cybersecurity, itself a more recent development in this research domain. However, this project is adjacent to such technical research, looking at similar topics in cybersecurity – modern-day cyber threats and cyber crises – from a different, more policy and governance-oriented perspective.

As noted in the "defining core concepts" section above, literature surrounding the concept of cybersecurity governance itself can be quite varied. In scholarship including Urgessa, Pernice, and von Solms and von Solms, the authors have grappled with varied and, at times, competing definitions of the term "cyber-

---

34 Berg, et al., 2016, p. 208.

35 See, for example, Madnick, 1978, p. 61.

36 Fidler, 2017, p. 452; Warner, 2017, p. 782–783

37 Mohanta, 2017, p. 2; Robert and Chen, 2004, p. 3.

38 Robert and Chen, 2004, p. 1-3.

security governance."[39] The work of Urgessa, which compiled definitions from a variety of global institutional settings, especially indicates that in some contexts, definitions of cybersecurity governance can be quite vague.[40] A large body of scholarship has also focused on international-level cybersecurity governance. For example, a great deal of attention is paid in scholarship to ideas around cybersecurity and behaviour in cyberspace amongst the broader West, and Russia and China.[41] A comparatively smaller body of literature looks at how cybersecurity governance can be structured and carried out within a single-country context. For example, Kim outlined a series of core elements (i.e. educating the end-user, monitoring and alerts, and up-to-date technology) for reducing cyber risks in government. Kim's overarching conclusion, in 2017, was that with cyberattacks becoming increasingly sophisticated and lucrative, this rise in threats would therefore lead to increased awareness and funding, particularly from governments, further leading to preventative measures and security.[42] Such a conclusion, that governments must prioritise and provide resources for cybersecurity-related issues, was perhaps novel at the time of Kim's writing, but is now widely accepted in cybersecurity literature and practice. Thus, this dissertation does precisely what Kim suggests, while looking at the ways in which such conclusions are implemented in the case of Estonia. It looks at how the Estonian government undertakes decisions and policies to bolster cybersecurity, knowing that the increased threat landscape has meant that cybersecurity governance has already been identified as a policy area of concern.

Similarly, Tagarev has established a comprehensive list of 33 governance issues related to cybersecurity facing the members of the European Union (EU), particularly as the EU aims to establish cybersecurity competency centres.[43] In this work, Tagarev concludes that these specific needs and governance priorities can be used for arranging cybersecurity collaborative formats, potentially for establishing a European industrial, technology and research cybersecurity competence centre alongside national coordination centres.[44] Tagarev's work examines the establishment of cybersecurity governance structures at a different level of governance, the EU, a supranational level, to that of this project, which has a domestic focus. However, this PhD research could be looked at together with Tagarev's, as making a contribution to the study of establishing cybersecurity governance structures at a different level of governance currently missing from this work. Additionally, Backman has explored the components that lead to the creation of national cybersecurity centres, using the examples of the UK, US, Finland, Germany, and the Netherlands, part of which includes institutional

[39] Urgessa, 2020, p. 4–5; Pernice, 2018, p. 118; von Solms and von Solms, 2018.

[40] Urgessa, 2020.

[41] Giles, 2012; Broeders, Adamson, and Creemers, 2019, and Georgieva, 2020.

[42] Kim, 2017, p. 10.

[43] Tagarev, 2020.

[44] Tagarev, 2020, p. 15.

structures and frameworks.[45] Backman's work found that, despite differences in size and other factors across governments, common features include national cybersecurity strategies, organisation frameworks delineating management tasks, and common tasks and responsibilities across a national cybersecurity centre.[46] These conclusions, written in 2015, are similar to those of Kim, as both came relatively early in the overall development of the field of cybersecurity governance. Thus, such conclusions about the centrality, timeliness, and importance of cybersecurity governance have crystallised over time, becoming widely accepted in both literature and practice. This PhD project particularly looks at the organisational frameworks and common tasks and responsibilities undertaken as part of the Estonian cybersecurity governance ecosystem, more broadly than just as national cybersecurity centres, as Backman has discussed. It is an extension of these conclusions about cybersecurity governance's importance, updated to account for present-day cybersecurity realities.

Additional scholarly work has looked at role distribution during cyber crisis management, specifically looking at the municipal level of governance.[47] Scholarship by Backman has examined how cyber crisis fits within broader transboundary crisis literature, while Fichtner has explored the factors that shape institutional definitions of cybersecurity and responses to cyber crisis.[48] The Estonian cyberattacks of 2007, which represent a significant inciting event in the timeframe examined in this research project and each of its studies, provided a case study in several of these above mentioned articles, in the work of Areng, Boeke, Backman, and Collier. Indeed, Boeke acknowledges that Estonia has been a critical case study in the emerging field of cyber crisis management, as one of the first global instances of a state crafting a response to a cyber crisis.[49] However, the focus of Study III, a paper centred around the Estonian case and looking at the 2007 cyberattacks – alongside other cyber crises – through a crisis management lens, is quite distinct from the approaches of these existing papers. Thus, Study III contributes to the emerging research topic of cybersecurity and crisis management by looking at four instances of cyber crisis in Estonia, and the governance responses that were undertaken in each instance, a longitudinal approach that is lacking from the literature. More broadly, this is a novel contribution to the overarching body of literature on cybersecurity and crisis management, which is underdeveloped and lacks an examination of cyber crises in a particular context or setting, over multiple crises and an extended period of time.

The past two decades have seen the emergence of a body of scholarship devoted to digital transformation, including a focus on these processes undertaken in the public sector. Foundational works on e-governance include Dunleavy,

---

45 Backman, 2015.

46 Backman, 2015, p. 15.

47 Ostby and Katt, 2019.

48 Backman, 2020; Fichtner, 2018, p. 2.

49 Boeke, 2017.

Margetts, Bastow, and Tinkler's "Digital Era Governance" and Homburg's "Understanding e-Government," dating back to the 2000s.[50] The topic has been studied rather extensively in the time since, with scholarship expanding understandings and knowledge in the field of e-governance. More recent works, such as Meijer, Bolivar, and Gil-Garcia, have reflected on trends in the adoption and implementation of e-governance across 15 years of digitalisation in the public sector.[51] Drawing from scholarship on the topic over a decade and a half, they indicate overall patterns in e-governance and its contribution to the trust of citizens, reduction of red tape, and better government performance under strong managerial leadership and openness.[52] Scholarship from Janowski has provided a model in the evolution of digital government over time, a four-phase model comprised of 1) digitisation (technology's entry into government); 2) transformation (technology impacting government organization); 3) engagement (technology impacting government stakeholders); and 4) contextualisation (technology impacting sectors and communities).[53] Conversely, Mergel, Edelmann, and Haug have sought to define the process of digital transformation, including the 'why' and 'how' of this process, derived from interviews with responsible government personnel.[54] Amongst their findings include a breakdown of ideas gained from these government personnel about why digital transformation is being undertaken, in what parts of government, via what types of public service delivery, and to what extent. These works discuss the process of digital developments and the realities of reaching a highly-digitalised state, but what is largely missing in this literature is substantive discussion of the cybersecurity needs of an e-governance system. While implicitly, they demonstrate that increased digitalisation can necessitate cybersecurity parameters via the increased vulnerabilities and surface area for attack vectors, such discussion is lacking from much of the current body of literature. Thus, this PhD project contributes at the nexus of these discussions surrounding how to govern cybersecurity in a highly-digitalised context.

Additionally, works such as Tassabehji, Hackney, and Popovic, have furthered the e-governance research that came before, by applying Dunleavy's digital era governance concept in action in American municipalities; their main conclusion is that, based on the case organisations that they studied, digital era government is diffusing into public institutional language, and that e-government has resulted from a push for "efficiency, effectiveness, cost savings and citizen centricity."[55] Among these works, and others, such as D'Agostino, Schwester, Carrizales, and Melitski, and Bannister and Connolly mentioned earlier in this section, there have

---

50 Dunleavy, Margetts, Bastow, and Tinkler, 2008.

51 Meijer, Bolivar, and Gil-Garcia, 2018, p. 1–6.

52 Meijer, Bolivar, and Gil-Garcia, 2018, p. 5.

53 Janowski, 2015, p. 221.

54 Mergel, Edelmann, and Haug, 2019.

55 Tassabehji, Hackney, and Popovic, 2016, p. 236.

been multiple attempts in the literature to grapple with the terminology of, and related to, e-governance, given that there can be ambiguity in how the term is understood across entities; however, the definitions outlined above have been derived directly from their works. Scholarship outlined above, such as Dunleavy, Margetts, Bastow, and Tinkler, Homburg, Janowski, and Mergel, Edelmann, and Haug, are foundational texts in the field of e-governance and, as such, provide a broader overview of the field as a whole. While this research project belongs to the same overarching research topic of e-governance and digitalisation literature, it is a much more narrowed and specific examination of location and context within this field. Specifically, Study I is an exploratory case study looking at how several of these core concepts surrounding e-governance have been implemented in the Estonian case, while building upon the definition of e-governance derived from D'Agostino, Schwester, Carrizales, and Melitski, and Bannister and Connolly to frame Studies I through III.

As an early and pervasive instance of e-governance adoption and implementation, the Estonian case study features heavily in e-governance literature, but in rather specific contexts. In the earliest such instances, scholars such as Ernsdorff and Berbec, and Kitsing looked at the initial development and successes of Estonian digitalisation in the mid- to late-2000s, providing an overview of the e-governance structure. Ernsdorff and Berbec particularly focused on the now-defunct participatory platform TOM and internet voting, concluding that "early investment in ICT, accompanied by the necessary reforms has made of Estonia one of the most development states in e-government in Europe, even in the world." [56] Interestingly, Kitsing highlighted other elements of the Estonian e-governance system, including public-private partnerships for the provision of e-governance, and the decentralised nature of the data exchange platform X-Road, which forms the backbone of Estonian e-governance. Ultimately, Kitsing concludes that, while there are both synergies and mismatches in the Estonian system – especially surrounding the future directions for the system itself – there is no doubt that the "Estonian government has made tremendous progress in implementing digital government," thus echoing the findings of Ernsdorff and Berbec.[57] In a similar manner to these works, Study I aims to provide a comprehensive overview of Estonian e-governance, albeit one that is updated to account for new developments in the time leading up to the COVID-19 pandemic, which have been numerous in the time elapsed since Kitsing and, especially, Ernsdorff and Berbec produced these works.

Literature pertaining to a variety of more specific aspects of the Estonian e-governance system has been ample in the past decade. Examples include Kerikmäe, Troitino, and Shumilo, and Kattel and Mergel, writing on the development and perceptions surrounding Estonian e-governance, Solvak, et al. on the adoption of e-services, Solvak and Vassil, and Vinkel and Krimmer on the Estonian adoption

[56] Ernsdorff and Berbec, 2007, p. 180.

[57] Kitsing, 2018, p. 2–3, 7, 9.

and future prospects for internet voting, and Kotka, Vargas, and Korjus, and Tammpuu and Masso on the e-Residency programme.[58] Kerikmäe, Troitino, and Shumilo debate whether Estonian e-governance represents an idol or an ideal, ultimately concluding that, while effective branding strategies play an important role in how Estonia markets itself, both local and international perceptions are mainly of Estonian e-governance as an ideal, by which other governments could use "Estonia as a pathfinder to learn from."[59] Kattel and Mergel similarly conclude that Estonian digital transformation is a success, based on the threefold approach of its context (i.e. location, size, proximity to Scandinavia), governance principles, and design approaches to the technology itself.[60] Solvak, et al., used approximately 2.1 billion rows of anonymised log data to study the diffusion of e-services in Estonia, finding that 1) the diffusion of e-governance is linear rather than sigmoid-shaped; 2) age is positively related to the diffusion of e-governance technologies; and 3) women are typically faster adopters of e-governance technologies than men.[61] While approached in an entirely different methodological manner from this PhD project, this work particularly shares a nexus with Study I in creating an overview of the Estonian e-governance system; however, Solvak, et al. aim to do so in order to examine broader diffusion trends using vast quantities of data, while Study I does so to identify the cybersecurity governance needs of Estonian e-governance, setting the foundations for subsequent analyses in Studies II and III.

Upon outlining internet voting trends in Estonia and contrasting this case with Switzerland and Norway, Vinkel and Krimmer conclude that i-voting has been implemented in Estonia "as a solid voting method," and one which bolsters the "e-Stonia" narrative surrounding digital capabilities.[62] Furthermore, they indicate that the buildup of internet voting takes time, and that there is no single characteristic that punctuates a working system in Estonia, Switzerland, or Norway. Solvak and Vassil looked at Estonian i-voting in an attempt to distinguish what aspects are persistent and what are habitual using surveys conducted following elections, ultimately concluding that 1) past i-voting is strongly associated with current i-voting; 2) associations between resources and current i-voting are weak; and 3) support attitudes are not associated with higher likelihood of repetitive i-voting.[63]

In their work examining the Estonian e-Residency programme, Kotka, Vargas, and Korjus employ Actor Network Theory (ANT), a framework which examines "the vital role of non-human entities, and human agents' interactions with them,"

---

[58] Kerikmäe, Troitino, and Shumilo, 2019; Kattel and Mergel, 2019; Solvak, et al., 2019; Solvak and Vassil, 2017; Vinkel and Krimmer, 2016; Kotka, Vargas, and Korjus, 2015; Tammpuu and Masso, 2018.

[59] Kerikmäe, Troitino, and Shumilo, 2019, p. 77–78.

[60] Kattel and Mergel, 2019, p. 154–157.

[61] Solvak, et al., 2019, p. 52.

[62] Vinkel and Krimmer, 2016, p. 249.

[63] Solvak and Vassil, 2017, p. 13–14.

in the context of the e-Residency programme's technical elements, and components of Estonian e-governance such as X-Road and eID.[64] They ultimately use this theoretical approach to frame the origins of e-Residency, as well as to map out its actors, and the benefits and risks of this programme, concluding that the notion of e-Residency has the potential to, at most, lead to a redefinition of the nation-state, while also prompting new fields of enquiry in governance and public administration studies.[65] While Tammpuu and Masso do not go quite so far in their assessment of the impacts of the e-Residency programme, they do conclude that the programme both contextualises and alters existing e-Estonia narratives around e-governance, as it promotes Estonia's image as a transnational society and a virtual state, incorporating this into the country's branding.[66] While the ANT theoretical approach represents a compelling way to map a core component of the Estonian e-governance system in the work of Kotka, Vargas, and Korjus, it is a departure from the approach employed in this paper; this is particularly due to its heavy focus on non-human entities. Although this PhD project similarly broaches topics related to technology comprising the Estonian e-governance system, its approach is not concerned with the relationship between non-human and human entities, but rather, the human processes involving governance and decision-making. Furthermore, the focus of this research project is not on the branding of Estonia and its digitalisation process; while this represents an interesting segment of research in the Estonian e-governance space, this project is primarily focused on the cybersecurity governance processes that are necessitated by and unfold from this highly-digitalised environment. This body of literature focuses on various aspects of Estonian e-governance, whether they be e-services, i-voting, or the e-Residency programme, demonstrating the multi-faceted nature of the digitalised offerings within Estonia. However, much like the broad body of e-governance literature described above, this literature lacks discussion of the cybersecurity needs of these various components of the Estonian e-governance system. Thus, this PhD project makes a number of key contributions to these gaps: firstly, in Study I it provides an up-to-date overview of the Estonian e-governance landscape beyond what is outlined in these previous studies. Secondly, it looks at the process of governing cybersecurity around this wide range of digitalised provisions, given that all of these provisions are effectively vulnerable to the same sophisticated and ever-evolving cyber threat landscape and need to be secured accordingly.

Although this PhD project is situated in a similarly narrow study of e-governance in the Estonian context as the above outlined studies, it varies and makes new contributions in novel ways: firstly, Study I is situated adjacent to these studies, by providing an overview of the e-governance system in Estonia that is somewhat broader than these studies, which looks at very specific aspects

[64] Kotka, Vargas, and Korjus, 2015, p. 2.

[65] Kotka, Vargas, and Korjus, 2015, p. 17.

[66] Tammpuu and Masso, 2018, p. 14–15.

of Estonian e-governance. However, it also takes a further step by outlining the ways in which e-governance provisions need to be secured, setting up the subsequent research of Studies II and III, and representing a departure from this aforementioned scholarship. Furthermore, this PhD project represents an updated examination of Estonian e-governance, as some of these papers were written as long as a decade, or even a decade and a half, ago; this is a fast-moving domain, and in this period of time, many new developments have occurred in Estonian e-governance.

Separate from e-governance literature, Estonian cybersecurity has also been studied as a case study: firstly, as an example of a small state that is a global norm-setter in the domain of cybersecurity, and secondly, with specific attention paid to the 2007 cyberattacks and the political decision-making and legal reforms that followed.[67] Crandall and Allan's main conclusions surround Estonia as a norm entrepreneur in the domain of cybersecurity norms, especially using its membership in NATO to derive an organisational platform for its cyber agenda.[68] Czosseck, Ottis, and Talihärm describe the national cybersecurity strategy, government structures, legal amendments, a new Emergency Act, and the development of organisations devoted to cybersecurity among the main outcomes of the 2007 cyberattacks.[69] They subsequently conclude that "the cyber attacks against Estonia were not as severe as often referred to, [but] prompted a wake-up call concerning the risks associated with the 'careless use' of digital information technologies."[70] Herzog similarly provides an overview of the 2007 cyberattacks and reflects on some of the outcomes of the attacks, but particularly focuses on new NATO and EU directions for cybersecurity in a departure from Czosseck, Ottis, and Talihärm.[71] Broadly, Herzog concludes that the 2007 cyberattacks and a new digital era have prompted foreign and security policies of nation-states to adapt to these new realities accordingly.[72] This project, and especially Study III, shares parallels with these works in their examination of governance outcomes from the 2007 cyberattacks, both domestic and international ones in the context of Study III. However, Study III examines further crises beyond the 2007 cyberattacks, to gain insight into the landscape of cybersecurity crisis decision-making over a longer period of time. Herzog also uses the terminology 'cyber terrorism' and 'cyber warfare' to describe the events of the 2007 cyberattacks in Estonia, terminology which I reject for the entirety of this project, across Studies I, II, and III, as it simply does not encapsulate the events that unfolded. Rather, 'cyberattacks,' in a similar fashion to the work of Czosseck, Ottis, and Talihärm, or 'cyber incursions' more accurately describe the events examined in this project.

---

67 Crandall and Allan, 2015; Czosseck, Ottis, and Talihärm, 2018; Herzog, 2017.

68 Crandall and Allan, 2015, p. 362.

69 Czosseck, Ottis, and Talihärm, 2018, p. 58–62.

70 Czosseck, Ottis, and Talihärm, 2018, p. 63.

71 Herzog, 2017, p. 54.

72 Herzog, 2017, p. 56.

Only a limited body of scholarship has considered e-governance and cybersecurity together and in-depth in the Estonian case. Paršovs and Skierka have both studied cybersecurity concerns in the context of the 2017 eID crisis.[73] In one work, Paršovs looked at the security flaws in the key management of the Estonian eID card, concluding that improved security engineering practices could have been employed to avoid a breach of security requirements from the card's manufacturer, and that without fundamental changes to this manufacturing process, cybersecurity incidents could happen again.[74] In a second work, Paršovs similarly outlined issues with the ID card and noted that legal non-compliance in the eID crisis was the result of 1) a lack of technical preparedness; 2) 'sub-optimal' decisions undertaken under time pressure; and 3) the 'critical nature' of the eID crisis.[75] Paršovs also subsequently makes a set of technical recommendations based on the paper's findings.[76] Skierka's work also examined the eID crisis, from a governance perspective rather than the technical approach undertaken by Paršovs, concluding that Estonia's e-governance maturity meant that a shutdown of services or electronic authentication was not an option amidst this crisis, rather necessitating "public-private network structures and their common norms and goals" for the purpose of crisis management.[77] Study III similarly looks at responses to the eID crisis, from a governance standpoint most aligned with the work of Skierka, however it does so alongside other crises affecting Estonian e-governance over the focus period of this PhD project. While this research project utilises the same case study of Estonia and features an overlap with the study of the eID crisis, this project provides novel contributions via its study of the Estonian cybersecurity governance ecosystem in Study II, a topic not broached in detail in prior literature. Particularly, Study III builds upon this work by Paršovs and Skierka, looking at Estonian cybersecurity crises longitudinally over a period of approximately 15 years; while this includes the 2017 eID crisis, which was a central focus in both of their works, this study also examines governance responses to the 2007 cyberattacks, the COVID-19 pandemic, and the 2022 full-scale invasion of Ukraine by Russia. In doing so, Study III tracks governance responses in crises in the cybersecurity domain over time.

In the literature described above, there is a distinct lack of comparative research in the precise topics examined in this paper. Firstly, there are difficulties in comparing Estonia to other mature cases in the domains of cybersecurity governance and digitalisation, because in these domains, many countries have innovated comparatively much more recently. For example, there is novel recent research on cyberattacks that impacted digitalisation provisions, or the public

[73] Paršovs 2020a; Paršovs, 2020b; Skierka, 2023.

[74] Paršovs, 2020a, p. 1799.

[75] Paršovs, 2020b, p. 468.

[76] Paršovs, 2020b, p. 469.

[77] Skierka, 2023, p. 9.

sector more broadly, in Albania[78] and Costa Rica,[79] but these cases lack the maturity of the Estonian case and could not be directly compared from a governance or crisis response perspective; these crises have been experienced more than a decade and a half after Estonia began grappling with such circumstances and these cases are simply too young for a direct comparison. Conversely, there are instances of comparative research on Estonia and other mature cases in adjacent domains within cybersecurity governance research, or even military domains such as cyber commands. For example, Boeke has looked comparatively at Estonia, Denmark, the Netherlands, and Czechia, specifically examining how states often struggle to adapt existing institutional infrastructures to address cybersecurity crises,[80] while Collier has examined governmental institutional structures in place for broaching crises, alongside NGO involvement and international initiatives in the crisis response process, comparatively studying Estonia and the United Kingdom.[81] In Collier's work, one particularly interesting finding is that Estonia and the United Kingdom share "a clear focus on civilian-led organisations that manage and coordinate cyber crisis situations," as well as the strong presence of the private sector in governmental cybersecurity processes.[82] This represents a particularly interesting synthesis with both Studies II and III, which also identify the primary civilian, rather than military, ministerial purview for cybersecurity governance in Estonia, as well as the relationship between public and private sectors, not only in a crisis environment, as in Collier's work, but in the broader cybersecurity governance ecosystem. Boeke similarly points out that a key way in which Estonia varies from Denmark, for example, is the civilian leadership for cybersecurity.[83] Ultimately, Boeke's work concludes that governments face two main choices when organising cyber defence and crisis management structures, which these comparative cases have broached in different ways: 1) whether the Computer Emergency Response Team (CERT) is located inside or outside the intelligence community, and 2) whether to centralise or distribute cyber capacity.[84] However, while in many ways directly adjacent to this PhD project, this existing scholarship is lacking a focus on the specific topics of crafting a cybersecurity governance ecosystem, or forming governance responses to cybersecurity crises affecting e-governance, both broached in this project. Thus, it is compelling to use Estonia as a single critical case to conduct this research, while comparative research could be a pathway for future research, outlined in greater detail in the conclusion section of this dissertation.

---

78 Pavel, 2024.

79 Datta and Acton, 2024.

80 Boeke, 2017.

81 Collier, 2016.

82 Boeke, 2017, p. 19-20, p. 31.

83 Boeke, 2017, p. 7.

84 Boeke, 2017, p. 13.

Thus, this research project similarly aims to contribute at this nexus of cybersecurity and e-governance, but each of the studies comprising this overarching research project make a more specific contribution to a particular gap in the existing scholarship. The first such gap, to which Study I makes a contribution, is an up-to-date macro-level overview of the Estonian e-governance system around the time of the COVID-19 pandemic. It provides an exploratory case study and, as such, a detailed exploration of the Estonian e-governance case, while also identifying the key cybersecurity needs of the Estonian e-governance system, providing a foundation for the theoretical and analytical contributions of Studies II and III. As outlined in the literature review above, a large body of scholarship is devoted to very specific aspects of the Estonian e-governance system, such as e-services, internet voting, or e-residency. Conversely, Study I provides a much broader overview of the Estonian e-governance system, collating publicly available information on the entire system from the various, distinct entities that comprise it. Doing so provides the case selection logic that underpins the remainder of this PhD project, and indeed the justification for cybersecurity needs of the Estonian e-governance system, taking a more analytical look at these functions and the governance processes underpinning them in-depth in the subsequent studies.

The second gap in the existing body of literature, to which Study II contributes, is in studying policy change in the context of cybersecurity. Weible, et al., define policy change as "the creation or modification of an existing public policy," with a particular emphasis on "how government can adapt through public policies to signal their responsiveness to societal needs and wants."[85] Policy change has long been a field of study within the broader setting of public administration and public policy research scholarship, broaching a broad range of policy domains, dating back for more than five decades.[86] Throughout previous decades, policy change literature has included focuses on fields such as social and civil rights policy,[87] environmental policy,[88] and stressors in policy-making,[89] among others. Indeed, some scholarship has deemed policy change a "mature field" of research.[90] Within this field of policy change is the more specific study of policy learning, most broadly defined as "adjusting understandings and beliefs related to public policy."[91] The research of Bennett and Howlett asserts that "policies change in a variety of different ways," including by learning, while Hall sees learning as a normal part of the policy-making process.[92] Some of the earliest

85 Weible, Heikkila, deLeon, and Sabatier, 2011, p. 1.

86 See, for example, Truman, 1964.

87 Tishler, 1971; Bullock and Lamb, 1984.

88 Crenson, 1971; Jones, 1976.

89 Wilson, 2000.

90 Bardach, 2009.

91 Moyson, Scholten, and Weible, 2017, p. 162.

92 Bennett and Howlett, 1992; Hall, 1993.

policy learning scholarship dates back to around the same time as the earliest aforementioned policy change literature; for example, Deutsch in 1965 noted that governments use constant "feedback" and "steering" to enhance government's "learning capacity."[93] May has indicated two instruments of policy learning: firstly, via social policy learning around the "social construction of policy problems, the scope of policy, or policy goals," and political learning, the "lessons about policy processes and prospects."[94] Furthermore, May argues that these instruments are not mutually exclusive and can often both be present in the process of policy change; indeed, both are present in the study of policy change and policy learning in Study II. Therefore, Study II looks at both the broader policy change and the more specific policy learning as a subset of policy change research.

However, while the study of policy change and policy learning has existed for more than half a century, with varying focus on timely policy domains, there is still limited research specifically examining these topics within the scope of cybersecurity. In more recent years, even as cybersecurity has emerged as a timely topic for research, policy change and policy learning literature has featured a predominant focus on topics related to the COVID-19 pandemic itself,[95] or policy change in other fields, such as renewable energy or public transport, in relation to the COVID-19 pandemic.[96] Conversely, earlier in this literature review section, there has been an in-depth examination of research on e-governance and cybersecurity governance, but among this scholarship, there is a distinct lack of explicit mention of policy change or its use as a core conceptual framework. Thus, there is a prominent gap in the literature, where cybersecurity as a domain is largely missing from the ongoing scholarship on policy change. As a timely and pressing policy concern, and a field in which policy has been forced to form and adapt to ever-evolving cybersecurity realities, there is a compelling argument to be made for cybersecurity to be studied in the context of policy change. Therefore, Study II aims to contribute to this particular gap, by looking at cybersecurity governance, using the Estonian case and examining such topics from a more mid-level perspective, to look at how the topic has become a policy priority and how a governance ecosystem formed and changed over time in response to the issue at hand. In the literature review above, cybersecurity and e-governance scholarship have typically examined their respective topics at the mid-level; thus, this research remains consistent in the level of examination, while using novel theoretical frameworks in this domain. Beyond this specific focus on policy change in the formation of the Estonian cybersecurity governance ecosystem in Study II, there is a compelling prospect for the future study of policy change in various other aspects of the domain of cybersecurity governance. As cybersecurity

93 Deutsch, 1965.

94 May, 1992, p. 332.

95 Zaki and Wayenberg, 2023; Crowe, et al., 2023; Zaki, Pattyn, and Wayenberg, 2023.

96 Hoang, et al., 2021; Marsden and Docherty, 2021.

realities continue to shift and evolve, and the associated policies and governance processes similarly continue to form, the potential for gaining new theoretical and practical insights are numerous.

The third gap in this field of research is crisis management in the domain of cybersecurity; as this section outlines, a limited body of literature has studied crises in the context of cybersecurity, but crises do occur in this domain and it is a worthwhile and timely topic to be studied, especially in relation to e-governance. Much like policy change, crisis management is also a field dating back several decades of study, examining a broad range of crisis types, but only recently featuring a focus on cybersecurity. Scholarship on the topic from Coombs has loosely called crisis a "broad term related to disruptions of some kind," while crisis management is "a set of factors designed to combat crises and to lessen the actual damage inflicted by" them.[97] In decades of work on political crisis management, Boin, et al. have acknowledged and written about the broad range of domains in which crises have been experienced, ranging from natural disasters, to humanitarian emergencies, to terrorist attacks.[98] In the 2017 edition of their work, Boin, et al. note that cybersecurity represents a new domain area for study within the broader scholarship of crisis management.[99] The criteria for determining what constitutes a crisis, employed in Study III, has been drawn from this same foundational work, while further exploring the crisis management models of Pearson and Clair, Jin, et al., and Jaques, which focus on environmental context, readiness, and post-crisis management, respectively.[100] Thus, this crisis management literature has framed the approach to crisis, and indeed the real-world examples of crisis, examined in Study III at a mid-level perspective, similar to the approach to policy change in Study II. Overall, this research project aims to contribute new knowledge to the broader and emerging field of cybersecurity and e-governance, drawing specifically from the Estonian case to do so. The studies that comprise this research contribute to varied and more specific gaps in the existing literature, as outlined above. Thus, the project makes theoretical contributions to the broader domains of cybersecurity and e-governance, and more specifically in the fields of policy change and crisis management. Additionally, this research project makes practical contributions, learning from these studies in particular theoretical domains, and engaging in knowledge production that can help governments grappling with these issues in real time.

---

97 Coombs, Holladay, and Tachkova, 2019, p. 31; Coombs, 2018, p. 1.

98 Boin, 't Hart, Stern, and Sundelius, 2017, p. 1.

99 Boin, 't Hart, Stern, and Sundelius, 2017, p. 3.

100 Boin, 't Hart, Stern, and Sundelius, 2017, p. 5–7; Pearson and Clair, 1998, p. 66; Jin, Coombs, Wang, van der Meer, and Shivers, 2023, p. 4–5; Jaques, 2007, p. 150–151.

2.3. Theoretical Approaches of Studies I, II, and III & Justification

This sub-section provides an overview of the theoretical frameworks employed in the studies that comprise this project. As was shown in Table 1, several core concepts appear across all three studies, while each study has its own distinctive conceptual approach and theoretical framework that was deemed most appropriate for the research question chosen in each respective paper. As indicated in Table 1, the core concepts of cybersecurity, cybersecurity governance, and e-governance or digital governance are present across Studies I, II, and III. However, Study I is largely atheoretical, serving the specific role of an exploratory case study and providing foundations for theoretical inquiry in subsequent studies. Consequently, Study II examines the concept of policy change using a collaborative governance theoretical framework, while Study III looks at the concept of cyber crisis management through the theoretical lens of historical institutionalism. The specific approaches to the theoretical frameworks used in these studies is outlined in greater detail below.

Study I has a unique role in this overarching project, providing an exploratory case study into the topic of digitalisation in Estonia in the time period surrounding the COVID-19 pandemic, while also providing context into how cybersecurity can be governed in a governmental setting and framing some of the potential cybersecurity concerns that can arise in this domain. As such, it sets the groundwork for the subsequent papers comprising this project, both topically and in the theoretical and analytical contributions of these papers. As such, Study I deliberately does not incorporate theory, as its specific aim was to be descriptive, to explore the case in great depth, rather than to build theory. By studying the Estonian case in such depth, while remaining separate from theory, Study I provided the foundation for Studies II and III, which each have a specific and fitting theoretical approach described in greater detail below.

Study II examines the cybersecurity governance ecosystem in Estonia, using collaborative governance theory to examine the concept of policy change in the domain of cybersecurity governance. This study's collaborative governance theoretical approach emphasises the broad array of different actors involved in the governance process. The definition of collaborative governance used in this study has been drawn from the foundational work of Emerson, Nabatchi, and Balogh, who have contributed multiple pieces of scholarship on this theoretical approach. They define collaborative governance as "the processes and structures of public policy decision making and management that engage people constructively across the boundaries of public agencies, levels of government, and/or the public, private and civic spheres in order to carry out a public purpose that could not otherwise be accomplished."[101] In further scholarship, Emerson and Ahn have described the "many moving parts in a dynamic relationship over time, con-

[101] Emerson, Nabatchi, and Balogh, 2012, p. 2.

necting different institutional structures, multiple leaders, diverse stakeholders, and complicated substantive policy changes,"[102] while Newman, et al. indicate that the actors involved in governance process are one or more agencies, with stakeholders beyond the government.[103] In further scholarship, Ansell and Gash indicate that in practice collaborative governance can take on multiple forms, including the governance processes around "laws and rules that pertain to the provision of public goods," as well as "collective decision making that includes both public and private actors."[104] The main approach derived from collaborative governance literature for Study II is Emerson and Ahn's three core collaborative dynamics, which should be present in instances of collaborative governance, and these dynamics are: 1) principled engagement (including mutual understanding and shared commitment), 2) shared motivation (including shared definitions and interactive deliberation or decision-making), and 3) joint capacity (through what they call "combination of procedural/institutional arrangements, leadership, knowledge, and resources"); all of these dynamics are not static and may change or shift over time.[105]

Collaborative governance theory is particularly pertinent and valuable for observing cybersecurity governance and policy change, in the scope of Study II. Firstly, the definitions and criteria of collaborative governance and collaborative dynamics outlined above are particularly applicable in the domain of cybersecurity governance. For example, these works describe "multiple moving parts in a dynamic relationship" for the purpose of "substantive policy change," which encapsulate the multi-faceted process of governing cybersecurity and setting up an institutional ecosystem to serve this aim[106]. In this regard, Study II revisits the varying components of collaborative governance from Ansell and Gash's work in practice; the moving parts of the dynamic relationship and substantive policy change appear in the context of various policies and legislation, involving different parts of government and the private sector, as this work describes.[107] Secondly, existing scholarship has seen Emerson and Ahn's collaborative dynamics applied in diverse fields and case studies; this includes environmental restoration in the Florida Everglades, innovation platforms in Malawi, and healthcare networks in Morocco.[108] Given that these fields are, by their nature, multi-faceted and multi-stakeholder policy domains, attributes which cybersecurity governance shares, they make a compelling case for the applicability of collaborative governance theory, and more specifically, these collaborative dynamics. Notably, these

[102] Emerson and Ahn, 2015, p. 63.

[103] Newman, Barnes, Sullivan, and Knops, 2004, p. 204.

[104] Ansell and Gash, 2008, p. 545.

[105] Emerson and Ahn, 2015, p. 64.

[106] Emerson and Ahn, 2015, p. 63.

[107] Ansell and Gash, 2008, p. 545.

[108] Heikkila and Gerlak, 2015, p. 73–79; Mikwamba, et al., 2021, p. 259-261; Belrhiti, et al., 2024, p. 412-414.

collaborative dynamics offer a set of criteria alongside which Estonian cybersecurity governance and policy change processes can be compared and assessed, making a novel theoretical contribution to certain gaps in the policy change literature outlined earlier in this section.

Study III uses a historical institutionalist theoretical framework to look at cybersecurity crises affecting e-governance in Estonia over a period of time similar to that of this research project, 2007–2023. Particularly, this historical institutionalist approach frames cybersecurity crises and e-governance in the Estonian case through institutional path dependencies, treating the cybersecurity crises as critical junctures, which Mahoney, Mohamedali, and Nguyen define as "a relatively short period in time during which an event or set of events occurs that has a large and enduring subsequent impact."[109] As Fioretos, Falleti, and Sheingate (2016) indicate, critical junctures mark the start of path-dependent processes, whereby future outcomes, decisions, or processes are a result of those that came before them.[110] Therefore, the governance processes that follow the cybersecurity crises examined in this paper form critical junctures to study, deriving findings from the experiences and ideas presented by the decision-makers who were directly involved at the time of these junctures. Specifically, the historical institutionalist approach undertaken in this paper is derived from the work of Pierson and Skocpol, whereby research uses critical junctures and long-term processes to understand "overarching contexts and interacting processes that shape and reshape states, politics, and public policmaking [sic]."[111] This approach recognises that the 16-year period encompassed by this research project is relatively short in the grander picture of critical junctures; other research into historical institutionalism may use critical junctures over far greater periods of time. However, considering how recently the fields of cybersecurity and e-governance have developed, such an approach is justified by the fact that these junctures have occurred over a majority of the history of these topics. This study looks less at the crises themselves, but rather the governance and political decision-making undertaken in the aftermath of these cybersecurity crises, aimed at bolstering cybersecurity in the future. Critical junctures and crises are intrinsically interconnected in the context of this study, contributing to the gap in the literature on cybersecurity and crisis management identified earlier in this section.

[109] Mahoney, Mohamedali, and Nguyen, 2016, p. 77.

[110] Fioeretos, Falleti, and Sheingate, 2016, p. 9

[111] Pierson and Skocpol, 2002, p. 2.

3. RESEARCH DESIGN & METHODOLOGICAL APPROACH

This section provides insights into the research design and methodological approaches used in this research project, justification for the selection of these approaches, and potential limitations and how these were mitigated. This project has applied multiple qualitative methods and research designs to gain nuanced insight into the governance and decision-making processes surrounding cybersecurity and e-governance in Estonia. The first paper employed an exploratory case study methodology and document analysis to examine the core ways in which the Estonian e-governance model has evolved, using the COVID-19 pandemic as a time marker, before, during, and after which the digitalisation structure and e-governance process can be observed. The second and third papers have used expert interviewing as their core methodological approach, to look at how the cybersecurity governance model of Estonia has shifted over time and in response to cybersecurity crises affecting e-governance, respectively.

This qualitative approach was deliberately selected for its alignment with the topics studied in this research project. By definition, qualitative research is a "situated activity that locates the observer in the world,"[112] and employs a "naturalistic, interpretive approach, concerned with exploring phenomena 'from the interior.'" [113] From Mitchell, cited in Lichtman: "the issue of qualitative versus quantitative methods is rooted first and foremost in the character of the phenomena investigated,"[114] while multiple prominent works go on to indicate the core criteria that align with qualitative research: concerned with 'what,' 'why,' and 'how' questions, rather than 'how many'; a focus on processes; uses in-depth study; small group size, which is non-random, in their natural setting; and uses purposeful and snowball sampling.[115] Given that this project seeks to look at the 'how' pertaining to cybersecurity governance and e-governance processes and decision-making in Estonia, this methodological approach was particularly logical. Thus, the overarching topic and research questions addressed in this project most naturally and inherently aligned with qualitative research methods.

3.1. Methodological Approach to Studies I, II, and III & Justification

Study I was an exploratory case study, providing an examination of Estonian e-governance as a critical case aimed at gaining in-depth knowledge about this topic in this one specific setting. Stewart indicates that exploratory research should be conducted "when a topic is not well understood… [aiming] to explore the area,

[112] Denzin and Lincoln, 1994, p. 10.

[113] Ormston, Spencer, Barnard, and Snape, 2013, p. 3.

[114] Lichtman, 2013, p. 13.

[115] Lichtman, p. 13, 16; Denzin and Lincoln, 1994, p. 10.

gather preliminary data, and identify patterns or ideas that can lead to the formulation of hypotheses."[116] Yin further indicates that the goal of an exploratory study is "to develop pertinent hypotheses and propositions for further inquiry," which is precisely the role Study I serves in this broader PhD project, providing foundations in the Estonian e-governance system to analytically examine the cybersecurity governance considerations surrounding it in subsequent studies.[117] In Study I, I have conducted desk research to compile publicly-available information on the topic of Estonian e-governance, employing document analysis to analyse this information. The information was derived from a literature review of academic and expert commentary, governmental websites and messaging, and news media, typically situated within the Estonian context, but also drawing from some international sources of commentary. Firstly, the academic literature was drawn from a body of scholarship examining the topic of e-governance, digital governance, or digitalisation in Estonia, while more specific sub-sections of this literature focused on e-services, internet voting, and data exchange (or X-Road, specifically) as core elements of Estonian e-governance. Given the paper's focus on the time period surrounding the COVID-19 pandemic, Study I also drew from the limited but emerging body of literature related to COVID-19 responses in Estonia. Governmental documents came from the responsible entities across the Estonian government, including the State Information System Authority, the eesti.ee State Portal, e-Estonia Briefing Centre, Accelerate Estonia, and accessed legislation from Riigi Teataja. Additional information on X-Road, which now exists separately from solely Estonian government entities, was accessed from the X-Road website. For domain-specific information, documentation was accessed from the Ministry of Education (including their database for e-learning resources during the COVID-19 pandemic), Health Board, and the Crisis and Emergency Information Portal (kriis.ee). News media was accessed from Estonian Public Broadcasting (ERR), Postimees, and Delfi, seeking topics related to COVID-19 and digitalisation – in the leadup to and during the implementation of pandemic-related lockdowns and other measures – while some additional notable international media reporting on Estonian e-governance was taken from the New Yorker and the Atlantic. A large amount of information and sources were collated to inform this study, comprising necessary groundwork and forming foundations to build upon theoretically in the subsequent studies. This also demonstrates a systematised and replicable approach to the collation of information across multiple sources to inform the exploratory case study.

The specific analytical approach utilised in this paper was derived from the Sage Handbook of Public Policy, and particularly highlighted the e-governance process in Estonia surrounding the COVID-19 pandemic by asking: what problem exists? Who does it impact? What available policy options exist to address the problem? Which policy option is the most desirable? What other variables

[116] Stewart, 2025.

[117] Yin, 2018, p. 10.

should be considered? Additionally, the paper adopted van Djik's broad definition of political participants as "those 'elected or appointed, as the central players in the polity,'… but also… politically-engaged citizenry, political organisations, or key commentators in academia and the media."[118] Thus, this paper looks at the publicly-available documentation from this range of political participants to address the above policy analysis questions and glean how Estonian e-governance processes have evolved and shifted with the COVID-19 pandemic. Additionally, this paper provides a foundation for the subsequent studies by identifying the cybersecurity concerns surrounding e-governance, necessitating further research on how e-governance provisions can be secured via cybersecurity governance ecosystems and crisis response. As was noted in the paper itself, the benefit of the exploratory case study approach was that it "allows for in-depth examination of a single case, Estonia, in gleaning increased understanding of a particular phenomenon, Estonian e-government."[119] Indeed, this methodological approach provided a foundational understanding of the Estonian e-governance landscape, setting up the Estonian case as the basis for further analytical examination in subsequent studies.

The approaches of Studies II and III build upon the first paper's use of publicly-available information; the second and third papers then employ expert interviewing as the core method, in order to gain insight into the governance process from the decision-makers themselves. The methodological approaches undertaken in the second and third papers are very similar to one another, as interviewing was carried out for both papers at the same time, from November 2022 to April 2023. However, there was a separate set of questions asked for Study II and for Study III within these interviews and, as outlined below, with Study III, responsible decision-makers only responded to questions related to crises over which they had their purview. These papers used semi-structured expert interviews, speaking to individuals inside the Estonian government, who had their purview over cybersecurity governance and/or e-governance decision-making during the time period examined in this project. However, expert interviewing was not used in isolation, but rather, triangulated vis-à-vis other publicly available information – government documentation, official government messaging, other messaging and commentary, and news media – to verify information presented by interviewees. Methods scholarship points to the various benefits of expert interviewing, including gaining interpretive and procedural knowledge about political processes and events, which is the precise aim of these two papers, looking at the Estonian cybersecurity governance ecosystem, and cybersecurity crisis response, respectively.[120] As noted by Von Soest, expert interviewing can generate important insights "about the 'what' and 'how' of political processes and

[118] Carmichael, 2021, p. 12–13; Van Dijk, 1997, p. 13.

[119] Carmichael, 2021, p. 12.

[120] Littig, 2009, p. 99; Von Soest, 2022, p. 284.

events," which directly aligns with the overarching topics and the more specific research questions of the second and third papers.[121]

Within the field of expert interviewing, there is also an important clarification around what constitutes an expert versus an elite respondent. As noted in methodological scholarship, interviewees can constitute both experts and elites, and thus, I have argued in both of these papers that the respondents in this Estonian case do constitute both.[122] While expertise is "based on real knowledge," the elite are those who "occupy top positions in… political structures," and "exercise significant influence."[123] Amongst the interviewees consulted for this project, are individuals in positions of decision-making power who were directly involved with and greatly influenced the cybersecurity governance process across various parts of the Estonian government; to engage in this process, these individuals similarly possessed the necessary field-specific expertise in the domain of cybersecurity needed to undertake this decision-making in the first place. Furthermore, with these interviews, the decision was undertaken to include 'inside' rather than 'outside' knowledge, as the aim of the papers was to gain insight into the decision-making process from those directly involved with the decision-making process; as the main aim was to consult the personnel "who actually shaped the political or social process of interest" – in this case, cybersecurity governance – the main benefit of these interviewees was their direct participation in the processes being studied, especially vis-à-vis outsiders who did not play a role in this decision-making process.[124] While this inherently leaves 'outside' voices out of this conversation, and is not necessarily representative of Estonian society as a whole, not accounting for other sectors (i.e. private sector or civil society) involved in cybersecurity, it derives information from those most directly involved in the decision-making process, which is arguably the most valuable for deriving insights into the decision-making process itself.

Furthermore, there is a compelling case to be made for the use of interviewing versus other forms of qualitative methodology. For example, the same interview questionnaire that was ultimately used for this research could have been sent out to the respondents and written responses could have been received instead; however, I argue that the richness of the data received by speaking to the interviewees in-person, as well as being able to prompt further elaboration or ask follow-up questions, enriched the project overall. Using semi-structured interviewing allowed for flexibility when conducting the interviews, allowing for follow-up questions and breadth in the response of the interviewees, which ultimately resulted in richer data. For example, an entire additional section of findings in Study III looked at external crises beyond Estonia; this had not been part of the initial questionnaire that focused on four identified crises in Estonia, but rather,

---

[121] Von Soest, 2022, p. 284.

[122] Littig, 2009, p. 108.

[123] Von Soest, 2022, p. 278.

[124] Von Soest, 2022, p. 279.

emerged as an additional and significant finding of the semi-structured interview process. Expert interviewing was also more apt for the research questions being posed than document analysis, as I was interested in the decision-making behind what happened, both in the creation of the Estonian cybersecurity governance ecosystem and the responses to various cybersecurity crises. Though document analysis may have provided insight into the formalised part of the decision-making process, expert interviewing provided insight into the underpinnings of the government process that simply could not have been gleaned exclusively from official documentation. This is indeed reflected in the data that was derived from the interviews.

Expert interviewing was also the most logical choice of methodology relative to the theoretical approaches undertaken in both Studies II and III. Given the collaborative governance approach of Study II, which emphasised the range of stakeholders involved in the cybersecurity governance process and the collaborative dynamics between them, it was apt to interview those stakeholders themselves to gain insight into the dynamics that underpin the Estonian cybersecurity governance ecosystem. Similarly, with Study III, the historical institutionalist theoretical approach treated the four key cybersecurity crises examined in the paper as critical junctures at which cybersecurity governance learnings could be observed, and thus, interviewing the decision-makers involved in the governance processes at those critical junctures was particularly illuminating and appropriate.

An initial list of prospective interviewees was determined using purposive sampling via preliminary research into the cybersecurity governance ecosystem of Estonia, and cybersecurity crises that have befallen the Estonian e-governance system in recent years; information on the decision-makers involved in these processes was typically publicly-available on Estonian government websites with contact information also available.[125] These interviewees were contacted via email, with an introduction to the project and a request for interview. Once the initial list of prospective interviewees was contacted and interviews were arranged and conducted, snowball sampling was employed, whereby the initial interviewees suggested further relevant individuals with whom I should speak.[126] Interviewees were pre-sent the questionnaire, in order to adequately prepare for the questions I would ask, as well as an informed consent form to be signed prior to participation in the interview, which provided details on the use of data for multiple scholarly articles and the right to withdraw from the study. These processes were carried out in line with Estonian research ethics guidelines.[127]

The interview questionnaire consisted of an introductory section of questions, which queried the interviewees' roles and relationship with cybersecurity governance and e-governance in Estonia. This was followed by two topical blocks of questions, one for each of the papers that would be informed by the interviewing,

[125] See, for example, the contacts page of the State Information System Authority (RIA), 2025.

[126] Turner, 2014.

[127] University of Tartu, 2017.

and a final concluding block of questions. The interviews were semi-structured, which allowed for additional ideas to be added by the interviewees, and which also allowed for me to ask follow-up questions or seek clarification on ideas put forward by the interviewees. The format of the interview questionnaire can be seen in Appendix A. For the second paper on the cybersecurity governance ecosystem, I requested that all interviewees answer all questions in the block of questions, which broached their personal and institutional definitions of the term cybersecurity governance, the structure of the cybersecurity governance ecosystem in Estonia, and practical realities of the understandings of the term cybersecurity governance.

For the third paper on cybersecurity crises, I notified interviewees beforehand that I would like them to respond to questions about the crises during which they held decision-making roles. This meant that the interviewees only answered questions surrounding the crises during which they were in decision-making positions. In some instances, interviewees responded to the questions for one or two crises, while in a few instances, interviewees were in decision-making crises during all four crises examined in the paper. For this third paper, in response to both the blocks of questions devoted to Estonian crises and the concluding block of questions, the semi-structured nature of the interviews also prompted responses related to other crises beyond the four crises studied in the paper. For example, responses extended to the 2011 Fukushima earthquake in Japan or the 2017 NotPetya cyberattacks, which targeted Ukraine but ultimately spread globally, and how Estonian cybersecurity governance was undertaken with such external crises in mind.

Ultimately, ten interviews were conducted with officials involved in cybersecurity decision-making, particularly around e-governance, inside the Estonian government. The pool of interviewees was derived from the Ministry of Economic Affairs and Communications (MKM), the Ministry of Defence (MOD), State Information Systems Authority (RIA), Electoral Management Board (EMB), the Presidency of the Republic of Estonia, and the Government Office of Estonia. The interviews ranged in length from 30 minutes to two hours. All interviews and prior communication with interviewees were carried out in English rather than Estonian, as I had only completed one semester of Estonian language training at the time that I began undertaking these interviews. Overall, this did not present issues, as all interviewees spoke English to a high level and articulated ideas clearly. As the published papers that drew from these interviews were also all in English, it allowed quotations to be used directly from the interviews.

These interviews were recorded, and then later transcribed using the Otter AI transcription service, followed with further proofreading to ensure that the transcription matched what was said in the interview, with the original recording file that had been saved in a secure OneDrive deleted upon the completion of this process. Once the transcriptions were completed, the interview transcripts for both the second and third papers were coded in a similar style using a concept-based coding down approach. This approach employed a combination of descriptive coding, firstly, and then interpretive coding, to categorise ideas that emerged

in the interviews, and to do so in line with the research questions posed in each of the respective papers.[128] The approach to coding was used because it "specifically name[s]" and "systematically connects" concepts and governance processes that the respondents mentioned throughout the interviews.[129] The codebooks used to categorise these ideas were developed following Braun and Clarke's thematic analysis, which aims "to record or chart the developing analysis as well as to guide data coding."[130] In Study II, the codebook was developed with the first layer aligned with the two code research questions of the paper, with a second layer for the sub-questions of each initial research question, and a third layer for the common themes of responses provided by the respondents. Conversely, for Study III, the first layer of the codebook was initially developed in line with the four core crises examined in the paper, while subsequent layers addressed the research questions and the different categories of responses and decision-making undertaken within each crisis.

As previously mentioned, all interviewees signed an informed consent form prior to participating in the interviews; in this form, they also selected how they wished to be referred to within the research papers. Of the ten interviewees, four consented to be referred to by their names and positions, while the remaining six interviewees requested to be referred to by a pseudonym based on their current or previous role. I worked with these six interviewees to describe their role in a manner that was sufficiently detailed for the paper, but with which the interviewees were satisfied that their identity would not be compromised. Ultimately, in the second paper, I simply referred to interviewees by the common identifier "Interview A, B, C, etc.," and when roles were utilised, for example in the context of defining the term cybersecurity governance in an approach that was meant to be deliberately layered and multi-faceted, interviewees were referenced merely in alphabetical order of the common identifier. This process of labelling interviewees became more difficult with the third paper, given that the role of interviewees varied significantly across the four crises examined, which ranged from 2007 to 2022. Names were used for the four interviewees who consented to be cited by name; however, the additional six interviewees were referred to by their current or former role, held at the time of the crisis in question. However, there was no common identifier used across the interviewees in this paper, a departure from the second paper. This is because the Estonian cybersecurity and e-governance communities are small, it would be possible to triangulate who held such roles over time, thus rendering the interviewees potentially identifiable, even if pseudonymised.

[128] King, Horrocks, and Brooks, 2019, p. 204.

[129] Strauss and Corbin, 1998, p. 176

[130] Braun and Clark, 2022, p. 12.

3.2. Methodological and Practical Limitations

Some potential limitations arose over the course of conducting this research, but attempts were made to mitigate such limitations to the greatest extent possible. The timeframe examined during this project spans almost two decades, from 2007 and the cyberattacks against the Estonian government, news media, and banking websites in that year. More recent events, such as the COVID-19 pandemic or Russia's full-scale invasion of Ukraine in 2022 were naturally more fresh in the memories of participants, owing to the recency of these events. Despite the elapsed time, interviewees were able to describe the decision-making processes surrounding earlier events, like the 2007 cyberattacks and 2017 eID crisis, in great detail; as an addition to this, information was triangulated and verified vis-à-vis other publicly available information from those times. Additionally, the timeframe examined in this paper was altered over the course of this project, in response to major world events that had an impact on the topics being studied, which could simply not be omitted from this project. Initially, this project looked at the time period of 2007 to 2021; I had been encouraged to have a clearly delineated time period for this project, so as have a contained scope of the project and avoid the difficulties or risks of straying beyond that. However, Russia's full-scale invasion of Ukraine, which began on 24 February 2022, three weeks after I moved to Estonia to begin undertaking this research project, caused me to make a change. It would have, in my view, been irresponsible to examine cybersecurity governance, especially in Estonia, when the cybersecurity landscape was so fundamentally impacted by the full-scale invasion, both for Ukraine and its allies. Therefore, I extended the time period of this project to 2023, to encompass the significant cybersecurity governance responses to the full-scale invasion within the articles comprising my PhD.

Owing to the smallness of the Estonian cybersecurity and digitalisation communities, a few potential limitations arose in the interviewing process. Firstly, there was a small pool of interviewees with whom I could speak. Over the period of 2007 to 2023, personnel in this field have frequently changed roles, both within different parts of government, as well as in the private sector. Sometimes this presented difficulties for tracing and contacting interviewees with whom to speak; however, this difficulty was often mitigated by referrals from previous interviewees, who not only recommended further interviewees via snowball sampling, but also often sent emails of introduction. At one point in the interviewing, responses to my interview requests stagnated slightly; in response, a former Estonian President who participated in the project advised me to follow up on the emails to each of the unresponsive prospective interviews, and to CC the former President in the emails, in order to show their endorsement of the research project and prompt quicker responses from the prospective interviewees. This approach ultimately proved successful in many instances. However, there was still a small number of personnel with whom I was unable to speak, despite numerous efforts – via email, other channels, and through personal connections. This is perhaps a logical outcome, given the busy schedules of government

personnel. Given the time period examined in this PhD project, from 2007 to 2023, there were also potential limitations arising from the time elapsed since the start of this time period and the decision-making processes surrounding the 2007 cyberattacks, responses to this crisis, and the crafting of a cybersecurity governance ecosystem in the years following. There was a risk of recall bias from interviewees, especially when more than a decade had passed since these events at the time of interviewing. In addition to recall bias, there was also potential bias posed by government officials who had an interest in portraying government actions in a positive light. This phenomenon was not present pervasively, as interviewees did indeed show the messiness and multitude of considerations undertaken as they sought to govern cybersecurity. While both of these potential biases were unavoidable, I attempted to mitigate both to the greatest extent possible by triangulating information presented by the interviewees with other publicly-available information, from governmental, news media, and other sources, to verify their claims.

There are also inherent limitations to the scope of this research, by nature of its deliberately narrow focus for this PhD project. As noted earlier in this section, Studies II and III in particular undertook elite interviewing and drew from inside perspectives on the decision-making process, rather than outside ones. While I have previously explained why this approach was taken, it does leave out particular outsider voices in conversations surrounding cybersecurity and e-governance in Estonia. For example, it prioritises governmental interviewees over prospective interviewees in other parts of Estonian society, such as the private sector or civil society actors, as well as everyday citizens. The interviewees also came only from the national-level government, leaving out local government-level actors, although this was quite deliberate, as the phenomena I was examining are governed predominantly at the national-level in Estonia. While the interviewees were selected based on their expertise and roles, they were all ethnically Estonian, and thus not entirely demographically representative of Estonia's makeup. However, this PhD project does not claim to be representative of the whole of Estonian society. Rather, especially in the context of Studies II and III, it aims to derive learnings from the decision-makers most directly involved in crafting Estonia's cybersecurity governance ecosystem and responding to cybersecurity crises affecting its digitalised provisions. This research looks at the institutions and personnel where the decisions were undertaken, rather than looking at interpretation beyond these entities.

As a result of the narrowed scope of the PhD project, various considerations surrounding cybersecurity and e-governance were intentionally omitted because they fell outside of the focus of the project and its studies. For example, there are indeed important and interesting avenues for research surrounding topics such as surveillance, inequality, or data governance, which could also be compellingly studied alongside cybersecurity and e-governance. However, given that this PhD project was concerned with how cybersecurity itself is governed in a highly-digitalised context, and with how a cybersecurity governance ecosystem is formed and how crises are responded to, such aforementioned topics simply fell beyond

the scope of this project and were therefore not considered in-depth in the project or its studies. Including such topics in this research would have represented an over-extension, and possibly also necessitated changes in the methodological or theoretical approaches. These topics represent potential avenues for future research into adjacent topics related to e-governance and cybersecurity; however, in its current form, this project has a bounded topical focus that aligns with the theoretical frameworks and methodological decisions undertaken.

4. FINDINGS

This section outlines the ways in which the overall project addresses the overarching research questions, while also looking at the specific findings of each study. Furthermore, this section justifies how these findings are connected to one another, while contributing to gaps in the existing body of literature.

4.1. Major Findings of Studies I, II, and III

Collectively, these studies have addressed the overarching research questions posed in this PhD project: *in what ways have the cybersecurity governance models aimed at securing e-governance provisions in Estonia evolved over the period of 2007 to 2023, and whether and in what ways do critical events or changed circumstances explain the changes in these cybersecurity governance models over time?* Indeed, overall approaches to cybersecurity governance in 2023, at the end of the time period examined for this project, look fundamentally different from those which existed in 2007, at the beginning of this focal time period. While Estonia's digital transformation was already well underway in 2007, the 16 years examined in this PhD project saw a significant expansion of the e-governance offerings. Although electronic identification, X-Road as a data exchange platform, some e-services, and internet voting were already available, by the onset of the COVID-19 pandemic in 2020, real estate transactions, marriage, and divorce were the only services not yet available online, all of which have since become available online. With this increasingly digitalised context, the 'surface area' for potential cyberattacks and incursions increased too, prompting a need for policy to address this ever-evolving domain. Thus, both the broader shift in the global cybersecurity threat landscape and specific critical events (for example, the crises examined in Study III) significantly shaped changes in cybersecurity governance over the period of 2007 to 2023. The governance structures in place in Estonia, aimed at dealing with cybersecurity, were impacted by changed circumstances, namely increased digitalisation, which saw the selection of the Ministry of Economic Affairs and Communications holding primary ministerial purview for cybersecurity, on the basis of its relationship with the private sector for digitalisation-related relationships. Furthermore, critical cyber incidents, such as the 2007 cyberattacks or the eID crisis in 2017, also shaped subsequent changes to cybersecurity governance structures, the implementation of policies, and specific approaches to cybersecurity in domains such as communications, all of which were aimed at bolstering future cybersecurity.

More broadly, these studies have collectively demonstrated that a highly-digitalised context, featuring advanced and mature e-governance provisions, will have high cybersecurity needs, by nature of the wider prospects for cyberattacks or other cyber incursions in such a digitalised setting. Thus, there is a need for an appropriate cybersecurity governance ecosystem to be established, which reflects

both the cybersecurity needs and localised priorities – which may include governance, security, and cultural realities – of a particular setting. Finally, while such initiatives generally contribute to a more secure environment for digitalised provisions, it certainly remains possible that cyberattacks and cyber incursions, potentially leading to cyber crises, can still unfold. Thus, it is important that, within this cybersecurity governance ecosystem, there are parameters in place for dealing with crisis from a technical standpoint, as well as policy and communication perspectives, all aimed at bolstering the cybersecurity of digitalised provisions in the future. Together, the findings of Studies I, II, and III have indicated that cybersecurity governance models, specifically those aimed at securing e-governance provisions in the highly-digitalised Estonian context, have indeed changed over the period of 2007 to 2023, in the myriad specific and more general ways described above.

Study I aimed to contextualise the state of the e-governance system in Estonia around the time of the COVID-19 pandemic, exploring how the e-governance offerings evolved with the pandemic and beyond. By the onset of the COVID-19 pandemic at the start of 2020, a robust offering of digitalised provisions were already available in Estonia; the major exceptions were three particular e-services – marriage, divorce, and real estate transactions – and the provision of education, which was predominantly an in-person undertaking prior to the pandemic. However, the onset of the COVID-19 pandemic prompted the introduction of new digitalised services, namely the move to fully online education dating from the earliest days of lockdowns, the introduction of contact tracing applications to align with the new public health realities of the pandemic, and the repurposing of technologies from Estonia's e-Residency programme for use in real estate transactions, a provision that had previously not been digitalised. An additional finding from this paper focused on the expansion of Estonia's e-governance, in both domestic and international contexts, both underscoring the global relevance of Estonian e-governance and the continued need for innovation and adaptation domestically. The paper acknowledges that Estonia is no longer unique as an exporter of e-governance solutions, as other countries have innovated in this space as well, but a combination of the e-governance system's availability, effectiveness, and efficiency, alongside effective branding, tailored international outreach, and continued strategic assessment of the system have provided opportunities for the expansion of Estonian e-governance practices beyond the country's borders.[131] By exploring the e-governance system of Estonia and its specific workings and needs, Study I also implicitly identified cybersecurity concerns across various parts of this system, including in e-learning and expanded e-services, which provide a foundation for studying more specific aspects of cybersecurity governance in a highly digitalised setting in subsequent papers.

Study II sought to examine the development of the cybersecurity governance ecosystem in Estonia over time, as well as practical and institutional under-

[131] Carmichael, 2021, p. 46–47.

standings of the term cybersecurity governance and the realities that can arise from these understandings. Firstly, this study found that the 2007 cyberattacks prompted cybersecurity governance as a policy concern requiring institutional structure and ministerial responsibility to be shifted from the Ministry of Defence (MOD) to a predominantly civilian purview under the Ministry of Economic Affairs and Communications (MKM), along with the empowerment of the State Information System Authority (RIA) and CERT. The decision to make this ministerial shift was largely due to the Estonian prioritisation of digitalisation, given that MKM had strong relations with the private sector for digitalisation-related engagement. Interestingly, the term cybersecurity governance is not formally codified, but is defined by a strong informal consensus, rooted in shared norms and values, held amongst relevant stakeholders. While tensions did occasionally emerge around understandings of cybersecurity governance, this was often due to small ambiguities in the roles, or differing leadership styles in key roles, and could be mitigated by interpersonal connections within the tight-knit Estonian cybersecurity community or RIA auditing mechanisms. These instances also demonstrated Emerson and Ahn's collaborative dynamics, showing instances of principled engagement, shared motivation, and joint capacity in the establishment and implementation of the Estonian cybersecurity governance ecosystem, with a common goal of securing extensive e-governance provisions in the country.

Study III looked at four key cybersecurity crises impacting Estonian e-governance – the 2007 cyberattacks, the 2017 eID crisis, the COVID-19 pandemic, and Russia's full-scale invasion of Ukraine in 2022 – to examine the decision-making processes that followed these crises. Specific decision-making outcomes included, for example, the establishment of the NATO Cooperative Cyber Defence Centre of Excellence, funding for cybersecurity-related education initiatives, and the creation of new cybersecurity governance structures (arising from the 2007 cyberattacks) and 'lessons learned' processes for reflection and improvement post-crisis (a main outcome of the 2017 eID crisis). More broadly, three consistent governance themes were present across these crises: the first was learning from experience across each crisis examined in this study, and from external crises, for additional preparedness in the event of future crises or cybersecurity threats. This includes crafting an ecosystem for governing cybersecurity that reflects the localised needs of a place and having crisis preparedness measures in place. Second, was a clear and transparent communication approach to cyber crises, to ensure that cybersecurity-related information is relayed effectively to the general public. Third, these crises showed the importance of innovation in times of non-crisis, as the crises examined often acted as expediters of ongoing policy ideas or initiatives. It is crucial to consistently innovate in the cybersecurity domain, despite potential barriers to actually pushing ideas through, as such ideas can be of most use and possibly put in place quicker in times of crisis.

These findings are collectively part of a nuanced mechanism, which exists at different parts of the crisis cycle. For example, crafting a cybersecurity ecosystem and innovation on cybersecurity-related topics takes place in times of non-crisis, where cyberattacks or other major cyber incidents are not unfolding in a crisis

environment. Conversely, the clear and transparent communications approach would be most necessary as a cyber crisis unfolds. Therefore, while these specific findings, and how they are carried out in a government context, do not hold relevance at all times, they have importance based on circumstance and especially timing within the crisis cycle. It is crucial that all parts of this mechanism exist, however, as they interact with one another, arising in different times. The interplay between these mechanisms may also offer an interesting avenue for further research, to investigate how these mechanisms interact as governance processes are undertaken amidst crisis and non-crisis, and if any of these themes have greater relative importance.

4.2. Contributions and Linkages Between Studies

As noted in section 2, this research project, and the specific papers that comprise it, aim to contribute theoretically to gaps in the current body of scholarship, as well as practically, with implications for government entities in Estonia and beyond. More broadly, these papers contribute to literature on cybersecurity and e-governance, but additionally, they contribute new knowledge to specific gaps on policy change and collaborative governance (Study II) and historical institutionalism and crisis management (Study III) in the domain of cybersecurity. Study I has provided a comprehensive overview of the Estonian e-governance system surrounding the COVID-19 pandemic via an exploratory case study, providing an in-depth examination of Estonia as a critical case in the fields of e-governance and cybersecurity. The article looks at the prospects for further development of this system domestically and internationally, while also identifying the specific cybersecurity needs of the Estonian e-governance system that provide a foundation for the topics examined in Studies II and III. Study II has approached the development and evolution of the Estonian cybersecurity governance ecosystem, holding this multi-faceted and multi-stakeholder process up to collaborative governance literature, specifically the collaborative dynamics of Emerson and Ahn. In doing so, this study has provided a novel contribution by bringing the cybersecurity domain into policy change literature, while also applying a collaborative governance theoretical framework in a compelling new domain. Furthermore, it has built upon the work of Study I, by showing how a cybersecurity governance ecosystem is formed in a highly digitalised setting, like the context of digitalisation that was explored in-depth in the first paper. Study III has examined crisis management and decision-making in response to key cybersecurity crises befalling the Estonian e-governance system over a 16-year period, representing a departure from the existing body of crisis management and cybersecurity literature outlined in section 2. This study has built upon both Studies I and II, looking at crisis in a highly digitalised context, in the critical Estonian case, while also examining how governance and decision-making were undertaken within the cybersecurity governance ecosystem that was examined in Study II.

There are inherent linkages between these papers themselves and the contributions that they make; the findings in these three studies are intrinsically connected and collectively address the broader research questions posed in this research project, focused on the development of cybersecurity governance pertaining to e-governance over time in the Estonian context. In the findings of these papers there is significant cross-over, as consistent ideas re-emerge in this research, validating their overall contributions. These studies build upon one another, firstly with Study I, by laying the foundations of the project and providing an overview of the Estonian e-governance system to be examined throughout the project, collating publicly available information to depict this digitalisation landscape and its evolution over time. This study has also identified the specific needs, particularly the cybersecurity concerns, around Estonian e-governance, necessitating further research on how cybersecurity can be governed, especially in a highly-digitalised setting. Next, Study II continues by looking at the development of this cybersecurity governance ecosystem and how it has shifted over time, while analytically broaching the practical realities of defining the term cybersecurity governance, the complexities of which were already introduced in section 2. Finally, Study III continues to build upon the themes of Study I and Study II, but looking at governance responses in times of cybersecurity crises that affect e-governance; this study looks at cybersecurity crises that have occurred in a highly-digitalised context, while examining how such crises are broached within the cybersecurity governance ecosystem that has been instituted in order to address such cybersecurity concerns.

There is a common thread across these studies surrounding ideas of times of crisis and non-crisis, which is present in all three papers. Indeed, the COVID-19 pandemic prompted some e-governance service expansion in Study I, while the 2007 DDoS cyberattacks were the impetus for the crafting of a coherent cybersecurity governance ecosystem in Study II, and all four crises domestically, in addition to external crises, prompted core policy changes and initiatives intended to bolster cybersecurity in the future, as outlined in Study III. Thus, this finding, across all three papers, emphasises an overarching idea that innovation in the cybersecurity domain must be ongoing and ever-evolving to adapt to changing realities and cyber threat landscapes. Doing so facilitates a level of preparedness that means when crisis does strike, a likely possibility in the current cyber threat landscape, innovation will likely be expedited and can be leveraged to bolster future cybersecurity. Theoretically, these studies are linked by the collaborative governance and historical institutionalist theories that they apply; in Study II, the collaborative governance approach encompasses a broad range of actors involved in a particular governance process – in this case, cybersecurity governance – with stakeholders across different government entities and the private sector working together toward a common goal of bolstered cybersecurity. While Study III employs historical institutionalist theory, treating cybersecurity crises as critical junctures, key points at which decision-making and governance processes unfold. These theories are intrinsically connected in the study of cybersecurity governance: a large range of actors across different institutions are engaged in the

cybersecurity governance process, engaging in a myriad of different ways, and when faced with critical junctures, typically in the form of a cybersecurity crisis, these actors will be required to engage with one another in the governing and decision-making surrounding cybersecurity.

Together, these articles have sought to answer the overarching research question of how the cybersecurity governance of Estonian e-governance has evolved over the period of 2007 to 2023, by illustrating the ways in which cybersecurity governance has shifted, alongside e-governance, shaped by domestic and international realities, and internal and external crises, in a manner that is nuanced, non-linear, and reflective of the given circumstances of the time. They demonstrate the high cybersecurity needs of a mature highly-digitalised setting, and the subsequent governance processes – based in multi-faceted and multi-stakeholder collaborative dynamics, and crisis response – to ensure preparedness for and response to ever-evolving cybersecurity realities.

5. DISCUSSION

While the previous section discussed the linkages and contributions of the overarching research project, as well as the individual papers that comprise it, this section discusses the overall implications of this research and the prospective avenues for future research stemming from this research project.

The first major set of implications of this project are theoretical. As outlined in section 2 and 4, there is currently a predominant focus in the literature on international cybersecurity governance, or the examination of the topic of domestic cybersecurity governance from varied settings; thus, this project contributes knowledge to cybersecurity governance scholarship within a domestic, single-country context, using the valuable critical case of Estonia. It is important and illuminating to have research focusing on domestic settings, as it is complementary to the existing literature on international cybersecurity governance, while simultaneously providing new knowledge on well-functioning cybersecurity governance in a domestic context. This research project provides compelling new scholarship on the cybersecurity governance processes particularly surrounding e-governance, in a single-setting critical case, a mature and pervasive instance of digitalisation requiring cybersecurity provisions. Domestic contexts comprise the international context in the first place, so it is crucial that research in both domains exists. Additional theoretical contributions come via the application of new or underused theoretical approaches to the domain of cybersecurity governance. Study II's use of collaborative governance to examine policy change in the domain of cybersecurity governance is twofold, first it presents cybersecurity governance as a timely and relevant domain to examine in the context of policy change, and second, it validates and extends the use of Emerson and Ahn's collaborative dynamics in a multi-faceted and multi-stakeholder cybersecurity context. It shows that a myriad of actors involved in the cybersecurity governance process can act in pursuit of a common goal, cybersecurity, and craft an overarching cybersecurity governance ecosystem, ultimately showing how policy change occurs in the domain of cybersecurity governance through a lens of collaborative governance. Study III's use of a historical institutionalist approach, treating cyber crises as critical junctures that prompt governance decision-making and responses, is also a notable and novel contribution to the broader body of cybersecurity governance scholarship, where literature on cybersecurity crises, more broadly, is currently rather scarce.

There are indeed also practical implications arising from the findings of this research project. Overall learnings surrounding the conditions for the establishment of a cybersecurity governance ecosystem via adaptive institutional structures that reflect on-the-ground intricacies and realities, innovation in times of crisis and non-crisis, and public and ongoing communications around cybersecurity more broadly, and crises more specifically, are all applicable and useful for governments around the world undergoing various stages of their respective digital transformations. A number of findings in Studies II and III are particularly

illuminating and adaptable for the localised intricacies of other governmental settings. Study II has shown that the cybersecurity governance ecosystem in Estonia placed primary ministerial purview with MKM, as a way of prioritising the country's digitalisation, given the ministry's strong relationships with the private sector providers of digitalisation solutions. This shows that primary cybersecurity purview should be determined with the unique policy needs and intricacies of a place prioritised. Furthermore, Study II showed that, in Estonia, cybersecurity governance as a term was not codified but, rather, commonly understood by cybersecurity personnel across the government based on shared goals and values within this domain. Thus, cybersecurity governance rooted in shared culture and priorities is critical and embedded in broader political and security contexts that shape the culture more broadly. While these findings are unique to Estonia's specific context, more broadly, these findings could be applicable in other settings. When crafting a cybersecurity governance ecosystem, a government may not prioritise digitalisation like Estonia, but will have other governmental priorities based on political, cultural, security, or other nuances of that particular place. Thus, cybersecurity governance in a specific setting is indicative of and shaped by the broader local context. Similarly, the concept and approach to cybersecurity governance itself should be commonly understood, whether by codified or non-codified means; determining whether to codify this understanding should be based on shared culture and values surrounding cybersecurity in a particular setting. Additionally, Study III found multiple crisis management approaches, employed by the Estonian government, which could be adapted for use by other governments facing cybersecurity crises in their e-governance systems. Firstly, a clear and transparent communications approach, aimed at reassuring a potentially concerned general populace. Secondly, a trend of learning from prior experience to shape responses in the event of future cybersecurity events or even crises. Thirdly, this study revealed a need to innovate in times of non-crisis, as crisis can expedite policies or other initiatives. These learnings could be applied to other settings, where governments could communicate clearly, undergo reflection and learning processes, and prompt innovation in times of non-crisis to bolster preparedness. Thus, the new knowledge generated in this research on Estonia could be potentially useful in specific settings such as emerging e-governance systems, small nations, or local governments in larger settings, with the potential to scale these learnings to other settings as well. Additionally, this research on cybersecurity governance and e-governance in Estonia is particularly informative to the Estonian government itself, as this system and the changing realities and threat landscape continue to evolve in the future.

There are several prospective avenues for future research that stem from the findings of this research project. Because of the contained nature of the timeframes studied in this research project, from 2007 to 2023, and also due to the fast-paced changes ongoing in the fields of cybersecurity and e-governance, there are several new directions for research in the ensuing years resulting from the Estonian case, that go beyond the scope of this research project. Beyond Study I, which outlined the Estonian e-governance system at the time of the COVID-19

pandemic, could be an update to represent the present-day landscape, five years later. At the time of conducting the research in Study I, at the onset of the COVID-19 pandemic, the Estonian government prominently noted that the online provisions not available online in Estonia were marriage, divorce, and real estate transactions.[132] Within one of the findings of Study I, that COVID-19 prompted an expansion of e-services in Estonia, was that authentication technologies used for the Estonian e-Residency programme from private-sector partner Veriff were repurposed for use in a real estate setting, moving that provision online.[133] By the end of 2024, marriage and divorce were also available online, and by early 2025, the Estonian government pronounced that it was 100% digital.[134] Therefore, the overview of Estonian e-governance from Study I could be updated to encompass the present day, while examining what factors, whether crisis or non-crisis elements, prompted said changes. Examining these changes and shifts in the landscape, of both digitalisation and cybersecurity governance, over a more prolonged period of time could have interesting practical and research outcomes for both the Estonian case and other international contexts, as other governments similarly seek to expand their e-governance offerings.

While I argue that there are valuable learnings from the Estonian context for governmental settings beyond Estonia's borders, there are certainly instances where one might expect these learnings to travel best into other contexts. For example, these learnings would likely be most applicable in contexts where a set of features similar to Estonia exist: a democratic system of governance, but also a unitary governance structure, and a small and highly-digitalised setting. However, these conditions are not the only requisites for the applicability of Estonian learnings. The first condition, democracy, may indeed be requisite; it is unlikely that the governance learnings would travel well into a non-democratic context. The other conditions, conversely, may require more extensive adaptability to apply learnings from Estonia to an external context. For example, a federal system of governance, a larger country, or a state with a lower level of digital maturity may still learn from Estonia, but with more adaptation to their localised context required. This comparative research, alongside other research pathways, could be explored in greater depth in future research.

This PhD project could contribute to a continued research programme, in both the conceptual approaches and theoretical frameworks applied in the studies of this PhD project, especially as they relate to the domain of cybersecurity. Policy change remains a phenomenon to be studied in relation to cybersecurity governance, as the rapidly-changing cyber threat landscape means that policy and governance structures must be in place to broach such threats. Given the multi-faceted and multi-stakeholder nature of cybersecurity governance, both in Estonia and beyond, collaborative governance theory, and especially the collaborative

[132] Carmichael, 2021, p. 26.

[133] Carmichael, 2021, p. 37.

[134] Kriisa, 2025.

dynamics examined in Study II, remain a compelling lens through which to examine the phenomena of policy change in the cybersecurity domain. Also related to the evolving cyber threat landscape, it remains likely that cyber crises will continue to unfold, as new and sophisticated methods of cyberattacks and other cyber incursions emerge. Thus, there are possibilities for further research on governance responses to cyber crises using historical institutionalist theory as in Study III, in order to trace critical junctures and path dependencies over time, with a specific focus on bolstered cybersecurity measures being the product of path dependencies in policies and decision-making.

There are also avenues for further research specifically at the nexus of cybersecurity governance and e-governance in the Estonian case, as an extension of this PhD project. While Study II examined the formation of the Estonian cybersecurity governance ecosystem and its shift of primary ministerial purview from the Ministry of Defence to the Ministry of Economic Affairs and Communications, there are now prospects for future longitudinal study of the institutional structures for cybersecurity governance in Estonia and what prompts shifts within them. As of 1st January 2025, the primary ministerial purview for cybersecurity within the Estonian government has shifted once again, from MKM to a newly-created Ministry of Justice and Digital Affairs.[135] This shift was undertaken in order to prioritise aligning Estonia's digitalised system and processes with legislation more closely.[136] An initial assessment of this new ministerial purview, shows the decision to place responsibility with the Ministry of Justice and Digital Affairs aligns with Study II's finding that the ministerial purview is decided based on policy priorities of the time; while that priority was digitalisation relationships with the private sector and MKM in Study II, that priority is seemingly the alignment of legislation and digitalisation with the Ministry of Justice and Digital Affairs. Thus, this additional shift in Estonia's cybersecurity governance ecosystem offers an interesting opportunity to examine the Estonian case over a more extended period of time, while also potentially deriving broader lessons for other settings with shifts in cybersecurity governance, and institutional structures more broadly, over time. Additionally, such a study could further theoretical contributions in the study of collaborative governance and collaborative dynamics in the field of cybersecurity governance, by examining the evolution of these processes over a more extended time period.

These findings, arising from the research project, also open potential avenues for comparative case studies to examine cybersecurity governance ecosystems and their relationship to e-governance systems in other countries or governmental settings, as well as cybersecurity crisis management and decision-making. Previously outlined scholarship, including Boeke and Collier, has examined Estonia comparatively with countries such as the United Kingdom, the Netherlands, or Czechia on other aspects of cybersecurity governance and institutional structures

[135] Mäekivi, 2025.

[136] Republic of Estonia Ministry of Justice and Digital Affairs, 2025.

for crisis response. As previously mentioned, comparative research on these topics between Estonia and other mature cases are currently rather lacking, therefore this could provide interesting new avenues for research on the topics of crafting a cybersecurity governance ecosystem or responding to cybersecurity crises that impact e-governance structures. Additionally, these topics could be studied vis-à-vis other small states, with high levels of digitalisation or sophisticated cybersecurity governance structures, such as Singapore, or with less mature case studies, such as Costa Rica or Albania, as most-different cases in terms of digital maturity, as they develop over time. Such research could provide theoretical contributions in the domain of cybersecurity vis-à-vis collaborative governance or historical institutionalism, the approaches used in this project, by providing comparative insight into mature cases; it could also provide practical learnings on these topics for younger cases, in instances where governments continue to develop their e-governance systems and cybersecurity governance. However, this represents a non-exhaustive list of possible future research directions resulting from this project.

6. CONCLUSION

This research project has broached the Estonian cybersecurity governance and e-governance systems over the period of 2007 to 2023, responding to the overarching questions, which queried: in what ways have the cybersecurity governance models aimed at securing e-governance provisions in Estonia evolved over the period of 2007 to 2023, and whether and in what ways do critical events or changed circumstances explain the changes in these cybersecurity governance models over time? This project has done so via three research papers, which examined 1) the evolution of Estonia's e-governance landscape in line with the COVID-19 pandemic, 2) the development of the Estonian cybersecurity governance ecosystem over time and understandings surrounding cybersecurity governance itself within the Estonian government, and 3) governmental crisis response and decision-making around four key cybersecurity crises affecting e-governance (the 2007 cyberattacks, the 2017 eID crisis, the 2020 COVID-19 pandemic, and Russia's 2022 full-scale invasion of Ukraine). In doing so, and by using Estonia as a critical case in the topics of digitalisation and cybersecurity, this project has made valuable theoretical and practical contributions, contributing to existing scholarship and potentially informing both the Estonian government and other governments undergoing digital transformation.

Firstly, the project has made important contributions to gaps in existing scholarship conceptually by examining the phenomena of policy change and crisis response, and theoretically by applying collaborative governance and historical institutionalist theories. As noted in the literature review above, cybersecurity governance as a domain for research in these broader theoretical fields remains rather scarce, and there is much new knowledge to be derived in these fields. This project has contributed to some of the existing gaps in the scholarship at the nexus of cybersecurity governance, e-governance, and these theoretical approaches. This project has also indicated pathways for further research in these theoretical domains, which could contribute to a compelling research programme of cybersecurity governance, as the global cybersecurity landscape inevitably continues to evolve in coming years. More practically, Estonia's learnings over a rather extensive period of experience with digitalisation and cybersecurity offer valuable insights to governments elsewhere as they similarly undergo digital transformation and potentially face cybersecurity crises. Specifically, governments beyond Estonia could adapt Estonian approaches to crafting a cybersecurity governance ecosystem and responding to cybersecurity crises to their own localised intricacies. As noted in the previous section, these learnings would likely travel best to other democratic, unitary, small, and highly digitalised governments but could also be adapted for other contexts. This could include the prioritisation of certain policy areas when allocating ministerial purview within a cybersecurity governance ecosystem, or crafting crisis responses with clear communications, promoting cybersecurity innovation in times of non-crisis, and learning from prior crises to bolster cybersecurity of digitalisation provisions in

the future. As has been noted earlier, this project does not advocate for a direct replication of Estonian practices in other settings, but rather, a thoughtful employment of the learnings derived from each of the studies comprising this research project, applied in the intricacies of the localised context. There are inherently practical learnings on institutional setup and cybersecurity governance ecosystems, and crisis response that, while endemic to Estonia's particular context, could certainly have practical applicability in other contexts amidst a dynamic and ever-changing cybersecurity threat landscape that appears poised to continue evolving into the future.

REFERENCES

Annamalah, Sanmugam. 2024. "The Value of Case Study Research in Practice: A Methodological Review with Practical Insights from Organisational Studies." *Journal of Applied Economic Sciences* 19 (16): 485–98. https://doi.org/10.57017/jaes.v19.4(86).11.

Ansell, Chris, and Alison Gash. 2008. "Collaborative Governance in Theory and Practice." *Journal of Public Administration Research and Theory* 18 (4): 543–71. https://doi.org/10.1093/jopart/mum032.

Antoniuk, Daryna. 2024. "'Unprecedented' Interference Targets Moldova's Elections." Therecord.media. October 21, 2024. https://therecord.media/unprecedented-interference-moldova-elections-cyberattack.

Areng, Liina. 2013. "International Cyber Crisis Management and Conflict Resolution Mechanisms." In *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy*, edited by K. Ziolkowski, 565–93. NATO Cooperative Cyber Defence Centre of Excellence.

Aru-Chabilan, Heli. 2020. "Tiger Leap for Digital Turn in the Estonian Education." *Educational Media International* 57 (1): 61–72. https://doi.org/10.1080/09523987.2020.1744858.

Backman, Sarah. 2015. "Organising National Cybersecurity Centres." *Information & Security: An International Journal* 32 (1): 9–26. https://doi.org/10.11610/isij.3206.

———. 2020. "Conceptualizing Cyber Crises." *Journal of Contingencies and Crisis Management* 29 (4). https://doi.org/10.1111/1468-5973.12347.

Bannister, Frank, and Regina Connolly. 2012. "Defining E-Governance." *E-Service Journal* 8 (2): 3–25. https://doi.org/10.2979/eservicej.8.2.3.

Bardach, Eugene. 2006. "Policy Dynamics." In *The Oxford Handbook of Public Policy*, edited by Michael Moran, Martin Rein, and Robert E. Goodin, 336–66. Oxford: Oxford University Press.

Belrhiti, Zakaria, Maryam Bigdeli, Anis Lakhal, Kawtar Dib, Saad Zbiri, and Sanaa Belabbes. 2024. "Unravelling Collaborative Governance Dynamics within Healthcare Networks: A Scoping Review." *Health Policy and Planning* 39 (4). https://doi.org/10.1093/heapol/czae005.

Bennett, Colin, and Michael Howlett. 1992. "The Lessons of Leaming: Reconciling Theories of Policy Leaming and Policy Change." *Policy Sciences* 1: 275–94. https://www.sfu.ca/~howlett/documents/16845049.pdf.

Berg, Kristi, Joseph N. Crawford, and Thomas Seymour. 2016. "Unbreakable: A Concise Overview of Cybersecurity." *Issues in Information Systems* 17 (4). https://doi.org/10.48009/4_iis_2016_208-221.

Biberaj, Aleksander, Enida Sheme, Alban Rakipi, Sonila Xhaferllari, Renalda Kushe, and Mirjeta Alinci. 2022. "Cyber Attack against E-Albania and Its Social, Economic and Strategic Effects." *Journal of Corporate Governance, Insurance, and Risk Management* 9 (2): 341–47. https://doi.org/10.56578/jcgirm090204.

Boeke, Sergei. 2017. "National Cyber Crisis Management: Different European Approaches." *Governance* 31 (3): 449–64. https://doi.org/10.1111/gove.12309.

Boin, Arjen, Paul 't Hart, Eric Stern, and Bengt Sundelius. 2017. *The Politics of Crisis Management*. Cambridge, UK: Cambridge University Press.

Braun, Virginia, and Victoria Clarke. 2022. "Conceptual and Design Thinking for Thematic Analysis." *Qualitative Psychology* 9 (1): 3–26. https://doi.org/10.1037/qup0000196.

Broeders, Dennis, Liisi Adamson, and Rogier Creemers. 2019. “Coalition of the Unwilling? Chinese and Russian Perspectives on Cyberspace.” Ssrn.com. October 2019. https://ssrn.com/abstract=3493600.

Bullock, Charles S, and Charles M Lamb. 1984. *Implementation of Civil Rights Policy*. Thomson Brooks/Cole.

Collier, Jamie. 2016. “Strategies of Cyber Crisis Management: Lessons from the Approaches of Estonia and the United Kingdom.” *Ethics and Policies for Cyber Operations*, December, 187–212. https://doi.org/10.1007/978-3-319-45300-2_11.

“Contacts: RIA.” 2025. Republic of Estonia State Information System Authority. 2025. https://www.ria.ee/en/contact.

Coombs, Timothy. 2018. “Crisis Communication.” *The International Encyclopedia of Strategic Communication*, August, 1–12. https://doi.org/10.1002/9781119010722.iesc0054.

Coombs, W. Timothy, Sherry J. Holladay, and Elina Tachkova. 2019. “Crisis Communication, Risk Communication, and Issues Management.” In *Public Relations Theory: Application and Understanding*. Hoboken, NJ: Wiley-Blackwell.

Craigen, Dan, Nadia Diakun-Thibault, and Randy Purse. 2014. “Defining Cybersecurity.” *Technology Innovation Management Review* 4 (10): 13–21. https://doi.org/10.22215/timreview/835.

Crandall, Matthew, and Collin Allan. 2015. “Small States and Big Ideas: Estonia’s Battle for Cybersecurity Norms.” *Contemporary Security Policy* 36 (2): 346–68. https://doi.org/10.1080/13523260.2015.1061765.

Crenson, Matthew A. 1971. *The Un-Politics of Air Pollution: A Study of Non-Decisionmaking in the Cities*. The Johns Hopkins Press.

Crowe, Deserai A., Rob A. DeLeo, Elizabeth A. Albright, Kristin Taylor, Tom Birkland, Manli Zhang, Elizabeth Koebele, Nathan Jeschke, Elizabeth A. Shanahan, and Caleb Cage. 2022. “Policy Learning and Change during Crisis: COVID-19 Policy Responses across Six States.” *Review of Policy Research* 40 (1): 10–35. https://doi.org/10.1111/ropr.12511.

D’Agostino, Maria Josephine, Richard Schwester, Tony Carrizales, and James Melitski. 2011. “A Study of E-Government and E-Governance: An Empirical Examination of Municipal Websites.” *Public Administration Quarterly* 35 (1): 3–25. http://dx.doi.org/10.2307/41804540.

Datta, Pratim Milton, and Thomas Acton. 2024. “Ransomware and Costa Rica’s National Emergency: A Defense Framework and Teaching Case.” *Journal of Information Technology Teaching Cases*, December, 204388692211490. https://doi.org/10.1177/20438869221149042.

Denzin, Norman K., and Yvonna S. Lincoln. 1994. *Handbook of Qualitative Research*. Thousand Oaks, CA: Sage.

Deutsch, Karl Wolfgang. 1965. *The Nerves of Government: Models of Political Communication and Control*. New York, N.Y.: Free Press.

Dunleavy, Patrick, Helen Margetts, Simon Bastow, and Jane Tinkler. 2008. *Digital Era Governance*. OUP Oxford.

Emerson, Kirk, and Minwoo Ahn. 2015. “Collaborative Governance Regimes: Informing Practice through Research.” In *Collaborative Governance Regimes*. Washington, D.C.: Georgetown University Press.

Emerson, Kirk, Tina Nabatchi, and Stephen Balogh. 2012. “An Integrative Framework for Collaborative Governance.” *Journal of Public Administration Research and Theory* 22 (1): 1–29. https://doi.org/10.1093/jopart/mur011.

Ernsdorff, Marc, and Adriana Berbec. 2007. “Estonia: The Short Road to E-Government and E-Democracy.” In *E-Government in Europe*, 171–83. Routledge.

ERR News. 2020. “President: Estonia Set Cyber Threat Precedent on UNSC.” ERR News. May 5, 2020. https://news.err.ee/1085703/president-estonia-set-cyber-threat-precedent-on-unsc.

———. 2023. “President Karis: Cyber Security Must Involve Whole of Society.” *ERR News.*, June 1, 2023.

“Estonian Code of Conduct for Research Integrity.” 2017. University of Tartu. University of Tartu. 2017. https://ut.ee/sites/default/files/inline-files/code_of_conduct_for_research_integrity_eng_1.pdf.

European Commission. 2022. “The Digital Economy and Society Index (DESI).” *European Commission* . https://digital-strategy.ec.europa.eu/en/policies/desi.

Ferdousi, Bilquis. 2024. “The Importance of Defining Cybersecurity from a Transdisciplinary Approach.” *Journal of Systemics, Cybernetics, and Informatics/Journal of Systemics Cybernetics and Informatics* 22 (1): 150–64. https://doi.org/10.54808/jsci.22.01.150.

Fichtner, Laura. 2018. “What Kind of Cyber Security? Theorising Cyber Security and Mapping Approaches.” *Internet Policy Review* 7 (2). https://doi.org/10.14763/2018.2.788.

Fidler, Bradley. 2017. “Cybersecurity Governance: A Prehistory and Its Implications.” *Digital Policy, Regulation and Governance* 19 (6): 449–65. https://doi.org/10.1108/dprg-05-2017-0026.

Fioretos, Orfeo, Tulia G. Falleti, and Adam Sheingate. 2016. “Historical Institutionalism in Political Science.” In *Oxford Handbook of Historical Institutionalism*, edited by Orfeo Fioretos, Tulia G. Falleti, and Adam Sheingate, 1–32. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199662814.013.1.

Flyvberg, Bent. 2011. “Case Study.” In *The Sage Handbook of Qualitative Research (4th Edition)*, edited by Norman K. Denzin and Yvonna S. Lincoln, 301–16. Thousand Oaks, CA: Sage.

Georgieva, Ilina. 2019. “The Unexpected Norm-Setters: Intelligence Agencies in Cyberspace.” *Contemporary Security Policy* 41 (1): 33–54. https://doi.org/10.1080/13523260.2019.1677389.

Giles, Keir. 2012. “Russia’s Public Stance on Cyberspace Issues.” IEEE Xplore. June 1, 2012. https://ieeexplore.ieee.org/document/6243966.

Hall, Peter A. 1993. “Policy Paradigms, Social Learning, and the State: The Case of Economic Policymaking in Britain.” *Comparative Politics* 25 (3): 275–96. https://doi.org/10.2307/422246.

Härmand, Kai. 2021. “Digitalisation before and after the Covid-19 Crisis.” *ERA Forum*, February. https://doi.org/10.1007/s12027-021-00656-8.

Heikkila, Tanya, and Andrea K. Gerlak. 2015. “Case Illustration: The Everglades Restoration Task Force.” In *Collaborative Governance Regimes*, edited by Kirk Emerson and Tina Nabatchi, 73–80. Washington, D.C.: Georgetown University Press.

Hankewitz, Sten. 2020. “The Estonian E-Governance Academy to Help Tonga with Digital Transformation.” Estonian World. December 8, 2020. https://estonianworld.com/technology/the-estonian-e-governance-academy-to-help-tonga-with-digital-transformation/.

Herzog, Stephen. 2017. “Ten Years after the Estonian Cyberattacks: Defense and Adaptation in the Age of Digital Insecurity.” *Georgetown Journal of International Affairs* 18 (3): 67–78. https://doi.org/10.1353/gia.2017.0038.

Hoang, Anh Tuan, Sandro Nižetić, Aykut I. Olcer, Hwai Chyuan Ong, Wei-Hsin Chen, Cheng Tung Chong, Sabu Thomas, Suhaib A. Bandh, and Xuan Phuong Nguyen. 2021. "Impacts of COVID-19 Pandemic on the Global Energy System and the Shift Progress to Renewable Energy: Opportunities, Challenges, and Policy Implications." *Energy Policy* 154 (112322): 112322. https://doi.org/10.1016/j.enpol.2021.112322.

Hysa, Xhimi. 2022. "Critical Case." In *The Sage Encyclopedia of Research Design (2nd Edition)*, edited by Bruce B. Frey, 355–56. Thousand Oaks, CA: Sage.

"Introduction to the Ministry." 2025. Republic of Estonia Ministry of Justice and Digital Affairs. 2025. https://www.justdigi.ee/en/ministry-news-and-contacts/about-ministry-and-minister/introduction-and-structure.

"Iranian State Actors Conduct Cyber Operations against the Government of Albania | CISA." 2022. Cybersecurity and Infrastructure Security Agency CISA. September 23, 2022. https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-264a.

Janowski, Tomasz. 2015. "Digital Government Evolution: From Transformation to Contextualization." *Government Information Quarterly* 32 (3): 221–36. https://doi.org/10.1016/j.giq.2015.07.001.

Jaques, Tony. 2007. "Issue Management and Crisis Management: An Integrated, Non-Linear, Relational Construct." *Public Relations Review* 33 (2): 147–57. https://doi.org/10.1016/j.pubrev.2007.02.001.

Jin, Yan, W.T. Coombs, Yijing Wang, Toni van der Meer, and Brittany N. Shivers. 2024. "'READINESS': A Keystone Concept beyond Organizational Crisis Preparedness and Resilience." *Journal of Contingencies and Crisis Management* 32 (1). https://doi.org/10.1111/1468-5973.12546.

Jones, Charles O. 1976. "Speculative Augmentation in Federal Air Pollution Policy-Making." In *Cases in Public Policy-Making*. New York, N.Y.: Rinehard and Winston.

Kattel, Rainer, and Ines Mergel. 2019. "Estonia's Digital Transformation: Mission Mystique and the Hiding Hand." *Great Policy Successes*, September, 143–60. https://doi.org/10.1093/oso/9780198843719.003.0008.

Kerikmäe, Tanel, David Ramiro Troitiño, and Olga Shumilo. 2019. "An Idol or an Ideal? A Case Study of Estonian E-Governance: Public Perceptions, Myths and Misbeliefs." *Acta Baltica Historiae et Philosophiae Scientiarum* 7 (1): 71–80. https://doi.org/10.11590/abhps.2019.1.05.

Kim, Joe. 2017. "Cyber-Security in Government: Reducing the Risk." *Computer Fraud & Security* 2017 (7): 8–11. https://doi.org/10.1016/s1361-3723(17)30059-3.

King, Nigel, Christine Horrocks, and Joanna Brooks. 2018. *Interviews in Qualitative Research*. Thousand Oaks, CA: Sage.

Kitsing, Meelis. 2018. "The Janus-Faced Approach to Governance: A Mismatch between Public Sector Reforms and Digital Government in Estonia." In *Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance*.

Kotka, Taavi, Carlos Ivan Vargas Alvarez de Castillo, and Kaspar Korjus. 2015. "Estonian E-Residency: Redefining the Nation-State in the Digital Era." *University of Oxford Cyber Studies Programme*. https://www.raulwalter.com/prod/wp-content/uploads/2015/10/Working_Paper_No.3_Kotka_Vargas_Korjus.pdf.

Kriisa, Kristiina. 2025. "Estonia: 100% Digital Government Services." E-Estonia. January 27, 2025. https://e-estonia.com/estonia-100-digital-government-services/.

Lichtman, Marilyn. 2013. *Qualitative Research for the Social Sciences*. Thousand Oaks, CA: Sage.

Littig, Beate. 2009. “Interviewing the Elite – Interviewing Experts: Is There a Difference?” In *Interviewing Experts*, edited by Alexander Bogner, Beate Littig, and Wolfgang Menz, 98–113. Springer.

Madnick, Stuart E. 1978. “Management Policies and Procedures Needed for Effective Computer Security.” *Sloan Management Review (Pre-1986)* 20 (1): 61. https://www.proquest.com/docview/206799278?fromopenview=true&pq-origsite=gscholar&sourcetype=Scholarly%20Journals.

Mäekivi, Ann. 2025. “Ministry of Justice Is Now Ministry of Justice and Digital Affairs.” Republic of Estonia Ministry of Justice and Digital Affairs. 2025. https://www.justdigi.ee/en/news/ministry-justice-now-ministry-justice-and-digital-affairs

Mahoney, James, Khairunnisa Mohamedali, and Christoph Nguyen. 2016. “Causality and Time in Historical Institutionalism.” In *Oxford Handbook of Historical Institutionalism*, edited by Orfeo Fioretos, Tulia G. Falleti, and Adam Sheingate, 71–87. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199662814.013.4.

May, Peter J. 1992. “Policy Learning and Failure.” *Journal of Public Policy* 12 (4): 331–54. https://www.jstor.org/stable/4007550.

Marsden, Greg, and Iain Docherty. 2021. “Mega-Disruptions and Policy Change: Lessons from the Mobility Sector in Response to the Covid-19 Pandemic in the UK.” *Transport Policy* 110 (September): 86–97. https://doi.org/10.1016/j.tranpol.2021.05.015.

Meijer, A. J., Manuel Pedro Rodríguez Bolívar, and J. Ramon Gil-Garcia. “From e-Government to Digital Era Governance and Beyond: Lessons from 15 Years of Research into Information and ommunications Technology in the Public Sector.” *Journal of Public Administration Research and Theory* (2018): 1–6.

Mergel, Ines, Noella Edelmann, and Nathalie Haug. 2019. “Defining Digital Transformation: Results from Expert Interviews.” *Government Information Quarterly* 36 (4): 101385. https://doi.org/10.1016/j.giq.2019.06.002.

Mikwamba, Kingsley, Joost Dessein, Daimon Kambewa, Lies Messely, and Robert Strong. 2020. “Collaborative Governance Dynamics in Innovation Platforms: Case of Malawi’s District Stakeholder Panel.” *The Journal of Agricultural Education and Extension* 27 (2): 255–75. https://doi.org/10.1080/1389224x.2020.1844767.

Mohanta, Ratikant Sadananda. 2017. “Evolution and Shift in Trends of Cyber Crime: An Overview.” *Cyber Times International Journal of Technology & Management* 10 (2): 1–4.

Moyson, Stéphane, Peter Scholten, and Christopher M. Weible. 2017. “Policy Learning and Policy Change: Theorizing Their Relations from Different Perspectives.” *Policy and Society* 36 (2): 161–77. https://doi.org/10.1080/14494035.2017.1331879.

Newman, Janet, Marian Barnes, Helen Sullivan, and Andrew Knops. 2004. “Public Participation and Collaborative Governance.” *Journal of Social Policy* 33 (2): 203–23. https://doi.org/10.1017/s0047279403007499.

OECD. 2023. “2023 OECD Digital Government Index: Results and Key Findings.” *OECD*. https://www.oecd.org/en/publications/2023-oecd-digital-government-index_1a89ed5e-en.html.

Ormston, Rachel , Liz Spencer, Matt Barnard, and Dawn Snape. 2013. “The Foundations of Qualitative Research.” In *A Guide for Social Science Students and Researchers*, edited by Jane Ritchie, Jane Lewis, Carol McNaughton Nicholls, and Rachel Ormston. Thousand Oaks, CA: Sage.

Ostby, Grethe, and Basel Katt. 2019. “Cyber Crisis Management Roles – a Municipality Responsibility Case Study.” In *Proceedings of the 4th International Conference on Information Technology in Disaster Risk Reduction*, 168–81.

Paršovs, Arnis. 2020. “Estonian Electronic Identity Card: Security Flaws in Key Management.” In *Proceedings of the 29th USENIX Security Symposium*.

———. 2020b. “Solving the Estonian ID Card Crisis: The Legal Issues.” In *17th International Conference on Information Systems for Crisis Response and Management*.

Pavel, Tal. 2024. “The Iranian Cyberattacks in Albania: Actors, Tactics, Targets.” *Dot.pl.*, no. I (December): 105–23. https://doi.org/10.60097/dotpl/196772.

Pearson, Christine M., and Judith A. Clair. 1998. “Reframing Crisis Management.” *The Academy of Management Review* 23 (1): 59–76. https://doi.org/10.2307/259099.

Pernice, Ingolf. 2018. “Global Cybersecurity Governance: A Constitutionalist Analysis.” *Global Constitutionalism* 7 (1): 112–41. https://doi.org/10.1017/s2045381718000023.

Pranggono, Bernardi, and Abdullahi Arabo. 2020. “COVID-19 Pandemic Cybersecurity Issues.” *Internet Technology Letters* 4 (2). https://doi.org/10.1002/itl2.247.

Runnel, Pille, Pille Pruulmann-Vengerfeldt, and Kristina Reinsalu. 2009. “The Estonian Tiger Leap from Post-Communism to the Information Society: From Policy to Practice.” *Journal of Baltic Studies* 40 (1): 29–51. https://doi.org/10.1080/01629770902722245.

Schiliro, Francesco. 2023. “Towards a Contemporary Definition of Cybersecurity.” *ArXiv Preprint*, February. https://doi.org/10.48550/arxiv.2302.02274.

Skierka, Isabel. 2023. “When Shutdown Is No Option: Identifying the Notion of the Digital Government Continuity Paradox in Estonia’s EID Crisis.” *Government Information Quarterly* 40 (1): 101781. https://doi.org/10.1016/j.giq.2022.101781.

Solvak, Mihkel, Taavi Unt, Dmitri Rozgonjuk, Andres Võrk, Märten Veskimäe, and Kristjan Vassil. 2019. “E-Governance Diffusion: Population Level E-Service Adoption Rates and Usage Patterns.” *Telematics and Informatics* 36 (March): 39–54. https://doi.org/10.1016/j.tele.2018.11.005.

Solvak, Mihkel, and Kristjan Vassil. 2017. “Could Internet Voting Halt Declining Electoral Turnout? New Evidence That E-Voting Is Habit Forming.” *Policy & Internet* 10 (1): 4–21. https://doi.org/10.1002/poi3.160.

Statista. 2023. “Europe Actions to Improve Digital Technologies 2023.” Statista. 2023. https://www.statista.com/statistics/1479460/europe-actions-to-improve-digital-technologies/.

Stewart, Lauren. 2025. “Exploratory Research | Definition, How to Conduct & Examples.” ATLAS.ti. February 11, 2025. https://atlasti.com/research-hub/exploratory-research#what-is-the-difference-between-exploratory-research-and-descriptive-research.

Strauss, Anselm, and Juliet Corbin. 1998. “Coding for Process.” In *Basics of Qualitative Research*, 163–78. Thousand Oaks, CA: Sage Publications.

Tagarev, Todor. 2020. “Towards the Design of a Collaborative Cybersecurity Networked Organisation: Identification and Prioritisation of Governance Needs and Objectives.” *Future Internet* 12 (4): 62. https://doi.org/10.3390/fi12040062.

Tammpuu, Piia, and Anu Masso. 2018. “‘Welcome to the Virtual State’: Estonian E-Residency and the Digitalised State as a Commodity.” *European Journal of Cultural Studies* 21 (5): 543–60. https://doi.org/10.1177/1367549417751148.

Tasheva, Iva. 2021. “Cybersecurity Post-COVID-19: Lessons Learned and Policy Recommendations.” *European View* 20 (2): 178168582110592. https://doi.org/10.1177/17816858211059250.

Tassabehji, Rana, Ray Hackney, and Aleš Popovič. 2016. “Emergent Digital Era Governance: Enacting the Role of the ‘Institutional Entrepreneur’ in Transformational Change.” *Government Information Quarterly* 33 (2): 223–36. https://doi.org/10.1016/j.giq.2016.04.003.

Tishler, Hace Sorel. 1971. *Self-Reliance and Social Security, 1870–1917*. Port Washington, N.Y.: Kennikat Press.
Toots, Anu, and Mart Laanpere. 2004. "Tiger in Focus – a National Survey of ICT in Estonian Schools." *Educational Media International* 41 (1): 7–18. https://doi.org/10.1080/0952398032000105049.
Truman, David B. 1964. *The Governmental Process*. Praeger.
Turner, Daniel. 2010. "Qualitative Interview Design: A Practical Guide for Novice Investigators." *The Qualitative Report* 15 (3): 754–60. https://doi.org/10.46743/2160-3715/2010.1178.
United Nations. 2022. "The Future of Digital Government: Trends, Insights and Conclusions." *United Nations*. https://desapublications.un.org/sites/default/files/publications/2022-11/Chapter%205.pdf.
United Nations Development Programme. 2023. "Evaluation of the UNDP Support to Digitalization of Public Services." *UNDP*. https://erc.undp.org/evaluation/documents/download/23004.
Urgessa, Worku Gedefa. 2020. "Multilateral Cybersecurity Governance: Divergent Conceptualizations and Its Origin." *Computer Law & Security Review* 36 (April): 105368. https://doi.org/10.1016/j.clsr.2019.105368.
Van Dijk, Teun A. 1997. "What Is Political Discourse Analysis." *Belgian Journal of Linguistics* 11 (1): 11–52.
Vinkel, Priit, and Robert Krimmer. 2016. "The How and Why to Internet Voting: An Attempt to Explain E-Stonia." In *Proceedings of the International Joint Conference on Electronic Voting*, 178–91. Springer.
Von Soest, Christian. 2022. "Why Do We Speak to Experts? Reviving the Strength of the Expert Interview Method." *Perspectives on Politics* 21 (1): 1–11. https://doi.org/10.1017/s1537592722001116.
Von Solms, Basie, and Rossouw Von Solms. 2018. "Cybersecurity and Information Security – What Goes Where?" *Information and Computer Security* 26 (1): 2–9. https://doi.org/10.1108/ics-04-2017-0025.
Warner, Michael. 2012. "Cybersecurity: A Pre-History." *Intelligence and National Security* 27 (5): 781–99. https://doi.org/10.1080/02684527.2012.708530.
Weible, Christopher M., Tanya Heikkila, Peter deLeon, and Paul A. Sabatier. 2011. "Understanding and Influencing the Policy Process." *Policy Sciences* 45 (1): 1–21. https://doi.org/10.1007/s11077-011-9143-5.
Wilson, Carter A. 2000. "Policy Regimes and Policy Change." *Journal of Public Policy* 20 (3): 247–74. https://doi.org/10.2307/4007691.
World Bank. 2022. "Digital Development: Global Practice." *World Bank*. https://thedocs.worldbank.org/en/doc/b16e2ba1cb754ab47a2dd1b214dd374e-0400062023/original/DigitalDevelopmentBrochure.pdf.
Yin, Robert K. 2018. *Case Study Research and Applications: Design and Methods*. 6th ed. Sage Publications.
Zaki, Bishoy Louis, Valérie Pattyn, and Ellen Wayenberg. 2022. "Policy Learning Type Shifts during Creeping Crises: A Storyboard of COVID-19 Driven Learning in Belgium." *European Policy Analysis* 9 (2). https://doi.org/10.1002/epa2.1165.
Zaki, Bishoy Louis, and Ellen Wayenberg. 2023. "Policy Learning and the COVID-19 Crisis: A Systematic Review of Scholarship and Key Lessons for Research and Practice." *Australian Journal of Public Administration* 83 (3). https://doi.org/10.1111/1467-8500.12598.

SUMMARY IN ESTONIAN

Küberjulgeoleku valitsemine Eesti digitaalse valitsemise mudelis, 2007–2023

Doktoritöös uuritakse, kuidas on valitsused rakendanud viimastel aastakümnetel suurenenud digitaliseerimise taustal küberjulgeoleku mehhanisme oma e-valitsemise korralduse kaitsmiseks. Täpsemalt analüüsitakse töös küberjulgeoleku valitsemisprotsesside ja -struktuuride arengut tugevalt digitaliseeritud kontekstis, kasutades Eestit kriitilise juhtumina nende keerukate nähtuste uurimiseks. Töös vaadeldakse, kuidas Eesti valitsemisprotsessid on aastatel 2007–2023 arenenud, analüüsides e-valitsemise ökosüsteemi, selle laienemist ajas ning sellest kõrgelt digitaliseeritud süsteemist tulenevaid julgeolekuvajadusi. Lisaks uuritakse doktoritöös, kuidas neile julgeolekuvajadustele vastamiseks on võimalik kujundada mitmetahuline ja mitme osapoolega küberjulgeoleku valitsemise (*cybersecurity governance*) ökosüsteem, mis hõlmab erinevaid ministeeriume, ametkondi ja muid valitsusasutusi, kelle vastutusalasse kuuluvad küberjulgeoleku valitsemise eri aspektid.

Doktoritöö koosneb kolmest uurimusest. **Uurimus I** on kaardistav juhtumiuuring, mis annab ülevaate Eesti e-valitsemise maastikust, selle ajaloost ja teenuste ulatusest kuni 2020. aasta ning COVID-19 pandeemia alguseni. See uurimus kasutab Eestit e-valitsemise valdkonna kriitilise juhtumina, kus digitaliseerimine saavutas kõrge taseme juba enne COVID-19 pandeemia puhkemist 2020. aastal. Metodoloogiliselt on tegemist dokumendiuuringuga, mis põhineb avalikult kättesaadavatel dokumentidel Eesti e-valitsemise kohta. Info pärineb peamiselt valitsuse veebilehekülgedelt, akadeemilistest ja ekspertkommentaaridest, uudismeediast ning rahvusvahelistest allikatest. Uurimus I oma põhjaliku ülevaatega Eesti digitaliseerimise alustest ja avalike digiteenuste arengust läbi aja võimaldas ka identifitseerida edasised teemad ja hüpoteesid tulevaseks teadustööks, olles seeläbi aluseks järgnevatele teoreetilistele ja analüütilistele käsitlustele uurimuses II ja III.

Uurimuse I tulemuste põhjal võib teha kolm olulist järeldust: esiteks, hoolimata Eesti kõrgest digitaliseerituse tasemest juba enne COVID-19 pandeemia algust, laienes veebipõhiste teenuste pakkumine pandeemia ajal siiski, vastavalt kehtestatud piirangutest tulenevatele vajadustele. Eelkõige võib välja tuua hariduse andmise veebipõhise korralduse ja kinnisvaratehingute notariaalsete toimingute digitaliseerimise. COVID-19 pandeemiaga seotud ühiskondlike protsesside muutused ajendasid innovatsiooni ja uute digitaliseeritud teenuste kasutuselevõttu.

Lisaks rõhutab uurimus I Eesti e-valitsemise globaalset olulisust, kuna riigi tehnoloogiaid ja e-valitsemise praktikaid võetakse üha enam kasutusele erinevates rahvusvahelistes kontekstides. Kuigi mitmed teisedki riigid on käesolevas doktoritöös vaadeldud ajavahemikul asunud täitma e-valitsemise lahenduste üleilmsete eksportijate rolli, on Eesti suutnud tugineda kättesaadavuse, tulemus-

likkuse ja efektiivsuse kombinatsioonile ning läbimõeldud strateegiale ja rahvusvahelisele visioonile, jätkamaks Eesti süsteemi laiendamist nii riigisiseselt kui ka globaalselt. Lõpetuseks võimaldab Eesti e-valitsemise süsteemi põhjalik käsitlus uurimuses I kaudselt tuvastada kogu selle ökosüsteemi potentsiaalsed küberjulgeolekuvajadused, pakkudes lähtekohta nende küberjulgeoleku valitsemise aspektide analüüsiks järgmistes uurimustes.

Uurimus II käsitlebki Eesti küberjulgeoleku valitsemise ökosüsteemi arengut ajas, keskendudes peamiselt valitsemissektori sisestele protsessidele ning analüüsib, miks kujunes konkreetne lähenemine küberjulgeoleku valitsemisele välja just sellisel kujul. Samuti uuritakse mõiste „küberjulgeoleku valitsemine" praktilisi ja institutsionaalseid käsitlusi ning nende käsitluste mõju küberjulgeoleku tegelikule valitsemisele. Uurimus II kasutab koostöise valitsemise (*collaborative governance*) teooriat analüütilise raamistikuna, käsitlemaks poliitikamuutuste (*policy change*) mõistet küberjulgeoleku valitsemisstruktuuride spetsiifilises kontekstis. Koostöise valitsemise teooriale tuginedes rõhutab uurimus II esiteks küberjulgeoleku valitsemisse kaasatud osapoolte paljusust ning teiseks analüüsib Emersoni ja Ahni (2015) kolme keskse koostöise dünaamika olemasolu, mis peaksid iseloomustama koostöise valitsemise juhtumeid: põhimõttekindel kaasatus, jagatud motivatsioon ja ühine tegutsemisvõimekus.

Metodoloogiliselt kasutab uurimus II poolstruktureeritud ekspertintervjuusid, kogumaks Eesti valitsusametnikelt nüansseeritud teavet valitsemisprotsessi ja otsuste tegemiste kohta. Intervjueeritavateks olid Eesti valitsuse otsusetegijad, kes olid otseselt kaasatud küberjulgeoleku valitsemise ökosüsteemi kujundamisel. Intervjuude käigus kogutud teavet trianguleeriti teiste avalikult kättesaadavate valitsusdokumentide ja -sõnumite, kommentaaride ning uudistega, kinnitamaks intervjueeritavate esitatud väiteid.

Uurimuse II peamised järeldused on kahetised. Esiteks tuvastas uurimus, et Eesti küberjulgeoleku valitsemise ökosüsteem kujunes välja 2007. aasta küberrünnakute tulemusel, mille järel määratleti kübejulgeoleku valitsemine poliitikavaldkonnana, mis nõuab asjakohaseid institutsionaalsed struktuure ja reageerimisvõimekust. Selle tulemusel nihkus küberjulgeoleku valitsemisstruktuur Kaitseministeeriumi vastutusalast tsiviilpädevusena Majandus- ja Kommunikatsiooniministeeriumile. See muutus tugevdas ka Riigi Infosüsteemi Ameti (RIA) ning selle küberintsidentide käsitlemise osakonna CERTi rolli, mida peetakse valitsemissektori kõige arenenuma tehnilise pädevuse kandjateks. Kõnealune küberjulgeoleku valitsemise ökosüsteem kujundati Eesti kõrget digitaliseerituse taset silmas pidades, kuna selle struktuuri juhtivad institutsioonid olid traditsiooniliselt hoidnud digitaliseerimisega seotud tegevuse eesmärgil kõige tugevamaid suhteid erasektoriga.

Teiseks leidis uurimus II, et mõiste „küberjulgeoleku valitsemine" ei ole Eesti valitsuses formaalselt kodifitseeritud, vaid pigem määratletud mitteametliku konsensuse kaudu, mis põhineb küberjulgeoleku valitsemisse kaasatud sidusrühmade jagatud normidel ja väärtustel. Kuigi mõnikord esines mõiste „küberjulgeoleku valitsemine" tõlgenduste tõttu pingeid, tulenesid need enamasti väikestest ebaselgustest rollijaotuses või erinevustest juhtimisstiilides ning neid oli kerge

lahendada. Taolised näited illustreerisid Emersoni ja Ahni (2015) koostöise dünaamika toimimist, näidates põhimõttekindlat kaasatust, jagatud motivatsiooni ja ühist tegutsemisvõimekust Eesti küberjulgeoleku valitsemise ökosüsteemi kujundamisel ning järjepidevust riigi digiteenuste turvalisuse tagamise eesmärgis.

Uurimus III käsitleb küberjulgeolekukriise, mis on mõjutanud e-valitsemise teenuseid, püüdes selgitada, kuidas tehakse kriisijärgseid otsuseid: milliseid võimalusi kaalutakse, milliseid valikuid tehakse, tugevdamaks küberjulgeolekut tulevikus. Uurimus analüüsib nelja olulist küberjulgeolekukriisi, mis on mõjutanud Eesti e-valitsemise ökosüsteemi: (1) 2007. aasta DDoS-küberrünnakud, mis järgnesid pronkssõduri kriisile Tallinnas, (2) 2017. aasta „eID kriis", mille käigus tuvastati haavatavused ligikaudu 800 000 Eesti ID-kaardis, (3) COVID-19 pandeemia, mis tõi kaasa uusi küberjulgeolekualaseid väljakutseid seoses inimestevahelise suhtluse üleminekuga veebikeskkonda; ning (4) Venemaa täiemahuline sissetung Ukrainasse 2022. aastal, mille käigus Ukraina liitlased – sealhulgas Eesti – pidid toime tulema poliitiliselt motiveeritud küberrünnakutega. Uurimus III kasutab ajaloolise institutsionalismi raamistikku, käsitledes neid küberjulgeolekriise kriitiliste pöördepunktidena ning jälgides Eesti valitsusasutuste rajasõltuvust nendes juhtumites, et teha järeldusi kriisijärgse otsustusprotsessi toimimise kohta.

Metodoloogiliselt kasutati uurimuses III sarnast lähenemist nagu uurimuses II: nendes kriisiolukordades otsuste tegemiste eest vastutavate isikutega viidi läbi poolstruktureeritud ekspertintervjuud, et saada ülevaade vastavatest otsustusprotsessidest. Sarnaselt uurimus II-ga võrreldi intervjuudest saadud teavet selle kinnitamiseks avalikult kättesaadava teabega. Analüüsitud nelja kriisi järgsete otsustusprotsesside kohta võib välja tuua kolm peamist järeldust. Esiteks, õppimine varasematest kriisidest, suunamaks otsuste tegemist tulevaste kriiside korral, mille tulemusel kujunesid aja jooksul välja küberjulgeoleku valitsemise rajasõltuvused. Teine keskne järeldus oli, et Eesti valitsus on küberjulgeolekukriiside käsitlemisel seadnud prioriteediks selge ja läbipaistva kommunikatsioonistrateegia, eeskätt küberjulgeolekuga seotud teabe esitamisel laiemale avalikkusele. Kolmandas näitas valitsuse reageerimine nendele kriisidele, kui oluline on jätkata innovatsiooni küberjulgeoleku valdkonnas ka kriisivälisel ajal, kuna kriisid ise kiirendasid sageli juba arutlusel olnud poliitiliste ideede või algatuste elluviimist.

Nende uurimuste lõikes ilmneb mitmeid ühiseid teemasid ja järeldusi, mis on seotud digitaliseerimise, küberjulgeoleku valitsemise ning nii kriisi- kui tavaolukordadega. Kui uurimus I tõstis esile Eesti küpse ja laiapõhjalise e-valitsemise maastiku, luues aluse sellega kaasnevatele küberjulgeolekuvajadustele, siis uurimused II ja III arendasid seda käsitlust edasi, analüüsides, kuidas küberjulgeoleku valitsemise ökosüsteem kujuneb ning kuidas suudab selline süsteem reageerida küberjulgeolekukriisidele. Need uuringud rõhutavad üldist arusaama, et innovatsioon ja pidev täiustamine küberjulgeoleku valdkonnas on järjepidev ning pidevalt arenev protsess. Küberjulgeoleku valitsemise ökosüsteemides peab valitsema valmisolek ja kohanemisvõime muutuvate olude ja küberohtude kontekstis.

Sellised protsessid on nüansirohkem ja harva lineaarsed; pigem peegeldavad need konkreetse aja ja koha tingimusi.

Laiemas plaanis on need uurimused näidanud, et küpses ja ulatuslikult digitaliseeritud kontekstis on küberjulgeolekuvajadused suuremad, tulenevalt küberohtude kõrgemast esinemise tõenäosusest sellises digitaalses keskkonnas. Seetõttu on vaja kujundada asjakohane küberjulgeoleku valitsemise ökosüsteem, mis peegeldab nii küberjulgeoleku vajadusi kui ka kohaliku keskkonna spetsiifilist konteksti – olgu need seotud valitsemise, julgeoleku, kultuuriliste, või muude aspektidega. Kuigi sellised algatused parandavad üldjuhul küberjulgeolekualast valmisolekut, ei ole neil võimalik ette näha kõiki potentsiaalseid kriise, mis võivad tulevikus esile kerkida, ega nende eest kaitsta. Seetõttu on vajalik, et küberjulgeoleku valitsemise ökosüsteemis oleksid ette nähtud meetmed kriisidega toimetulekuks: tehnilised, poliitilised ning kommunikatsiooniga seotud kaalutlused.

Käesolev doktoritöö annab panuse kasvavasse küberjulgeoleku ja e-valitsemise alasesse teaduskirjandusse, kasutades Eestit kui küpset kriitilist juhtumit uurimaks, kuidas küberjulgeoleku valitsemisstruktuurid ja -protsessid võivad areneda vastusena küberjulgeoleku tegelikkusele. Teoreetiliselt pakub töö uut teadmist, laiendades küberjulgeoleku uurimisvaldkonda koostöise valitsemise (uurimus II) ja ajaloolise institutsionalismi (uurimus II) teoreetilistele lähenemistele ning rakendades poliitikamuutuse (uurimus II) ja kriisihalduse (uurimus III) kontseptuaalseid raamistikke. Praktilisemas plaanis pakub doktoritöö Eesti küpse juhtumi põhjal järeldusi ja õppetunde, mida on võimalik kohandada ka teises riikides, kus esinevad sarnased küberjulgeolekualased väljakutsed. Olulisemal laiemalt kui pelgalt Eesti kontekstis on küberjulgeoleku valitsemisel suur väärtus pideval õppimisel, innovatsioonil, koostööl ja valmisolekul.

Doktoritöös käsitletud periood, mis hõlmab aastaid 2007–2023, on olnud küberjulgeoleku valdkonnas märkimisväärsete muutuste aeg, tuues kaasa näiteks uued ohuallikad ja ründevektorid, aga ka valitsuste reageerimisviisid. Kahtlemata jätkab küberjulgeoleku maastik kiiret arengut ka tulevikus. Seetõttu on praktilisest vaatenurgast üha olulisem uurida, kuidas on üha digitaliseeritumates kontekstides võimalik valitsemisstruktuure kujundada ja pidevalt kohandada, tagamaks digitaliseeritud teenuste ja süsteemide turvalisus.

PUBLICATIONS

APPENDIX A: INTERVIEW QUESTIONNAIRE

Section 1: Introductory Questions

1. Can you please briefly explain your current role?
2. What motivated to you to study/research/work in the field of cybersecurity/ e-governance? How long have you been in this field?

Section 2: Understanding of Cybersecurity Governance

1. How do you define the governance of cybersecurity/ cybersecurity governance?
2. How does your organisation/department define cybersecurity governance? Is this a spoken understanding or is this codified? Has this evolved over time?
3. Does your organisation/department's definition of cybersecurity governance vary from others inside Estonia? If so, what practical difficulties arise from these different understandings? Can you give examples?
4. If yes to previous question, how could gaps in understandings be bridged so that these difficulties could be mitigated?

Section 3: Cybersecurity Governance and the 2007 Cyberattacks

1. What was your role at the time of the 2007 cyberattacks? How were you involved in governance/decision-making at this time?
2. Can you describe governance initiatives that took place in the aftermath of the 2007 cyberattacks that led to improvements to overall Estonian cybersecurity, and more specifically, to its e-governance?
3. Were there other alternative decisions that were considered during this process? Why were the decisions that were made undertaken instead of these?
4. To what extent did the 2007 cyberattacks and their aftermath shape what has been called Estonia's role as an international 'norm-setter' in cybersecurity, or the role of cybersecurity in Estonia's foreign policy? Can you provide examples? 5. How were the 2007 cyberattacks perceived by actors outside of government during that time (ie. opposition, interest groups, citizens, businesses, etc.)?

Section 4: Cybersecurity Governance and the 2017 e-ID Crisis

1. What was your role at the time of the 2017 e-ID crisis? How were you involved in governance/decision-making at this time?
2. What decision-making was undertaken to make the government announcements surrounding the ID-card vulnerability when it did? To what extent was this impacted by the upcoming local elections using i-voting, and timelines associated with those elections?
3. Were other courses of action considered during this process? Why were the decisions that were made undertaken instead of the alternatives? Was the government concerned about exploitation of the vulnerability before the patch was applied, or public trust concerns when they made these decisions?

4. Does the governance response to the e-ID crisis offer a road map to future cybersecurity 'crises' or exogenous shock events, given that the event was resolved without major cybersecurity event or exploitation? Could anything have been done better?

Section 5: Cybersecurity Governance and the COVID-19 Pandemic

*Note: to a certain extent, the COVID-19 pandemic remains ongoing, but this refers to the new realities, including cybersecurity realities and the move online during lockdowns, that emerged in the earlier stages of the pandemic

1. What was your role at the onset of the COVID-19? How were you involved in governance/decision-making at this time?
2. A great deal of literature and cybersecurity reporting indicates that the onset of the COVID-19 pandemic saw sizable increases in cyberattacks globally; to what extent did the onset of the pandemic have an impact on cybersecurity, particularly surrounding e-governance in Estonia?
3. What cybersecurity governance measures were taken in the early days of the pandemic to ensure that changing global cybersecurity realities were mitigated in Estonia?
4. At the onset of the pandemic, Estonia already had very pervasive e-governance in place, so with a move away from in-person interactions with lockdowns imposed, the learning curve was less steep than elsewhere globally. However, some new digitalised government provisions were still necessary (such as fully online learning, expansion of e-services like real estate transactions); what decisions were undertaken to bolster the cybersecurity of these new provisions?

Section 6: Cybersecurity Governance and the Russian Invasion of Ukraine

1. What was your role at the time of the Russian invasion of Ukraine in February 2022, and do you remain in this role? How were/are you involved in governance/decision-making during this time?
2. Can you explain the ways in which Russia's invasion of Ukraine has impacted cybersecurity realities in Estonia? Specifically, how has this impacted the cybersecurity of Estonian e-governance?
3. What decision making related to cybersecurity governance has been undertaken since the start of the war to bolster the cybersecurity of Estonian e-governance? How successful have these mechanisms been? Could they offer a road map to future cybersecurity external shock factors?
4. In August 2022, the largest DDoS attacks since the 2007 cyberattacks, which were successfully repelled, received significant media attention; to what extent did decision-making both pre-dating and since the start of Russia's invasion contribute to this outcome?

Section 7: Additional Questions

1. Are there other critical junctures/external shock events that should be considered, in which Estonian cybersecurity governance related to its e-governance was tested? What was the response and did it bolster the overall cybersecurity of Estonian e-governance?
2. Who else should I speak to?

CURRICULUM VITAE

Name: Logan Carmichael
Date of birth: 6 September 1995
Email: loganecarmichael@gmail.com

Education:

2021–2026	University of Tartu, PhD Political Science
2018–2019	University of Auckland, MCTS Conflict and Terrorism Studies
2013–2017	University of Windsor, BA[Honours] Political Science

Relevant Work Experience:

2025–	Cybernetica AS, e-Governance Sales Specialist
2021–2025	University of Tartu, Junior Research Fellow in e-Governance
2024–2025	NATO Cooperative Cyber Defence Centre of Excellence, Visiting Scholar
2021	ASB Bank (Auckland, New Zealand), Cybersecurity Analyst

Participation in Research Projects:

2021–2025	ERA Chair of e-Governance and Digital Public Services (ECePS)

Publications:

Carmichael, Logan (2025). "Crafting a Cybersecurity Governance Ecosystem: Two Decades of Learning in Estonia," *European Policy Analysis*. https://doi.org/10.1002/epa2.70017

Carmichael, Logan (2025). "Lessons from Small and Highly-Digitalised Estonia: Decision-Making in the Aftermath of Cybersecurity Crises," *Internet Policy Review,* 14(3). https://doi.org/10.14763/2025.3.2028

Khutkyy, Dmytro and Logan Carmichael (2024). "Open Government Policy making by Popular Voting: Comparing Canada and New Zealand," *Journal of Public and Non-Profit Affairs,* https://doi.org/10.20899/jpna.sk21ph17

Carmichael, Logan and Bogdan Romanov (2022). "Domestic Decision-Making, Regional Linkages, and Cybersecurity Considerations: Implementation of Internet Voting in Russia, September 2021," *Proceedings of the Seventh International Joint Conference on Electronic Voting (E-Vote-ID).*

Carmichael, Logan (2021). "Exploring Estonian e-Government Before, During, and Beyond COVID-19," *New Zealand Journal of Research on Europe.*

ELULOOKIRJELDUS

Nimi: Logan Carmichael
Sünniaeg: 6 September 1995
E-post: loganecarmichael@gmail.com

Hariduskäik:

2021–2026	Tartu Ülikool, PhD Politoloogia
2018–2019	Aucklandi Ülikool, MCTS Konflikti- ja terrorismiuuringud
2013–2017	Windsori Ülikool, BA [Kiitusega] Riigiteadused

Töökogemus:

2025–	Cybernetica AS, e-valitsuse müügispetsialist
2021–2025	Tartu Ülikool, e-valitsuse nooremteadur
2024–2025	NATO Kooperatiivse Küberkaitse Kompetentsikeskus, külalisteadlane
2021	ASB Pank (Auckland, Uus Meremaa), küberturbe analüütik

Teadusprojektides osalemine:

2021–2025	ERA Chair e-valitsemise ja digitaalsete avalike teenuste valdkonnas (ECePS)

Publikatsioonid:

Carmichael, Logan (2025). "Crafting a Cybersecurity Governance Ecosystem: Two Decades of Learning in Estonia," *European Policy Analysis*. https://doi.org/10.1002/epa2.70017

Carmichael, Logan (2025). "Lessons from Small and Highly-Digitalised Estonia: Decision-Making in the Aftermath of Cybersecurity Crises," *Internet Policy Review,* 14(3). https://doi.org/10.14763/2025.3.2028

Khutkyy, Dmytro and Logan Carmichael (2024). "Open Government Policy making by Popular Voting: Comparing Canada and New Zealand," *Journal of Public and Non-Profit Affairs,* https://doi.org/10.20899/jpna.sk21ph17

Carmichael, Logan and Bogdan Romanov (2022). "Domestic Decision-Making, Regional Linkages, and Cybersecurity Considerations: Implementation of Internet Voting in Russia, September 2021," *Proceedings of the Seventh International Joint Conference on Electronic Voting (E-Vote-ID).*

Carmichael, Logan (2021). "Exploring Estonian e-Government Before, During, and Beyond COVID-19," *New Zealand Journal of Research on Europe.*

DISSERTATIONES RERUM POLITICARUM UNIVERSITATIS TARTUENSIS

1. **Allan Sikk.** Highways to power: new party success in three young democracies. Tartu, 2006.
2. **Holger Mölder.** Cooperative security dilemma – practicing the hobbesian security culture in the Kantian security environment. Tartu, 2010.
3. **Heiko Pääbo.** Potential of Collective Memory Based International Identity Conflicts in Post-Imperial Space. Tartu, 2011.
4. **Mihkel Solvak.** Private member's bills in parliament – a comparative study of Finland and Estonia. Tartu, 2011, 217 p.
5. **Viljar Veebel.** The role and impact of positive conditionality in the EU pre-accession policy. Tartu, 2012, 230 p.
6. **Alar Kilp.** Church authority in society, culture and politics after Communism. Tartu, 2012, 177 p.
7. **Maria Groeneveld.** The role of the state and society relationship in the foreign policy making process. Tartu, 2012, 193 p.
8. **Mari-Liis Sööt.** Explaining Corruption: Opportunities for Corruption and Institutional Trust. Tartu, 2013, 120 p.
9. **Kadri Lühiste.** Regime Support in European Democracies. Tartu, 2013, 124 p.
10. **Raul Toomla.** De facto states in the international system: Conditions for (in-)formal engagement. Tartu, 2013, 209 p.
11. **Andro Kitus.** A Post-Structuralist Concept of Legitimacy. A thesis in partial fulfilment of the requirements for the degree of Doctor of Philosophy. Tartu, 2014, 189 p.
12. **Kristian Lau Nielsen.** Soft Power Europe: The Lesser Contradiction in Terms and Practices. Tartu, 2016, 156 p.
13. **Birgit Poopuu.** Acting is everything: the European Union and the process of becoming a peacebuilder. Tartu, 2016, 242 p.
14. **Kristina Kallas.** Revisiting the triadic nexus: An analysis of the ethno-political interplay between Estonia, Russia and Estonian Russians. Tartu, 2016, 152 p.
15. **Liisa Talving.** Economic conditions and incumbent support: when and how does the economy matter? Tartu, 2016, 166 p.
16. **Ryhor Nizhnikau.** Externally Induced Institutional Change in the EU's Eastern Neighbourhood: Migration and Environment Reforms in Ukraine and Moldova in 2010–2015. Tartu 2017, 218 p.
17. **Kats Kivistik.** Relevance, Content and Effects of Left-Right Identification in Countries with Different Regime Trajectories. Tartu 2017, 204 p.
18. **Lukas Pukelis.** Informal mutual oversight mechanisms in coalition governments: Insights from the Baltic states for theory building. Tartu 2018, 145 p.
19. **Shota Kakabadze.** "The Caucasian Chalk Circle": Georgia's Self at the East/West Nexus. Tartu 2020, 186 p.

20. **Maksim Kulaev.** Trade unions, transformism and the survival of Russian authoritarianism. Tartu 2020, 151 p.
21. **Juhan Saharov.** From Economic Independence to Political Sovereignty: Inventing "Self-Management" in the Estonian SSR. Tartu 2021, 161 p.
22. **Andrii Nekoliak.** 'Memory Laws' and the Patterns of Collective Memory Regulation in Poland and Ukraine in 1989–2020: A Comparative Analysis. Tartu 2022, 263 p.
23. **Ivan Ulises Kentros Klyszcz.** How Does Violent Conflict Affect Paradiplomacy? An Exploratory Research with Cases from the North Caucasus. Tartu 2022, 200 p.
24. **Lelde Luik.** Re-evaluating the Role of Representative Institutions in Radical Democratic Theory: Lessons from Democratic Identity Construction in Latvia. Tartu 2023, 149 p.
25. **Ionut Chiruta.** Triadic Nexus Relationships in an Age of Populism: Interactions between Hungary, Romania and the Hungarian Minority in Szeklerland. Tartu 2023, 201 p.
26. **Sanshiro Hosaka.** Nothing but Politics? Explaining the Reproduction of Russian Narratives About the Events in Ukraine Among Japanese Scholars and Intellectuals 2014–2019. Tartu 2025, 224 p.
27. **Eoin Micheál McNamara.** The Risk Society's Stabilisation Failure? An Analysis of NATO and the International Security Assistance Force in Afghanistan. Tartu 2025, 370 p.
28. **Butrint Berisha.** Exploring the Role of Civil Society Organisations (CSOs) in Foreign Relations of De Facto States: A Comparative Analysis of Kosovo, Palestine and Taiwan. Tartu 2025, 236 p.
29. **George Spencer Terry.** Demanding Subjectivity: The Radical Right's Use of Discursively Empty Referent Objects within a Post-Foundational Logics Framework. Tartu 2025, 139 p.
30. **Michael Cole.** The People, the Elites and the Russia Factor: A Comparative Study of Populist Discourses in Georgia and Ukraine. Tartu 2025, 242 p.