



Securing e-Estonia: Challenges, Insecurities, Opportunities

Thesis submitted for the degree of
Doctor of Philosophy
At Royal Holloway, University of London

by

Alexander Hardy
Departments of Geography and Information Security
Royal Holloway, University of London

September 2019

Corrections 2021

Declaration of Authorship

I, Alexander Hardy, hereby declare that this thesis and the work presented in it is entirely my own. The work of others is clearly cited, where appropriate.

Signed

A handwritten signature in black ink, appearing to read 'Alexander Hardy', written over a faint, large, light-colored oval shape.

Date

11.11.2021

Acknowledgements

Firstly, I would like to thank the supervisory team involved in this project for their guidance, tireless feedback, and support over the past 4 years. It has been a supremely challenging project, and would not have been possible without the guidance of both Professor Klaus Dodds and Professor Lizzie Coles-Kemp for their endless patience and advice. Furthermore, my extreme gratitude to Professor Eiki Berg, who joined the supervisory team during my time spent at the University of Tartu, whose support since January 2018 has been constant and invaluable. I also extend my thanks to Leverhulme as well as DORA for funding this project.

I would further like to acknowledge the contributions of Dr. Geraint Price and Dr. Al Pinkerton, for their advice and guidance through the upgrade stages of the project. Their helpful comments helped to shape the direction of the research. I would further extend my extreme gratitude to all in the relevant departments at both Royal Holloway and Tartu University. I have not only found both environments stimulating and challenging but within them have also made friends for life. I thank all participants in this research for their stimulating discussions and feedback. Needless to say, the research would not exist without their generosity of time and contributions.

Last, but certainly not least, I extend my thanks to my family and friends for their support throughout this thesis, and my life, in general, these past few years. In particular, to my long-suffering parents, who will no doubt be enthused I can get a 'real job' now. I also thank my Grandfather for his persistence in asking how 'that University thing' is going. I extend particular gratitude to Carla for her patience, endless support, and for putting up with me. To my friends, particularly those at both Royal Holloway and the University of Tartu, as well as the many colleagues from other Universities I met along the way, I extend my heartfelt gratitude. Nick, Andreas, Pip, Simon, Nicola, Sabina, Vevila, Andrew, Kristel, Heidi, Eoin, Maili, Louis... and more. I am sure we will be friends far beyond academia. Without all of the above, this thesis could never have happened. Not to mention my friends outside of academia, who are consistently baffled by my endless travels in Eastern Europe but supportive nevertheless. A thank you to all. Finally, I also dedicate the thesis to my late Grandmother, who sadly did not see me complete the project.

Thesis Abstract

Estonia, as a nation, has progressed considerably since the resumption of independence in 1991. A national embrace of digital technology has been integral to the modernisation of the state in the Post-Soviet era. This embrace of technology has driven digital innovation and has led to the moniker e-Estonia being utilised by both the international media and the Estonian government. Estonia is also notable for its pioneering work towards the establishment of norms in cyber security and excellence in e-governance, and existing research has noted that Estonia's impact in these fields far exceeds that of most small nations (Crandall, 2014; Wrangé & Bengtsson, 2019; Adamson, 2019). Yet Estonia's rapid digitalisation of public and private life holds many contemporary security challenges. Those challenges are felt socially, politically, and technically in professional spaces and across wider Estonian society, where social and technical issues intersect. Estonia claims to be a 'digital society' with over 99% of public services available online (e-Estonia, 2019). Yet it is also arguably a digitally dependent society.

This thesis interrogates a top-down and a bottom-up perspective of e-Estonia 'the digital society' by exploring governmental geopolitics and the role of individual professional's personal cyber security concerns, and the overlap between the two. This analysis of e-Estonia is the culmination of a research project which involved nearly two years of living and working in Estonia. Methodologically, the thesis utilises interviews with high-ranking digital professionals drawn from the cyber security community working in the Estonian public and private sectors. The conclusions of the thesis are drawn from these interviews alongside ethnographic observations and critical engagement with supporting geopolitical and security literature.

The purpose of the thesis is to demonstrate the diversity of challenges and insecurities that the ubiquitous digitalisation of society has posed to Estonia and its citizens. Conversely, the thesis also explores the opportunities this digitalisation has brought about. This thesis considers the relationship between Estonian citizens and the state, the geopolitical nature of contemporary cyber security relations and how Estonia uses its international recognition as a digital pioneer to expand its influence internationally. It highlights the challenges, the insecurities, and the opportunities of Estonia's particular approaches to cyber security and ubiquitous e-governance. The thesis extrapolates wider lessons from these experiences and discusses their applicability in Estonia and beyond.

Securing e-Estonia: Challenges, Insecurities, Opportunities: Contents

1. Introduction	9
1.1 What is e-Estonia?	9
1.2 Doing Interdisciplinary Research and How This Thesis Happened	11
1.3 Thesis Structure Overview	13
2. Securing e-Estonia: Geopolitics, History, & Trust	19
2.1 Introduction	19
2.2 Estonia's Geopolitics, Geopolitical Narratives, and Why They Matter	19
2.3 What Shapes Threat Perception? Estonia and Beyond	21
2.4 Why do Everyday Geopolitics Matter to our Understanding of e-Estonia?	25
2.5 e-Estonia', Nation Branding, and Identity	26
2.6 Russia & the Baltic States: Clashing Identities & Contested Memories	29
2.7 Estonia's Small State (in)Security	31
2.8 Development, Dependency and Trust	34
2.9 Conclusions	37
3. Cyber Insecurities, Ubiquitous Connectivity & the Sociotechnical	39
3.1 Introduction	39
3.2 Security and the Sociotechnical	39
3.3 Studying security: Varied Approaches	41
3.4 Cyber security, Sociotechnical Interactions, and the Everyday	46
3.5 Critical Approaches to Cyber security	49
3.6 Ubiquitous Connectivity: The Proliferation of Connected Devices	52
3.7 Insecurity, Sociotechnical Interactions, and Political Implications	54
3.8 Cyber Insecurities, Sociotechnical Interactions	56
3.9 Conclusions	58
4. Research Design and Methodology	59
4.1 Introduction	59
4.2 Research Questions	60
4.3 Methods and Methodology	61
4.4 Interview Structure & Questions	64
4.5 Conducting Interviews with Digital Professionals: Sampling & Ethics	66
4.6 Utilising MAXQDA for Qualitative Analysis	70

4.7 Ontological and Theoretical Approaches to Qualitative Analysis	71
4.8 Thesis Anonymisation Guide	74
4.9 Methodological Reflections and Conclusions	79
5. e-Estonia & Post-Soviet Estonia: Contemporary Challenges	81
5.1 Introduction	81
5.2 Contemporary Estonian Politics	81
5.3 e-Estonia's Digital Professionals, the State, and Independence	83
5.4 Post-Soviet Estonia	85
5.5 How Digital Professionals Understand Cyber Security in Estonia Today	89
5.6 Performing e-Estonia	94
5.7 Connected Devices and Everyday Life in Estonia	97
5.8 A Tale of Two Estonias? e-Estonia and Post-Soviet Estonia	99
5.9 Conclusions	102
6. Estonia's Cyber Insecurities: Geopolitics & Russian Influence	104
6.1 Introduction	104
6.2 Estonia & e-Estonia's Geopolitical Insecurities	105
6.3 e-Estonia's Smart Devices	109
6.4 Why e-Estonia's Devices Matter	112
6.5 Managing Risk in e-Estonia	115
6.6 Geopolitical Anxiety, Insecurity, and Estonia's Nativist Trust	116
6.7 Disinformation	118
6.8 Everyday Cyber Geopolitics and Russia	122
6.9 Insecurities and Challenges	127
6.10 Conclusion	128
7. Estonia's Emerging e-Nordic Strategy: Opportunities	129
7.1 Introduction	129
7.2 What is e-Nordic?	130
7.3 What is the X-Road and How does it Work?	132
7.4 Who is Adopting X-Road and How the e-Nordic Vision Might Work	136
7.5 e-Estonia Beyond Estonian Borders	140
7.6 Why Develop Integrated, Cross-border e-Governance?	142
7.7 Challenges	146
7.8 Conclusion	147
8. Conclusion	148
8.1 Introduction	148

8.2 Unique Contributions & Developments from Existing Research	148
8.3 Cyber (in)Security and the Everyday	151
8.4 e-Estonia and the Challenges of Securing a Small State	154
8.5 Trust	154
8.6 Sociotechnical Relations and Ubiquitous e-governance	155
8.7 Methodological Reflections	156
8.8 Implications	157
8.9 Summary	158
8.10 Future research agendas	158
Annex	160
Interview Questions	160
Coding	162
Interview Transcripts	164
Participant A - 01.02.2019	164
Participant B - 08.03.18	169
Participant C - 14.2.18	178
Participant D - 20.3.2018	183
Participants E & F - 06.04.2018	189
Participant G - 09.4.2018	195
Participant H - 03.04.2018	201
Participant I - 23.09.2019	208
Participant J - 29.02.2019	212
Participant K - 27.03.2018	216
Participant L - 31.10.2017	222
Participant M - 07.03.2018	225
Participant N - 26.02.2019	229
Participant O - 06.02.2019	232
Participant P - 11.04.2018	235
Participant Q - 10.04.2018	240
Participants R & S - 01.03.2018	247
Participant T - 27.02.2019	258
Bibliography	262

List of Figures

Figure 1. - Mapping the history of the e-State	21
Figure 2. - e-Estonia showroom	27
Figure 3. - Key Interview Questions and Research Questions	64
Figure 4. - Ethics approval form	69
Figure 5. - X-Road ecosystem diagram	134
Figure 6. - X-Road integration diagram	138
Figure 7. - MAXQDA word map	162
Figure 8. - MAXQDA code relations browser	162
Figure 9. - MAXQBA code map	163
Figure 10. - Coding Visualisation Distribution	163
Figure 11. - Coding Visualisation Frequency	163

1. Introduction

1.1 What is e-Estonia?

“Could Estonia be the first ‘digital’ country?”

(*BBC News*, 2017)

“Estonians embrace life in a digital world”

(*New York Times*, Scott, 2014)

“Welcome to E-stonia, the world’s most digitally advanced society”

(*Wired Magazine*, Reynolds, 2016)

e-Estonia, as illustrated in the far from exhaustive quotations above, has become a popular media phenomenon in recent years. Through intensive self-promotion, leading Estonian politicians and institutions as well as notable international news outlets have promoted an image of Estonia as a world-leading, tech-savvy nation. In particular, Estonia self-publicises itself as being top of the national cyber security index (*e-Estonia*, 2018b), and the European Union itself has appointed an Estonian, Juhan Lepassaar, as director of Cyber security (ERR, 2019a). Media outlets in the western world have repeatedly hailed the innovation of e-Estonia as a model for the rest of the world. This thesis critically assesses whether this is the case, or conversely if Estonia is not quite the digital pioneer such reports suggest. In order to make this assessment, this thesis undertakes a critical, sociotechnical analysis of the different ways that matters of cyber security and e-governance influence contemporary Estonian society.

At this juncture, it is vital to establish what e-Estonia is and why it is worthy of such sociotechnical research. e-Estonia (occasionally E-stonia, depending on the author or outlet) might be succinctly summarised as the digital ecosystem of Estonia – the government-led interconnected systems of e-governance and the devices that interact with it (Vassil, 2015 & 2016; Krivý, 2021). e-Estonia is also a vision promoted by the Estonian government to outsiders – such as the e-Estonia website which proudly claims:

“We have built a digital society and we can show you how.”

(*e-Estonia*, 2019)

Of course, many modern societies can claim to be digital but for Estonia its digital prowess seems central to its national identity. In the further words of the Estonian government:

“e-Estonia offers more transparency and less bureaucracy! Estonia has built an efficient, secure and transparent ecosystem where 99% of governmental services are online”

(*e-Estonia*, 2021)

e-Estonia is often interpreted as referring to Estonia's extensive e-governance services – Estonia's digital ecosystem as outlined above (Vassil 2015 & 2016; Krivý, 2021). e-Estonia promotional material often suggests Estonia's digital ecosystem is 'world-leading' (in line with some of the opening quotations from foreign media outlets that opened this chapter). Likewise, successive Estonian Presidents and Prime Ministers have been keen to promote this perspective of Estonia to the rest of the world:

"Estonia has shown the path to successful e-Government"

(President Kersti Kaljulaid, 14.09.2019 cited in Talant, 2019)

However, e-Estonia is not limited to e-service provision alone. Estonia's 'digital society' is also notable for the Estonian Defence League Cyber Unit. The wider Defence League ('Kaitseliit' in Estonian) is a volunteer force of reservists charged with the military defence of the nation should its territorial integrity be threatened. The Defence League's Cyber Unit ('Küberkaitseliit' in Estonian) is comprised of those who work in the private sector for the nation's tech firms and volunteer their spare time to contribute to the defence of the digital nation (Cardash et al, 2013). Much like Estonia's ubiquitous e-governance, the Cyber Defence Unit has won international admiration (Blair, 2015 & *Wired* 2018).

Additionally, Estonia's 'e-residency' programme has also won international acclaim. This programme allows foreigners limited access to Estonian e-services through a state-issued digital identity. Non-Estonian residents who choose to become e-residents can consequently access Estonia's online business and tax systems as well as receive access to a digital identity. However, e-Residency does not provide any right to residency and has been critiqued as a 'shallow' form of nation branding creating the impression of a transnational, global Estonia (see Tampuu & Masso, 2018). Nevertheless, e-residency has been heavily promoted, including through PR exercises handing out complimentary e-residency permits to famous officials such as Japanese Prime Minister Shinzō Abe and notable British journalist Edward Lucas – arguably as part of a digital soft power strategy (Särav & Kermimäe, 2016 & Blue, 2020). Others have critiqued e-Estonia however. Kattel (2020) suggests that the international success of e-Estonia is a 'white lie'; the product of a 'narrow ideology'; and that the power of e-Estonia is overstated for a foreign audience which serves to mask Estonia's domestic problems.

Another aspect of e-Estonia which is of growing notoriety is the data embassy initiative. This initiative involves establishing server resources outside the nation's borders to ensure 'the digital continuity of the state' (Robinson & Martin, 2017). Essentially, backing up the data of the nation on hard files in an allied nation-state. This, Robinson & Martin also argue, is the latest instalment of reimagining the Estonian nation as e-Estonia, an initiative they suggest extends to e-residency, e-ID, e-health services, i-voting, and beyond, and forms part of a strategy to present the e-Estonia brand to the world.

It has also been suggested that e-Estonia is now intimately tied to modern Estonian citizenship and what it means to be Estonian in the 21st century (Björklund, 2016). Furthermore, security is at the heart of the idea of e-Estonia (Robinson & Hardy, 2021). Security of its digital services is also one of the marketing messages of the Estonian government, which emphasise the security of its service provision, with a strong focus on privacy. e-Estonia is also a product of strong public-private collaboration. This is evident in the background of the research participants of this thesis. Existing research has noted the importance of private businesses to the development of e-Estonia (Auväärt & Kaska, 2017) and the importance of securing both public and private realms (Paraskevopoulous, 2020)

In summary, e-Estonia can be considered a complex assemblage of Estonia's extensive e-governance and cyber defence infrastructure and institutions. This assemblage is both human and non-human, including both workers and citizens, as well as software and hardware. Current research has also suggested it is a form of modern nation branding, yet simultaneously it is also practical and citizen-centric. At its core, e-Estonia is a movement by the government of Estonia to facilitate citizen interactions with the state through electronic solutions. This has been noted to be a clear policy success (Kattel & Mergel, 2019). However, as this introduction has highlighted, e-Estonia is a diverse and complex concept. This thesis explores that diversity, as outlined further below.

1.2 Doing Interdisciplinary Research and How This Thesis Happened

This thesis is the product of an interdisciplinary research project, spanning multiple subject areas. The author's academic background before the project was as a Geopolitics and International Relations scholar. However, this thesis has arisen out of co-supervision between the Information Security Group and the Department of Geography at Royal Holloway. Consequently, the project is a product of these combined fields, as can be evidenced within the literature review chapters, which constitute the second and third chapters of this thesis. Overall, the findings of this thesis contribute to the academic fields of security studies, international relations, information security, and geopolitics, and hopefully have utility beyond academia in terms of policymaking. It is further informed by two years of living and working in Estonia, and supervised by a Professor of International Relations at the University of Tartu.

The thesis is inspired by the need for a mutual understanding between social and technical disciplines. It consequently employs sociotechnical and everyday approaches to frame these challenges. This thesis is further driven by the idea that we should recognise the study of cyber security and e-governance as an increasingly diverse research area, incorporating nontechnical and sociotechnical approaches to understand interactions between humans and technology. The research has been inspired by the growing recognition that cyber security is no longer merely the concern of technical experts (for example, McGraw [2013] notes the majority of policymakers are not tech-savvy, while Dunn-Cavelty & Balzacq [2016] argue that cyber security is increasingly concerned with a complex network of actors, including non-technical humans). Similarly, e-governance has seen an immense surge of interest due to the 'revolution' of e-business and information systems (Lee-Geiller & Lee, 2019). This interest goes far beyond technical audiences

alone, and contemporary research has noted that secure e-governance is increasingly focused on the development of citizen-centred approaches, driven by concerns relating to citizens' privacy, confidence, and trust (Yang et al, 2019).

These concerns with the development of secure e-governance are reflective of the changing nature of cyber security. Particularly in the western world, we live in an environment of ubiquitous connectivity. It is no longer responsible, nor realistic, to leave cyber security to those with a technical background, be it in programming, cryptography, or information security. Cyber security is increasingly concerned with the everyday, where humans increasingly interact with connected devices as part of mundane, daily activities (Ahn & Jung, 2016). This sociotechnical interaction means that security risks pervade daily life and create a discourse around everyday cyber security issues and concerns. This is characterised by an increased reliance upon technology, otherwise known as digital dependency. The security experience that arises from this digital dependency has geographical variances, depending upon the relative affluence of nations, levels of access to technology, devices, and connected services. Of crucial importance to this thesis is the local variances that determine engagement with, access to, and acceptability of e-services in different locales. These variables can influence the relative acceptability of a service in one location, and why it might not be acceptable in another. This thesis argues that e-Estonia is uniquely vulnerable yet also, in some ways, thrives because of these sociotechnical challenges. However, these challenges often bring insecurities to users. Conversely, e-Estonia represents an opportunity for the Estonian government to not only consolidate and expand services at home but also beyond Estonia's borders. Given the broadness of the challenges faced by Estonia, the thesis is titled:

Securing e-Estonia: Challenges, Insecurities, Opportunities

This title is reflective of the analytical work undertaken in the thesis, in addressing the research questions (the development of which are further elaborated in the Methodology Chapter 4) which are listed below:

- **What, in the Estonian context, is the relationship between the state, citizen, and everyday cyber security?**
- **Are cyber security concerns changing wider geopolitical and security concerns, especially in relation to Russia?**
- **How does Estonia use its status as a digital pioneer to extend its influence?**

These roughly highlight the major analytical themes of the thesis: That e-Estonia represents a challenge for Estonia (in the ever-changing relationships between the citizen, the state, and their everyday cyber security); that e-Estonia can generate and also reflective of insecurities (both cyber and geopolitical), and the e-Estonia also represents a major opportunity for Estonia to expand its influence (diplomatically and as a means of expanding soft power). The overall structure of the thesis is outlined in more detail below.

1.3 Thesis Structure Overview

This thesis is structured into 8 separate chapters. Chapters 5–7 address the above research questions, chapters 2 & 3 constitute the literature review, 4 the methodology, and 1 and 8, the introduction and conclusion respectively.

1. Introduction
2. Securing e-Estonia: Geopolitics, Trust, and Smallness
3. Everyday Cyber Insecurities, e-Governance and the Sociotechnical
4. Research Design and Methodology
5. e-Estonia & Post-Soviet Estonia: Contemporary Security challenges
6. Estonia's Everyday Cyber Geopolitics
7. Estonia's emerging e-Nordic strategy
8. Conclusions

The thesis is the culmination of a four-year project, involving primary research undertaken within the Republic of Estonia during an institutional visit to the University of Tartu, as well as numerous other visits to the country by the author. Other trips to Estonia included attending conferences and events within Estonia, primarily for the networking opportunities this provided, thus building research contacts within the country. This was integral to the research methodology, along with a visiting fellowship at the University of Tartu stretching two years (January 2018 to December 2019) and accompanied by multiple other visits between 2016–2021. These contacts spanned both the public and private sectors. The targeted participants for the conducted primary research were sourced based on professional connections to the tech industry in Estonia. The full justification for sourcing of participants is discussed further in the methods and methodology (Chapter 4), as well as the means of analysis, and reflection upon these methods.

This thesis (supported by the existing literature highlighted in Chapters 2 and 3) urges a more human-centred focus for cyber research and utilises qualitative approaches to the study of e-governance and cyber security concerns. The thesis also highlights the need for researchers to do more to address the increasingly mundane challenges of everyday digital life, arguing that the contemporary world has changed the nature of threats and that citizens are more reliant upon digital services than ever before. It is imperative that research must engage with the everyday impacts of digitalisation. This is outlined in Chapter 3, which discusses the 'everydayness' of cyber threats. This chapter raises moral and ethical arguments and also discusses the proliferation of connected devices as a source of potential insecurity. The argument is further framed around sociotechnical relations, and acknowledges the complexity of such studies, reflecting upon the utility of various concepts (such as assemblage and hybridity) as means to better comprehend the multiple and often seemingly conflicting ways in which cyber concerns are addressed academically.

Chapter 2 of the thesis establishes the contextual value and contribution of this study. This chapter focuses on Estonia itself as a case study and builds an argument that Estonian attitudes to cyber security and e-governance are closely

linked to Estonia's geopolitical concerns and interests. The chapter highlights the importance of trust and suggests that existing small state security research can be a helpful way to understand why Estonia behaves as it does. Meanwhile, the chapter also explores the modern history of Estonia, exploring how trust in the state has been an integral asset of the development of e-Estonia. Both Estonia's 'smallness' and the importance of 'trust' are both identified as important factors that have shaped e-Estonia. The decision to focus on Estonia as a case study is justified within this chapter with an explanation as to *why* Estonia matters as a case study. The chapter explores the idea of geopolitical narratives, and how these are shaped by cyber security concerns, but also conversely how geopolitical narratives shape cyber security concerns. The chapter defines a geopolitical narrative as the everyday expression and construction of national identities, or the repetition of perceived national anxieties or threats, inspired by the research of Sidaway & Power (2005), Dittmer (2009), Dittmer & Bos (2019) and Berg & Ehin (2013). The everyday repetition of narratives, the thesis argues, can also be evidenced in the construction of everyday cyber threats, but also be utilised to reinforce trust in the Estonian state, due to geopolitical proximity and Estonia's troubled relationship with Russia. The chapter concludes that wider geopolitical narratives affect cyber security concerns and that these geopolitical narratives can shape how individuals interact with technology.

One of the ways in which this thesis critically examines the e-Estonia narrative is to examine the security concerns of Estonians relating to cyber security and e-Government. It explores how Estonians navigate their everyday digital lives, including the new technologies, sociotechnical interactions, and ubiquitous connectivity of e-Estonia. The thesis additionally argues that many contemporary security concerns closely reflect contemporary geopolitics. While security is not a primary concern for citizens, it is nevertheless an important political issue. Most citizens, when questioned, hold opinions on such matters, even if they do not make an immediate connection to their daily lives. These opinions can often be linked to security anxieties or insecurities (Pain & Smith, 2016). Moreover, e-Estonia has become critically embedded within Estonian daily life, and this thesis represents an exploration of issues of digital dependency. This, the thesis argues, may have wider research impacts, and lessons from Estonia can be extrapolated beyond Estonia's borders, to other nations considering adopting similar e-governance practices, with high levels of connectivity, and with similarly challenging geopolitical neighbourhoods.

The analytical chapters of this thesis are informed by extensive fieldwork undertaken in Estonia. This fieldwork involved interviews conducted by the author in Estonia. However, interviews alone do not inform the thinking and analysis undertaken. This was also inspired by the substantial time spent by the author in Estonia. During this period the author has become a resident of Estonia and consequently possesses a digital identity. This grants access to the majority of e-services that Estonian citizens also have access to (withstanding the right to vote in national elections). During the time of the research, the author also regularly attended cyber security and e-governance-related events such as 'hackathons', networking sessions, conferences, talks, and more. The author's knowledge of the Estonian political landscape was also enhanced by time spent working as a visiting fellow at the Johan Skytte Institute of Political Science in Tartu. Further understanding of citizens' attitudes to cyber security was also shaped intangibly in non-formalised settings, supplemented by conversations with colleagues, friends, and acquaintances. These anecdotal ex-

periences alone of course do not inform the thesis, but inform ethnographic understanding, supplemented by the more formal research undertaken. More detailed explanations of the thesis's methodology can be found in Chapter 4.

It is also important to state the limits of this study. The author's fieldwork was predominantly spent embedded within an English-speaking academic department, in an affluent university city. Many cyber security and e-governance events in Estonia are heavily international – as is the tech industry, which is comparatively affluent and English-speaking. Further limitations are discussed both in the methodological chapter (4) and the conclusion (8).

However, the extensive time (by thesis research standards) spent in Estonia has provided the author with a deeper understanding and appreciation of Estonian culture, the social context of e-governance within the country, and the country's geopolitical situation. The research coincided with a sensitive period in the nation's recent history (given that post-2014 Russian Baltic relations have been remarkably poor – Trenin, 2020) and also with the 100th anniversary of Estonian independence (2018). Estonian geopolitical discourse frequently holds that Russia poses an existential threat to the country, and geopolitical anxieties are driven by fears of increased Russian assertiveness in Post-Soviet space (Wrange & Bengtsson, 2019). NATO forces, including UK personnel, have been stationed in Estonia in the post-Crimea annexation era as part of NATO's enhanced forward presence (EFP). The EFP has been argued to be a ritualistic and performative form of security, which exists more as a form of reassurance to the Baltic States and Poland, rather than a serious or effective military deterrent to Russia (Mälksoo, 2021). Nevertheless, it is important to the Baltic States. This is also reflected in the decision to locate the NATO Centre for Cooperative Cyber Defence Centre of Excellence in Tallinn (NATO CCDCOE). This is said to contribute to a sense of 'ontological' security and stability in a region which feels threatened, but also sends a message of multinational solidarity to Russia (Mälksoo, 2018)

Geopolitics (and its influence on digital professionals) is evidenced in the contributions of participants to this thesis. Geopolitically-driven security concerns were widespread – including matters of cyber security, engagement with the near-ubiquitous e-state, and the related, connected services it brings. These notions of everydayness, the sociotechnical and everyday cyber securities are developed throughout the thesis and are particularly reflected upon in Chapter 3, which also develops the conceptual basis of the thesis, identifying key literature across an interdisciplinary field including international relations, security studies, geopolitical, and information security disciplines. This thesis interprets the 'everyday' to mean the mundane interactions which are often treated as unimportant within daily life. This interpretation is heavily shaped by the contributions of Lefebvre (1987 & 1991) and more contemporarily (and explicitly within the study of security) by Stevens & Vaughan-Williams (2016) and Coles-Kemp & Hansen (2017). The 'sociotechnical' meanwhile, is defined as the everyday interactions between social life and technical systems and devices, inspired by the recent work of Malatji et al (2019) and Haddad & Binder (2019). Chapter 3 also focuses on the themes of sociotechnical relations, ubiquitous e-governance, and cyber security in the everyday. Of particular interest are the fields of critical security and critical geopolitics, which have increasingly begun to focus on everyday and mundane interactions and making connections with wider geopolitical and securitising narratives. Methodological consid-

erations, limitations, and more are developed both within Chapter 4 and in the final reflections in the conclusion (Chapter 8). Notable contributions that this research seeks to expand upon include Kello (2017), Betz & Stevens (2011) and Buchanan's (2016) works, which highlight the interdisciplinary nature of cyber security. The research expands upon everyday security approaches, urged by Stevens & Vaughan-Williams (2016), and applies this everyday focus to cyber security and e-governance.

Chapter 2 focuses on the contextual background of the thesis, highlighting why an Estonian case study matters to our wider understanding of the geopolitics of cyber security. This chapter addresses whether Estonian cyber security concerns reflect wider geopolitical concerns, building upon the work of Buchanan (2016) and Kello (2017). The chapter identifies important themes within existing literature such as small state security and trust and discusses how these are shaped by Estonia's geopolitical relationship with neighbouring Russia. The chapter further outlines how Estonian security (and cyber security) concerns are shaped by this geopolitical relationship. Furthermore, it explores Russian perspectives on these challenges and reflects upon the cyber security risks posed by continued poor relations between the two nations. It has also been argued by existing research that without trust, e-Estonia simply would not function, as it requires extraordinary levels of citizen consent for these ubiquitous digital services to be accepted. Bélanger & Carter (2008) and Männiste & Masso (2018), have highlighted the importance of trust in establishing functional e-governance and services, as well as catering to the privacy concerns of citizens in order to maintain that trust. Chapter 2 explores this in further detail and discusses this trust in relation to small state security and wider Estonian geopolitical concerns.

The analytical chapters of this thesis consist of chapters 5-7. These chapters form the bulk of the original contributions of this research, utilising the primary data gathered by the researcher and supplementary secondary data to support their argumentation. The direction of these chapters and research questions were inspired by the data, and more details of this process can be found within the methodology (Chapter 4). Chapter 5 focuses on the social, cultural and historic development of e-Estonia and it posits the question what, in the Estonian context, is the relationship between the state, citizens, and everyday cyber security? It discusses e-Estonia as a concept and a form of identity expression, reflecting upon how the *idea* of the e-state and ubiquitous connectivity have become part of what it means to be an Estonian. Moreover, the relationship between the state, citizens, and everyday cyber insecurity is explored in further detail. It also reflects upon the immediate Post-Soviet period and suggests that this was a formative era, crucial to the development of e-Estonia. Analysis within this chapter was informed by the research participants, where a notable pattern emerged discussing the development of e-Estonia as a product of Estonia's unique situation in the Post-Soviet years. Research participants repeatedly highlighted that this era allowed the government of newly re-independent Estonia extraordinary levels of freedom and trust to innovate with digital solutions. This develops further the work of Mälksoo (2015), Aalto (2013), and Cameron & Orenstein (2012) who note the legacy and memory of the Soviet era in shaping the contemporary security landscape in Estonia. Yet this chapter also notes the many challenges Estonia has faced in its recent history and highlights how ubiquitous digitalisation and the proliferation of connected devices, as well as Estonia's contemporary politics, pose new challenges to e-Estonia.

Chapter 6 of the thesis then moves on to explore how cyber security concerns in Estonia reflect geopolitical concerns, particularly relating to Russia. It explores the complex relationship between Estonians and their connected devices, their interactions with connected services, and how these inform their security anxieties. The chapter explores the idea of digital dependency, as well as the ways individual citizens navigate and mitigate their concerns with connected devices. It also discusses the geopolitical and national security aspects of e-Estonia. Following the findings of the research, the chapter also addresses the perceived growing hybridisation of threats, in particular, the idea of 'fake news' or disinformation, and how this represents a uniquely everyday concern, but also relates to an everyday geopolitical expression of Russia as a threatening actor, and something which poses a threat to Estonian national security.

It also reflects upon how Russia projects power in the region, via increasingly sociotechnical means. This includes the use of perceived disinformation, soft power, and propaganda via digital means, building upon existing research from Pigman (2018) and Tsvetkova (2020). The chapter focuses on feelings of cyber 'insecurity' and critically analyses the cyber sphere as a conduit for communicating geopolitically charged messages via disinformation. It reflects upon how the human aspects of cyber security (such as disinformation and human error) are crucial to the future of e-Estonia and reflects upon what it means for the long-term security of Estonia, building upon the work of Betz and Stevens (2011), who argue that omnipresent technology represents a significant security challenge to states and citizens alike.

Challenges for the state, but also opportunities to build human-focused, collaborative security are the subject of the analysis of Chapter 7, which investigates ongoing aims to integrate the X-Road e-governance platform of Estonia with that of Finland, Iceland, and the Faroe Islands (and potentially beyond in the future). It poses the question of how Estonia uses its status as a digital pioneer to expand its influence. The development of cross-border e-governance is considered important by the thesis as it represents the first organised implementation of an e-governance model similar to Estonia's beyond the Estonian border, as well as the first notable attempt to create interoperable, cross-border services between two sovereign states. The chapter builds upon existing small state literature such as Thorhallsson (2012 & 2018) that has argued that small states increasingly seek to expand their influence on the international stage by specialising in niche interests within the international community. What little small state cyber security research exists currently has focused on Estonia using cyber security to gain notoriety (Crandall & Allen, 2015) or focused on the ability of small states to benefit from alliances and institutions, such as Burton's (2013) paper on New Zealand.

Chapter 7 expands on both the Estonian case study and also the utility of institutional and regional cooperation, noting Estonia's significant links to the wider Nordic-Baltic region of northern Europe, which the thesis argues Estonia holds common ground socially and culturally with, as opposed to larger nations in Western Europe. Furthermore, it suggests that as a small state, Estonia has been granted significant goodwill and the ability to innovate and pursue modernisation strategies than other nations would be. Estonia's 'smallness' has enhanced public trust, a theme consistently highlighted within this research. Whilst specifically focused on the expansion of the X-Road to integrate Finland, Iceland, and the Faroe Islands, the chapter also considers other potential expansions, as well as the everyday

cyber security concerns which should guide the imposition of any ubiquitous systems of e-governance. It also notes that Estonia is quite happy to coordinate closely with other Post-Soviet nations such as Ukraine and Azerbaijan, it does not seek to formalise nor publicise closer relations in the same way as it does with its northern neighbours.

Chapter 8 brings together the findings of the project, offering conclusions and reflecting upon the contemporary challenges faced by e-Estonia. It makes suggestions of what can be learned from the Estonian experience and reflects upon the argumentation of the thesis, which suggests that e-Estonia is moulded by a complex mix of sociotechnical factors. These factors are wide-ranging and include societal norms, geopolitics, history, technology, and data. The conclusion also highlights the importance of ubiquitous connected devices to contemporary matters of cyber security and e-governance. It concludes that e-Estonia poses a complex, sociotechnical mix of challenges, insecurities, but also opportunities. These play out in the everyday lives of the digital professionals who maintain them. It is also a powerful form of nation-branding and a means to expand Estonian influence internationally. Finally, there is a discussion of the limitations of the project, and tentative suggestions for further research in this field.

2. Securing e-Estonia: Geopolitics, History, & Trust

2.1 Introduction

This chapter explores existing research that focuses on Estonia. The chapter addresses the research question How do Estonian cyber security concerns reflect wider geopolitical narratives? In order to achieve this, the chapter conducts an extensive literature review of existing geopolitical literature focusing on Estonia and the Baltic region.

It has been noted that Estonian security dilemmas are often said to roughly coincide with the concerns of many other small states (Crandall, 2014), yet the digital dimension of e-Estonia heightens vulnerabilities. This chapter highlights how Estonian cyber security and the perceived risks to Estonian e-governance are shaped by external geopolitical forces.

This chapter, along with chapter 3, represents an extensive literature review of existing research relevant to the project. While Chapter 3 deals with the more conceptual basis of the thesis, this chapter considers the contextual basis of the thesis, chiefly focusing upon Estonia itself, and the development of e-Estonia. This chapter highlights some of the key historical events which led to the founding of e-Estonia, noting important events from re-independence to the present day. It also notes the importance of geopolitical narratives and discusses the idea of Estonia being a nordic nation, and how this clashes with the Post-Soviet identity Estonia is often associated with. It also illuminates some of the conflicting geopolitical narratives between Estonia and neighbouring Russia and demonstrates that competing historic memory still plays an important role in the everyday geopolitics of the region. These competing geopolitical narratives, alongside feelings of smallness and insecurity, shape a hostile and suspicious attitude towards Russia. The chapter also explores the issue of trust, noting how vital it was in the immediate resumption of independence and the digitalisation that has shaped e-Estonia. It highlights how important trust remains for e-Estonia going forward. It suggests that both Estonia's 'smallness' and the role of citizens' trust are crucial to understanding the challenges and insecurities that shape Estonian security concerns.

2.2 Estonia's Geopolitics, Geopolitical Narratives, and Why They Matter

As this chapter is concerned with geopolitical narratives, it is pertinent to introduce what this terminology means. Existing research suggests that a geopolitical narrative might be something that shapes not only citizens' popular understandings of their nation, but also other nations'. Notable contributions to this field include Sidaway & Power's (2005) paper exploring the contemporary Portuguese identity. He argues geopolitical discourses are constitutive moments within the expression and construction of 'national' identities, highlighting the importance of historical legacies in shaping geopolitical narratives. This has some parallels with contemporary and still emerging Post-Soviet identities (Berg & Ehin, 2016, Morozov & Fofanova, 2016).

Dittmer & Bos (2019) and Dittmer's (2005) work on geopolitical narratives identify various theories of geopolitics and nationalism, relating them to popular culture and identity. While Dittmer (2005) frequently focused on the dis-

cursive ways in which national identities were reproduced in popular culture, Dittmer & Bos (2019) further explored alternative ways in which this might be expressed through everyday life including social media and computer games. What emerges is a growing research area interested in mundane, everyday interactions and technology, and how it communicates geopolitical narratives. This thesis furthers that interest in everyday sociotechnical interactions, and the geopolitical narratives which can be communicated by such means.

It is worth clarifying what Estonian geopolitical narratives might be evidenced in daily life. Berg & Ehin (2013) argue that dominant narratives and senses of identity are integral in shaping foreign policy, and establish dominant Estonian and wider Baltic geopolitical narratives within their research. They note that these include the politics of memory (particularly of the Soviet era), discourses of danger and insecurity in the wider Baltic region (relating to a perceived existential threat posed by neighbouring Russia), and narratives of smallness and vulnerability.

Another integral aspect of Estonia's geopolitics is both a perceived threatening neighbour (Wrange & Bengtsson, 2019) and patriotism and trust in Estonian self-governance. This has been noted in existing research such as Petsinis (2015) who argues that Estonian national survival is linked to a kind of 'ethnopolitics' and that guaranteeing the perceived ethnic Estonian character of the state is the nation's number one geopolitical concern. Estonia itself is consequently (supposedly) threatened by the shrinking Estonian population, and is also troubled by the significant Russian-speaking minority who are sometimes considered a legacy of the Soviet era (and are sometimes considered even more problematic due to the perceived threatening nature of modern Russia also). This has been noted in contemporary research, which has further argued that many of the Russian-speaking population in Estonia feel a stronger cultural affinity to Russia (see Cheskin, 2015 & Yatsyk, 2018 for more) and this shapes how those minorities interact with the Estonian and the Russian state. Most notably, the 2007 'Bronze Night', where local Russian-speaking communities in Estonia rioted due to the removal of a Soviet war statue highlighted this cultural cleavage. Russians (and Russian-speakers across the former Soviet Union) have been noted to value the historical memory of the Second World War/ Great Patriotic War and the defeat of fascism extremely highly (Sakwa, 2017), and this move was perceived as an offensive provocation by the Estonian state. 'Memory wars' between the Baltic States and Russia form part of a continually hostile relationship, due to conflicting opinions and memories of the events of the 20th century (Mälksoo, 2012 & 2018). The riots coincided with coordinated cyber attacks that have been linked to both the Estonian-Russian population domestically, and from within Russia itself (Hansen & Nissenbaum, 2009). These attacks, which crippled the e-state for several days, demonstrated how Estonia's connectivity represented a security risk that could be exploited by either a hostile power, or hostile civilians, and was triggered by the everyday geopolitical identities of Russian-Estonians, who felt marginalised within society (Yatsyk, 2018). These attacks did not lead to an immediate change of approach to Estonia's cyber security and e-governance, but rather prompted a gradual evolution of new approaches which continues to this day (Robinson & Hardy, 2021). Below, figure 1 illustrates a timeline of the development of e-Estonia from its inception at the resumption of Estonian independence to the present day. It charts all developments, be they political, social, or technical.



Figure 1: Mapping the History of the e-state. This timeline illustrates key moments in the development of e-Estonia as referenced by Research Participants. (Author's image)

2.3 What Shapes Threat Perception? Estonia and Beyond

Cyber security has its roots in information security which is often defined as being chiefly concerned with the confidentiality, integrity, and availability of data (Whittman & Mattard, 2011). However, many states are now coming to terms with contemporary threats to cyber security being increasingly diverse and having a geopolitical dimension (Hansen and Nissenbaum 2009), and Estonia is not alone in this regard (Robinson & Hardy, 2021). This, in turn, has bred multiple interpretations of what cyber security means. In the fields of international relations and security studies, for example, cyber security can be said to be one aspect of a wider national or human security concern (Buchanan, 2016 & Kello, 2018).

Scholars of international relations have argued that cyber security is blurring existing framings of international security. It is said to be constantly in flux, constantly evolving, and represents no less than a ‘revolution’ that is changing statecraft (Kello, 2018) citizens’ relationships with the state, sovereignty, and conflict (Betz & Stevens, 2011), and the nature of warfare itself (Rid, 2013 & Rid & Buchanan, 2014). Whilst ‘cyber war’ may, or may not happen, depending on whom you listen to (and which particular definition of that phrase you adopt), what is unquestionable is that cyber security has had an enormous impact on how contemporary security challenges to national security are perceived. Indeed, as has been argued by Dunn-Cavelty (2013), cyber security has changed the very way in which we discuss security in the online world, and there has been a growing securitisation of online life in recent years. This, as Buchanan (2016) suggests, leads to a fearful and anxious security environment, for both states and citizens, demonstrating a link between national-level cyber security concerns, and the concerns of the individual highlighted earlier in this chapter.

What is growingly evident, is both the threat cyber security poses on a national security level, but also crucially how citizens are increasingly expected to become security actants in ensuring both their own and national cyber security (see Stevens, 2020 & Stevens & Vaughan-Williams, 2016). This is connected to both an increasing connectivity and digital dependency within modern states. Cyber threats have also challenged and disrupted the hierarchy of state and non-state actors and blurred the lines of contemporary warfare (Rid, 2014). Plausible deniability and anonymity have enabled social movements, such as Anonymous, to wield considerable power comparable at times to the digital power of a state (see Kello, 2018 & Betz & Stevens, 2011). In a similar vein to non-state actors gaining power and agency, there has also been a considerable transformation of contemporary cyber security concerns. These, as identified also by Kello (2018) and Betz & Stevens (2011), include the possibility for non-state actors (as well as state-controlled information outlets) to control political narratives – particularly online via social media and dubious media outlets.

The fear of disinformation and dubious media outlets takes on geopolitically charged agency in the Baltic states, where Russian-language information linked to the Kremlin is feared to be influencing citizens and their national allegiances (Wrange & Bengtsson, 2019 & Cheskin, 2015). The possibility for malicious online actors (state and non-state alike) to shape political events by spreading disinformation further highlights the need for a move towards everyday cyber security approaches and a commitment to sociotechnical research. Such research might explore a multitude of different angles, including the everyday access to private services, safe access to secure e-governance, how the growth of connected devices changes perceptions of cyber risk, and some of the challenges this poses to governments and citizens alike in day-to-day life. Everyday security has also been critiqued as problematic. It has been argued that the leaking of security expectations into everyday life has meant that citizens are increasingly expected to become active security actors (to cite a familiar, everyday example, the expectation citizens report ‘suspicious behaviour’ in public places – Vaughan-Williams & Stevens, 2016). Similar expectations are becoming more and more frequent, and this expectation is progressing to the realm of cyber security. Vaughan-Williams & Stevens (2016) tackle such issues of security by seeking to measure the impact of security policy through engagement with citizens as a means of developing an understanding and relevance of such policy to people’s everyday lives. These approaches chimed with the

research of other critical security scholars, who have expressed concern with the increasing omnipresence of security in our everyday lives, and sought ways it might be challenged (Booth, 2005 & Neocleous, 2008).

Many security scholars have begun to explore the relationship between security processes and everyday life, such as Stevens & Vaughan-Williams (2016) Crawford & Hutchinson (2015), and Dourish et al (2004). They argue that the study of everyday life is of vital importance to understanding modern security challenges. Stevens & Vaughan-Williams (2016) note the increased presence of security fears of terrorist attacks in contemporary Britain, and the burden of such security increasingly being passed to the everyday citizen. They highlight instances such as when the public is asked to 'remain vigilant' and 'report suspicious behaviour' as common examples of these securitising processes in everyday life (Pink et al, 2018). Such security concerns can be directly related to the everyday geopolitical narratives which pervade security thinking. Smith & Pain's (2009) 'double helix' suggests that everyday life and geopolitics are integrally interwoven like DNA, and ever-present, if not always explicitly expressed. Thus, everyday geopolitical thinking influences everyday security decisions. In Estonia, the everyday geopolitical environment is overwhelmingly influenced by the perceived fear, or anxiety, of Russia (see Ehin & Berg, 2013, Morozov & Fofanova, 2016 & Jæger, 2000 for more). In combination, these processes have been conducive to producing a securitised environment.

This thesis is particularly interested in the geopolitical motivations and limitations of everyday cyber security. It has been suggested that one of the benefits of the power of 'cyber' is that it reproduces and reinforces existing discourses, as well as constructs and disseminates new ones (Betz & Stevens, 2011). Others argue, however, that a softer interpretation of cyber power contains the ability to make the people do something they would not ordinarily do by influencing actions or political decisions (Nye, 2010). It is also noted that interactions are less civil and that people often act differently or are emboldened in their behaviour in the online realm (Kello, 2018). This critical analysis of cyber has some parallels with the work of critical geopolitical research, such as Pain and Smith (2009), who suggest that fear and anxiety are crucial geopolitical phenomena, capable of shifting public opinion. This has some resonance with Buchanan (2016: 193) who claims that the core of the cyber security dilemma is about fear and escalation: the fear that causes the security dilemma to arise and the escalation that the security dilemma potentially brings about. This is also reflective of the concerns of 'securitisation' raised by Dunn-Cavelty (2013), which increasingly make the online world, and the connected services associated with it, unknown and potentially threatening to the citizen.

Of further interest is the geographically situated nature of the cyber. Sheldon (2014) argues that 'cyberspace' is inherently geographical, highlighting the situated and material nature of the hardware. Similar arguments can also be found in Kitchin & Dodge's (2011) *Code/Space*, which highlights the transformative power of software in shaping everyday life and spaces. Both arguments combine to illustrate the everyday geographies of both hardware and data itself. Geopolitically-charged interactions represent a significant security dilemma when many of these narratives now target ordinary citizens, and ubiquitous connectivity and services pervade daily life.

The security dilemma facing governments includes: how do everyday citizens negotiate the security challenges posed by ubiquitous connectivity and politicised cyberspace, and how do governments meet the challenges of providing everyday security to their citizens. This securitised environment might be characterised by increased potential threats, increased attack vectors for malicious actors, as well as the increased potential of technology to disrupt daily life.

Many critical scholars are interested in developing comprehensive and contextual research in cyber security, mindful that cyber threats are increasingly human, diverse, and their perception is amplified by human emotions. The human aspect of cyber security is a growth area within the subject. This thesis seeks to demonstrate that the human aspect is crucial to understanding the importance of cyber security and e-governance in everyday Estonian life. Scholars from various fields have highlighted how people interact with technology in sometimes unexpected ways, or in entirely normal, mundane ways, with potential consequences for their security (Stevens, 2018 & Coles Kemp, Ashenden & O'Hara, 2018). This includes the way migrants access technology (Coles-Kemp, Jensen & Talhouk, 2018), how everyday cyber risks can be visualised (Hall, Heath & Coles-Kemp, 2015), and how attackers tend to exploit human errors in cyber attacks (Safa, Von Solms & Futcher, 2016), and the impact of human behaviour on building functioning cyber security (Evans et al, 2016). A number of different critical approaches, too exhaustive to fully list, have influenced the argument that security must be 'built in' to mitigate human risks (McGraw, 2013). Matters of cyber security can thus be argued to be increasingly sociotechnical because cyber attacks and malicious actors increasingly target human errors (Balzacq & Dunn-Cavelty, 2016). Mundane, everyday security is now a growing concern in matters of cyber security and e-governance in Estonia, relevant to both citizens and the state.

Existing research has noted the ability to wage conflict utilising digital means (or utilise it as a supplementary means of disruption) has been deployed in a range of incidents ranging from the Stuxnet attacks (Balzacq & Cavelty, 2016), 'Wannacry disabling the NHS' (see Dwyer, 2018), to the 2007 Estonian 'cyber war' (see Hansen & Nissenbaum, 2009). Stuxnet and Wannacry were both, allegedly, spread largely due to human error. The Stuxnet attacks involved a malicious worm being inserted into the system, via human error – someone inserting a USB device they did not recognise. Wannacry meanwhile, preyed upon the failure to update systems. A routine, non-sophisticated attack which ended with severe consequences.

Meanwhile, the 'cyber war' on Estonia, consisted of a simple, brute force DDOS (Direct Denial of Service) attack and had a series of human impacts, temporarily bringing Estonia's e-governance systems down. This attack is a significant historic event in the history of modern Estonia and can be argued as a pivotal moment in the ongoing development of e-Estonia (Robinson & Hardy, 2021). The attack not only inflicted inconvenience on users (a problem amplified in Estonia due to the nation's digital dependency) but also became a symbolic Post-Soviet event. It is an early example of the 'hybrid' conflicts which some have argued have come to characterise Post-Soviet space (Mälksoo, 2018) and increased Russian aggression (Giles, 2016). 'Hybrid' events are delivered as cyber attacks combined with kinetic attacks or disruption (Galeotti, 2016). In Estonia, the DDOS attack was coordinated with rioting by Estonia's Russian minority, angered by the removal of the Soviet-era Bronze Soldier statue in Tallinn. It has been suggested that this

new type of conflict heightens the need to understand the relationship between human and non-human cyber challenges, and the need to develop international norms around cyber-attacks (Hansen & Nissenbaum, 2009). Such supposed ‘hybrid’ attacks have similarly been evidenced in the 2008 Russo-Georgian conflict, as well as the 2014 conflicts in Crimea and Donbas, Ukraine (Galeotti, 2016).

Consequently, geopolitics has a role to play in this Estonian case study, along with social, cultural and historic factors, which all hold a degree of influence over human interaction with digital devices. These numerous different factors play a role in shaping the digital ecosystem because cyber security is diverse and equally shaped by non-technical interactions as well as technical. The geopolitical is an aspect of the ‘sociotechnical’, a term elaborated further below.

2.4 Why do Everyday Geopolitics Matter to our Understanding of e-Estonia?

At this juncture, it is important to distinguish between formal geopolitics and an increased scholarly interest in everyday geopolitics. Whilst formal geopolitics might be conceptualised as state-centric international relations and the geographical determinism which shapes them, critical geopolitics (see Ó Tuathail, 1996, Dodds 2007 & Dittmer & Gray, 2010) is concerned with citizens and the discourse they engage with. This has led to a growing academic interest in ‘everyday geopolitics’ (Pain & Smith, 2008, Dittmer & Gray, 2010) As with everyday security, everyday geopolitics challenges powerful or hegemonic narratives and ways of thinking. Instead, it seeks increased focus on the mundane and ordinary (Sharp, 1993, Dittmer & Gray, 2010).

With the proliferation of ‘smart devices’ and the ‘internet of things’, we are seeing a proliferation of means to access and alter everyday geopolitics within daily life, via social media and the growth in online news outlets. This can be seen to both challenge, but also potentially reinforce existing power dynamics (Nye, 2010, Tsvetkova, 2020). The current cyber security policies for NATO and Estonia identify these two areas as growing cyber risks (Estonian Cyber Strategy, 2019). What emerges within both documents is an increasing focus on the mundane daily interactions between humans and technology (i.e. ‘everyday’ or ‘’’ interactions, further explored in chapter 3) ¹. Whilst neither term is explicitly used there is a clear recognition in official strategies that there is much work to be done to build increased cyber security awareness among the civilian population. This is highlighted by policies noting the need for education and improved working practices. The ‘everydayness’ of such challenges might best be symbolised in Estonia by the volunteer cyber defence league.

The cyber defence unit of the Kaitselit (Estonian defence league) is a volunteer organisation, integrated within government forces that contributes cyber security advice to the government, and actively works toward collective defence scenarios in the event of a future cyber-attack. The stated goals of the organisation are:

¹ Both strategies are available online:

Estonian Cyber Strategy [online] at <https://www.mkm.ee/en/objectives-activities/information-society/cyber-security> [Accessed 03/07/2018]

NATO Cyber Strategy [online] at: <https://www.nato.int/docu/review/2019/Also-in-2019/natos-role-in-cyberspace-alliance-defence/EN/index.htm> [Accessed 04/02/2019]

- a) the raising of society's awareness regarding cyber threats*
- b) the sharing of knowledge among IT specialists in the field of information security*
- c) participation in the crises management with protecting critical infrastructure “*

(Kaitsellit.ee)

This contrasts with top-down NATO approaches. However, the official NATO documents also highlight that everyday citizens are active participants in providing their own cyber security (NATO CCDCOE, 2018). This is to be achieved through a mixture of education and awareness, as well as a sense of personal responsibility on the citizen's behalf. Consequently, citizens become vital everyday actants within the wider security apparatus, through their everyday behaviour in cyberspace. This is driven by a degree of recognition that governments alone cannot assure the citizen's cyber security. NATO documents note the move towards everyday cyber security evidenced by the growth in the ubiquity of the IoT and the connective capability of seemingly mundane and everyday devices and the threats they represent. They also emphasise the benefit to citizens in becoming more cyber aware. However, the benefit is arguably weighted heavily in favour of the state, given the state's investment in cyber and digital technologies has forced citizens to become cyber aware, and the state cultivates resilience as a strategy, based upon citizens as security actants. These policy documents (NATO CCDCOE, 2018 & Estonian National Strategy, 2019) acknowledge the citizen as a participatory security actor. Individual citizens are framed as security actors and the Internet of Things is seen as a threat to, but also an enabler of national security.

2.5 e-Estonia', Nation Branding, and Identity

This section further investigates factors that have informed cyber security attitudes in Estonia. There is a growing global interest in cyber security matters, a perceived threat of increased Russian influence or aggression², as well as growing connectivity of daily life, thanks to the proliferation of connected devices. These concerns are exacerbated in e-Estonia, given the country's reliance on its e-services, which were highlighted by the 2007 DDOS attacks. However, e-Estonia should not only be conceptualised through the utility of public services and e-governance alone. e-Estonia is branded and marketed as an exportable commodity (Drechsler, 2018, Papp-Váry, 2018, & Mäe, 2017), perhaps further illustrated by the e-residency programme, as well as the modern e-governance visitor centre in Tallinn, which counts foreign dignitaries and investors among its many visitors. The promotion of the e-Estonia brand itself is a form of soft power, which casts Estonia as modern and Nordic, and disassociates Estonia from its Soviet past (Hardy, 2020, Tammpuu & Masso, 2018). The sharp contrast of modern Estonia's public image when compared to the Soviet past is simultaneous to continued poor relations with neighbouring Russia (whom many of the significant Russian-speaking population of modern Estonia are often, rightly or wrongly, assumed to favour)³. This contributes to a tense

² In particular in the realm of cyber security. Pigman (2018) argues that Russia represents a threat to contemporary cyber norms within the international system

³ The Russian-speaking population of Estonia numbers around 30% of the total population, and is often heavily concentrated in certain areas, such as Narva, Sillamäe, and Idu-Virumaa county, as well as Lasnamäe, and other areas of Tallinn. More discussion of this population and local concerns can be found in Cheskin (2015)

Geopolitical environment, which is highly influential in Estonian politics and permeates Estonian society. The Baltic states and Russia's foreign policy goals have regularly conflicted particularly since the Baltic states' collective decision to join NATO (for a summary of this, see Trenin, 2010) the 2014 war in Donbas, Ukraine, the annexation of Crimea, and the Russo-Georgian conflict in 2008 have all collectively contributed to a contemporary, nervous security situation in the Baltic region.

e-Estonia is fundamentally linked to the idea of what it is to be Estonian, and an intrinsic part of the Estonian identity (see Mäe, 2017 for analysis of e-Estonia as a form of identity in popular media discourse). It also provides Estonia with the opportunity to grow from its physical, or numerical smallness. Cyber security and e-governance thus take on exceptional importance for the Estonian state.



Figure 2: e-Estonia branded presentation at the e-governance showroom, Tallinn. Author's image. (17.11.2017)

e-Estonia also makes Estonia uniquely vulnerable digitally. When combined with the backdrop of tense Geopolitical relations with Russia, rapid technological advancement, and increased connectivity, the risks to e-Estonia are numerous. It has been argued that the emergence of big data, and small mundane everyday interactions that are increasingly digitised, are fundamentally changing the cyber security landscape (Aradau & Blanke, 2015). Increasingly banal and mundane daily interactions are underpinned by cyber security concerns, and ever more services are linked to connectivity. This widening and deepening of what cyber security entails have been emphasised by critical scholars for some time (eg: Hansen, 2009; Dunn-Cavelty, 2015, Kello, 2017) and this is increasingly becoming recognised within

governmental strategies⁴. There is thus a growing intersection of human security, insecurity, and cyber security. This suggests that the purpose of cyber security should be to provide security for users (be that user the individual, the state, or a private company), but also that those users can also be the biggest threat to cyber security if they are not familiar with proper security processes and procedures, or appreciate fully *why* those processes and procedures exist. This has growing appreciation among interdisciplinary research.

It has been previously argued that the 2007 ‘cyber war’ emerged from the context of a historical conflict (Sear, 2017). Cyber warfare is not a new phenomenon anymore and has not yet produced the more dramatic predictions of cyber war. Similarly, the conflicts in Ukraine and Georgia are unique, and grounded within the particular social, cultural and political conditions of those regions. ‘Hybrid’ warfare, as evidenced there, is not easily replicable in the Baltic States (Kasekamp, 2016). There are lessons to be learned from all scenarios, but each is deeply contextual (Toal, 2017). These events are less a ‘new cold war’ but instead a new, information-driven conflict, where contrasting regional narratives play out through disparate sources through the means of modern technology as the messenger. This can be conceptualised as both a form of deterrence defensively and offensively as a form of coercion. Digital deterrence is the terminology utilised by the Russian government (Tsvetkova, 2020), and Estonia is at the forefront of leading this Digital deterrence within NATO and the EU (Herzog, 2017 & McBrien, 2020). These digital forms of deterrence and coercion increasingly target ordinary citizens and challenge how we approach cyber security.

Classical ideas of security, to some extent, have been dependent upon geopolitics. Perceived friends and enemies can be narrated through discourse, as illustrated through popular geopolitics (Dalby, 1992; Sharp, 1993, O’Tuathail 1996). Estonia is a small nation, located crucially on a geopolitical fault line, where NATO and the European Union meet Russia. In the years following regaining its independence, Estonia rebuilt the nation, recovering from years of centralised government under Soviet occupation. This involved rebuilding state infrastructure but also cultivating a modern Estonian identity that had been oppressed during years of Soviet occupation. This allowed a blank canvas to cultivate an identity focusing upon historic Nordic, European and Western identities (Kuus, 2002). Part of this reimagining of what it means to be Estonian has been articulated through the embrace of the e-Estonia image: successful and modern (Mäe, 2017). This is also evidenced by the Estonian digital identity. Estonia’s e-government systems rely upon this digital identity to function, and it acts as an integral part of the authentication process. These digital identities are linked to a physical smart card, and are symbolic of the modern state, as these cards were issued upon re-independence in 1991, and continue to be to this day. They are issued to all Estonian citizens, whilst residents also receive a similar card, albeit without the right to access certain services such as e-voting in general elections⁵ (*e-Esto-*

⁴ See Estonian cyber strategies (see Estonian Cyber Strategy, 2014 & 2019), The goals of the Ministry of Foreign Affairs for the Russian Federation (2016), a review of Estonian Cyber Strategy to date (Robinson & Hardy, 2021) as well as NATO’s strategy (NATO CCDCOE, 2018). Jensen et al (2019) discuss strategies critically, pertaining to matters of Russian interference, and the contemporary security implications of disinformation.

⁵ Residents can, however, vote online in local elections or European elections (the latter only if they are a European Citizen, but the former is available to all long-term residents regardless of their origin).

nia, 2019). The Post-Soviet identity, for some, is something to be shunned as out-of-date, or not reflective of the diversity of modern nations, and should be retired (Erizanu, 2021).

As is common with smaller states, in a conventional security sense, Estonia is dependent upon alliance building with large states (Thorhallsson, 2016). In terms of military capability, Estonia alone would be powerless to resist invasion by a larger, more powerful neighbour. This logic was of course fundamental in the decision to join NATO, and that relationship now sees a British regiment posted to Tapa in Eastern Estonia. Estonia is very much a junior partner in NATO and holds relatively small influence – something which Estonia is aware of (McNamara, 2017 & Crandall 2015). However, in a cyber security context, Estonia has seized a leading role in the articulation of cyber security norms (Adamson, 2019). This might be evidenced by the NATO decision to place the Cyber Security Centre of Excellence in Tallinn. Through embracing a leading role in this ‘soft security’ area, it has been argued that Estonia has increased its influence in NATO, and helped shape cyber policy (most notably, the ability of member states to invoke collective defence [article five of the NATO charter] in the face of cyberattacks) (see Crandall & Allan, 2015). This is particularly noteworthy, given Estonia was targeted in such a way during 2007, and demonstrates how cyber security forms part of Estonian security thinking and strategy in the desire to be seen as a ‘regional leader’ in this field (Wrangle & Bengtsson, 2019).

The Estonian geopolitical situation can be summarised as one of precariousness (Aalto, 2002, Orange & Bengtsson, 2019). The Estonian state is located at a geopolitical frontline, where NATO meets Russia. The popular and everyday geopolitics of Estonia can be said to be shaped by the country’s complex past, and precarious present (see Aaltola, 2013, for more discussion of the multiple factors which shape Estonian geopolitics, and Berg & Ehin, 2016 for more on Estonian identity). Estonia lives a fearful geopolitical life, shaped by existential threats facing its independence, including the survival of its language and cultural traditions, as well as the experience of the recent past (Kuus, 2002). It has been argued in existing research that this is evidenced in both the discursive reproduction of Estonian identity, but also in a popular discourse which perceives Post-Soviet Russia as heavily securitised, and constantly menacing the independence of the Baltic states (see Jæger, 2000 & Morozov & Fofanova, 2016). These have been coopted within the digital sphere, as a means of preserving Estonia in the event of a catastrophic event – going as far as Estonia establishing a ‘data embassy’ to protect the digital infrastructure and data of the nation in the event of an invasion (Robinson & Martin, 2017). Yet Estonia continues to find common ground with its allies, pursuing cooperation on multiple fronts, in a series of cultural and economic as well as security-based projects, including cross-border e-governance and digital diplomacy (Hardy, 2020).

2.6 Russia & the Baltic States: Clashing Identities & Contested Memories

Whilst Russia is not motivated to pursue a direct strategy against Estonia (which is a very small nation and not central to Russian foreign policy goals). However, the Russian state does pursue a distinct strategy within the Baltic region, characterised by several factors. These generally include the protection of Russian speakers, of which Estonia has over

300,000 (Cheskin, 2015 & Toal, 2017). Whilst the majority of Estonian speakers live in the capital city of Tallinn, they comprise a majority of the population in the regions of Narva and Ida-Virumaa county in the North East of the country. This has prompted some concerns that these civilians might have stronger loyalties to the Russian state and/or be targeted to create secessionism or disloyalty to Estonia (Trenin, 2020). These fears are informed by the recent events in the Russian-speaking regions of Georgia and Ukraine, and an oft-cited Putin speech now seen as a precursor to recent geopolitical events, decrying the collapse of the Soviet Union as disastrous:

"Above all, we should acknowledge that the collapse of the Soviet Union was a major geopolitical disaster of the century. As for the Russian nation, it became a genuine drama. Tens of millions of our co-citizens and compatriots found themselves outside Russian territory. Moreover, the epidemic of disintegration infected Russia itself."

Vladimir Putin's 2005 address to the State Duma (kremlin.ru, 2005)

Roughly a quarter of the Estonian population identifies as Russian (although, as highlighted earlier, this is geographically clustered within certain areas). Neighbouring Latvia meanwhile has an even higher proportion of Russian speakers – partially due to settlement in the Soviet era. The perceived failure of Estonia (and Latvia) to integrate these peoples has received considerable academic interest in the Russian-speaking minorities due to Moscow's outspoken focus on their protection (see Cheskin, 2015 for further discussion). Other goals include access to infrastructure, and the limitation of NATO deployments in the region (Trenin, 2011). Furthermore, of vital importance is the access to citizenship for the aforementioned Russian community in Estonia and Latvia. It is noteworthy still that around 7% of the Estonian population remains stateless as of 2015 (Amnesty International, 2018). This is due to the ongoing existence of so-called 'grey passports' issued to Russian speakers, who are largely concentrated within Ida-Virumaa County (which contains the noted border town of Narva) as well as certain districts of Tallinn. In the immediate fallout of the Post-Soviet era, a political decision was made by Estonia (as well as in neighbouring Latvia), that Russian speakers would not be issued full citizenship of the newly re-independent state. Instead, passports were issued on ethnonationalistic grounds, while Russian speakers (who many within Estonia still regard as unwelcome occupants from the Soviet era) were granted 'grey passports'. These act as legitimate and internationally recognised travel documents, but do not confer full citizenship to their holder (Cheskin, 2015, Jašina-Schäfer & Cheskin, 2020). Additionally, Trenin (2020) and Sakwa (2017) suggest that wider Russian foreign policy goals also include the preservation of historic memory and the Soviet Union as victors over Nazi tyranny in Europe.

The continual conflict of memory politics between Russia and the Baltic states thus shapes continued diplomatic and formal relations. Such identity politics are often deeply emotive and shaped by the conflicts and memory of the tumultuous past in the region (Fofanova & Morozov, 2016) leading to rival popular geopolitical narratives. Furthermore, it has been argued that the Russian and Baltic identities fundamentally contrast as European and non-European, although this is complex, and highly contested (Morozov, 2015). The Kremlin under Vladimir Putin has continually utilised the events of the second world war (Великая Отечественная Война or Great Patriotic War in Russian)

and the existence of far-right groups in the Baltics, to cast the Baltic states as being sympathetic to Nazis. Frequently, Kremlin narratives also suggest that the Baltic States (and Ukraine for that matter) are guilty of rewriting the history of the region, particularly the war and the Soviet era, and view attacks on this time as provocative (Toal, 2016). The Russian narrative is one of liberation, and the Baltic states remain either ungrateful for such liberation and/or were sympathetic or even collaborative in the Nazi war effort (see Pieper, 2018 for more discussion of contemporary Russian popular geopolitical narratives). This perception came to a head with the movement of the Soviet-era bronze soldier statue in 2007.

Estonia, as a former state of the Soviet Union, also generally falls under the Russian government's characterisation of the 'near abroad' (the subject of Toal's [2016] research) which centres around Russian interference, and invasion of its neighbours, albeit with a focus upon the conflicts in Georgia and Ukraine. Toal notes that geopolitical narratives are popular, discursive visions and that Russian geopolitical narratives often starkly contrast with those of Georgia, Ukraine, and the United States. It is vital to appreciate, however, that the characterisation of Estonia as Post-Soviet is deeply contested and a sensitive subject area. The Baltic states unanimously consider the Soviet era from the conclusion of the second world war to the collapse of the union as an illegal, military occupation (Aalto, 2003 & Kuus, 2002). Consequently, the suggestion that the Soviet Union was a liberating force is deemed deeply offensive to the Baltic states and further fuels contempt between them and Russia.

2.7 Estonia's Small State (in)Security

As explained in the previous section, in both the cyber and conventional security realms, Estonia's security environment is often defined by the country's relationship with Russia. It is also shaped by the Soviet past, significant events since Estonia re-established autonomy, and now by a complex cyber security relationship. Research has noted that popular and everyday geopolitics defines not only national relationships with Russia, but also citizens' perceptions of Russia, and subsequently, the Russian people (Ojala, 2016). Popular geopolitics can be seen to shape both public perceptions, and also, in turn, shape governmental policy. Such politics can be driven by multiple factors including media discourse, perceived security concerns, popular culture or reactions to political initiatives such as immigration or security policy (see Dodds & Dittmer, 2009; McFarlane & Hay, 2003; Williams & Boyce, 2013). This in turn often casts one group as either an 'other', a sinister or menacing 'enemy' and can be linked to ideas of securitisation, a process whereby something is identified as a security concern, or in the case of the perceived Russian threat to Estonia, an existential threat, and is consequently repeated until it becomes an accepted norm. It has been suggested this can happen at both macro and micro levels; i.e. relations between states, but also in daily life (Buzan & Waever, 2009). It can also be a source of orientalism, producing an orientalist Soviet 'other' (Morozov, 2015). These threat narratives are consequently open to manipulation or exaggeration, for political purposes. Some research has highlighted how Russia is continually 'othered' by its European neighbours, and particularly guilty are those in the European North (see Browning, 2003 for further discussion on this).

The idea that Russia was a source of cyber insecurity through the spread of ‘fake news’ or information which specifically pushed the political objectives of the Putin regime is a persistent narrative within wider literature (see Giles, 2016 & Galeotti, 2016 as some examples). It has been argued that Russia has successfully weaponised disinformation, undermining public trust, through a multitude of state-owned, Russian language media outlets, utilising social media, through both official accounts, as well as supposed ‘Troll factories’, which flood popular western media networks with Kremlin-funded propaganda, leading some to label Russia’s digital actions as a threat to global norms (Pigman, 2018). Others have suggested this now forms a key part of Russia’s modern ‘cyber power’ (Tsvetkova, 2020). Alternative opinions go further, suggesting Russia’s actions are simply in line with western actions, and that it is popular to blame Russia for the political failures of the west (Sakwa, 2017).

Such is the level of concern, that disinformation is explicitly mentioned as a key concern in the Estonian cyber security review published by the Estonian Government (Estonia Cyber Security Review, 2017). In particular, the Kremlin-sponsored Sputnik Media Outlet has been identified as particularly troublesome, as well as other, less abrasive Russian language outlets available in Estonian territory. These serve to feed long-standing concerns of Russian language media outlets as a source of disinformation, to shape the Geopolitical views of minority Russian Estonian citizens (ERR, 2020).

Smallness and the idea of Estonia as a small state is also a recurring theme of research on Estonia. Researching Small Nations has been a growing academic field in the humanities in recent years. Since the early 2000s there has been a growing interest in small nations and how they interact with the wider international system and their small and large neighbours alike (Hey, 2003). Balddachino & Wivel (2018) have expanded upon this research recently, and note that while small states might often be considered weak and dependent on larger states, they are also more agile and can innovate more easily than larger neighbours. They also argue that institutions matter far more to them than to larger states and that dilemmas that might seem trivial to larger states can take on an increased sense of urgency. Finally, they suggest that other notable dilemmas for small states include debates of nationalism/cosmopolitanism and influence/autonomy. These debates can all be evidenced in Estonia. The issue of nationalism/cosmopolitanism is evident in arguments where Estonia’s Russian minority is positioned as a perceived security threat, whilst debates of influence and autonomy can be evidenced in Estonia’s heavy commitment to western institutionalism (which is further explored in Chapter 7). Additional notable contributions to the field of small state studies include Thorhallsson’s (2016 & 2019) theory of ‘shelter’, in which he argues that small states are essentially constantly seeking shelter within the International System, and that shelter and the survival of the small state is essentially granted by larger states. This comes in the form of either accepted neutrality or alliance-building, whereby one larger state protects the smaller state from other menacing larger states. He concludes that small states must have the shelter of larger states if they are to ‘survive and prosper’ (2019: 16). Similarly, Bailes et al (2017) argue that alliances are vital for small states to thrive. How alliances are pursued is often diverse and can utilise different specialisations, including technology. This is evident in Estonia, which has been particularly active in building closer alliances with both NATO and the European

Union, and has utilised technology – particularly expertise in cyber security and e-Governance to further those close links.

The nature of the hybridity of the Russian cyber threat carries into official governmental recognition. Contemporary research has observed perceived Russian notoriety in this field, utilising sophisticated disinformation campaigns to further political and strategic goals, and suggested that virtual weapons are a persistent irritant to international order (Mäliksoo, 2018: 378). The Russian government occasionally takes great glee on its social media outlets and in political statements in suggesting and ridiculing the idea that Russian disinformation even exists, let alone is as powerful as its opponents often suggest (*RT*, 2020). The general Russian stance, which is frequently perceived as both dismissive and aggressive by western nations has bred nervousness in the Baltic states. This has led some scholars to muse on whether Narva might be the next Crimea, given its similarly large Russian-speaking population, and also its proximity to the Russian border. Yet this is highly unlikely whilst Estonia is both a NATO and EU member (Trimbach & O’Lear, 2015; Kasekamp & Dahl, 2016). There are considerable NATO forces in the Baltic region, including a sizeable British regiment in Tapa, to deter any of the tactics that emerged in Crimea, that took under-prepared Ukrainian forces by surprise (Toal, 2017). ‘Hybrid warfare’ has been a term popularly coined to refer to Russian tactics in Eastern Ukraine in particular and has been thought to feature multiple factors including non-uniformed troops, the exploitation of a weakness in civil society, cyber attacks which feature disinformation and disruption (Lanoscka, 2016). These weaknesses are not as obvious in Estonia. Furthermore, as a NATO member, any perceived attack on the Estonian state would trigger a response by all NATO members.

This narrative of Russia as a threat has a continual, unifying effect on Estonian society, as whatever the Estonian government of the day does, it is considered preferable to the fear of domination from its neighbour (see Crandall & Allen, 2015 and Gold, 2019 for more on Estonia developing a niche geopolitical narrative). A parallel unifying effect can be seen in Russia. Some of the ideological basis of Putin’s foreign policy goals are drawn from the narrative of Russia facing an existential crisis, of Russian speakers being under threat in the ‘near abroad’, and the perceived menace of NATO expansionism into the Russian sphere of geopolitical influence (Leichtova, 2014, Toal, 2016). The protection of Russian speakers in former Soviet nations forms part of Putin’s foreign policy. This understandably generates anxiety in Estonia and also in neighbouring Latvia, given how such policy has been enacted in Eastern Ukraine and Crimea.

Crucial to all of this is the potential of plausible deniability of state-level involvement. Russian state-controlled news outlets, as well as official governmental sources, such as the particularly undiplomatic Russian Embassy UK Twitter account (@RussianEmbassy), frequently extol the lack of proof as a means of casting doubt upon accusations of Russian cyber interference, as well as frequently sarcastically mocking any negative news stories as being the fault of mythical Russian hackers. The Russian Embassy of Estonia account (@RusEmbEst) frequently shares the tweets of other embassies as well as state-sponsored news outfits such as Sputnik, pushing Kremlin-backed foreign policy. Capitalising on the problem of attribution being difficult within cyber contexts, these accounts are used to spread doubt and

question dominant western narratives, which invariably are labelled ‘Russophobic’. Whilst it is arguable that ‘cyber war’ is indeed a genuine threat (Rid, 2012 & Valeriano & Maness, 2015), it is clear cyber security issues can destabilise and disrupt international relations, geopolitics, and domestic politics alike.

2.8 Development, Dependency and Trust

Existing research has suggested that Estonia is increasingly reliant upon digital services (Crandall, 2016; Kalvet, 2012). This was exposed by the 2007 cyber-attacks, but Estonia has not sought to cut its digital dependency. Conversely, it has progressively increased its connected services, to a point where it is widely accepted that virtually every public service is available online (with a couple of notable exceptions, such as marriage). These have been developed and introduced over time, and over time there has been a gradual increase in service use (Solvak et al, 2019). Indeed, in the 2019 elections, a record number of voters cast their votes digitally (ERR, 2019). Fundamentally, this is due to a record of trust, as well as geopolitical stability which has allowed for investment in critical infrastructure, which is now tried and tested (Adamson, 2019). e-Estonia has been developed and enhanced over time by successful service adaption, generally after a ‘trial and error’ process (Drechsler, 2018). Critical research has suggested that such a ‘trial and error’ approach has been to the detriment of sections of Estonian society, or that indeed Estonia has cultivated ‘moral e-citizens’ and those that do not conform to established, digital behavioural norms are left with limited options for alternative interactions with the state (see Drechsler, 2018 & Björklund, 2016 respectively). Digital services are thus fundamental to everyday Estonian lives and there is, therefore, a link between the everyday and the state in a cyber sense.

In recent years, Estonia and the United States have become members of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications Security in the Context of International Security. One area of mutual concern is how to promote collaborative cyber security resilience. Estonia has recently sat at the United Nations Security Council as a non-permanent member (2020), presided over the EU Council (2017), and acted as co-ordinator for the Nordic-Baltic 8 (2020). Through this international outreach, Estonia has sought to advance its role as a technological soft power (Hardy, 2020) and cyber norms entrepreneur (Adamson, 2019). Research on Estonia can further highlight the challenges faced by small states, particularly in the field of cyber security and e-governance, illuminating experiences applicable to other small and large nations. Estonia maintains important relations with others and strategises at regional, European, and global scales respectively.

Geographers and other social scientists tend to distinguish between regional as a sort of geographical container – i.e. something territorial grounded, networked, and relational. ‘Regions’ are made through social relations and co-entanglement with others (Paasi, 2003). In the case of Estonia, ‘regional’ can be conceptualised as cooperation with its Baltic partners, and also with its Nordic neighbours. The Baltic states cooperate frequently on a regional level, in the Baltic Assembly, as well as within the Nordic-Baltic 8. Both are regional formats, which provide a format to find com-

mon cause and cooperation on international concerns. All political decisions taken are non-binding, but the formats are considered beneficial, and meetings are regular co-ordinate strategic approaches to international challenges.

The potential for regional cooperation to enhance more formal security decision making has been noted in existing research (Browning & Joenniemi, 2004), yet the potential for cyber security cooperation and integration is relatively unexplored. One of the analytical chapters of this thesis (chapter 8) argues that such regional cooperation can be highly beneficial and draws attention to the work of the Nordic Institute for Interoperability Studies, which is currently responsible for coordinating the successful integration of the X-Road platform between Estonia, Finland, and Iceland – an initiative which is arguably a digital region-building project.

Existing small state research has long suggested that small states band together, around shared mutual interests, or with larger allies for their continued security (see Thorhallson 2006, 2012 & 2016 & Bailes et al, 2016, for the further contextual basis of this within Europe, and the United Nations). Meanwhile, small state cyber security research is limited thus far, however, Burton (2013) suggests that geographical proximity is not crucial to such cooperation, noting New Zealand's collaboration with the UK and NATO in the realm of cyber security. This argument generally holds that globalisation and cyber space have rendered such regional cooperation redundant. Yet it does not consider the human aspects of cyber collaboration fully. New Zealand might well make a logical partner for the UK for social and cultural reasons, as well as commonly shared, perceived threats. In this regard, geography, and geopolitics are both a consideration.

Regarding Estonia's role in European security, Estonia is said to seek close relations with European partners and to expand its influence at the European level through socialisation in cyber security and e-government (Crandall, 2015 & Hardy, 2020) For Europe meanwhile, the establishment of norms as well as governance and systems are seen as key to Europe's 'cyber power' (Cavelty, 2018). However, it is vital to acknowledge that power is multifaceted and complex, and how it is wielded varies greatly. The European Union has generally focused on building resilience from risk, as opposed to developing great offensive power, and priorities have included the empowerment of citizens in the digital sphere as well as a focus on building norms among members (Cavelty, 2013). Estonia has been particularly active in seeking to shape those norms (Adamson, 2019). One of the more notable, European level cyber security, and specifically privacy achievements, has been the implementation of the GDPR (general data protection regulation) which, implemented in 2018, has made businesses operating within the European Union meet specific standards of data protection. This is arguably a flagship policy and has been hailed as powerful enough to 'change the world' and one of the most ambitious attempts to protect consumers and citizens rights (Albrecht, 2016). The failure of businesses to comply with these strict criteria is punishable by considerable fines. Concerning this study, it is noteworthy that Estonia used its presidency of the European Union to continue to push its agenda of cyber security, e-governance, integration, and common standards and norms (for more information, see eu2017.ee & Papp-Váry, 2018). This is reflected upon within later analysis, as an additional illustration of cyber security and e-governance as a means

of Estonian cyber power, as defined by Nye (2009), who argues that the deployment of soft and hard power techniques can simultaneously achieve foreign policy goals, and that ‘cyber power’ can be achieved through both.

Meanwhile, at the global level, Estonia is a very small power. Global cyber security is a complex phenomenon, and the primary challenges include the attribution of attacks, and the existence of malicious actors who would subvert the international order, (who exist on both a state and non-state-level) (Kello, 2017). They also lie in the proliferation of connected devices, the growing diversity of threats such as disinformation and sabotage, to even the existence of drones and other semi-autonomous machines, which disrupt the digital and non-digital spheres alike (Rid, 2016). Much existing research attempts to theorise the global security order in terms of cyber security. These have tended to focus on the potential disruption of global order (Buchanan, 2016) the advent of cyber war and deployment of cyber weapons (Rid, 2015) the projection of power, and the sovereignty of data (Betz & Stevens, 2013), and the complex relationships between the public and private sector (Kello, 2017). These large-scale theoretical explanations are overarching. Nevertheless, it is possible to extrapolate lessons to Estonia on a limited, and case-specific basis. The analytical chapters of this thesis focus upon ideas of trust, disinformation, e-governance, human error, disruption, anxiety, and fear. The lesson to be extrapolated from these specific narratives might be of human-centred, and constructivist, localised variances. This is discussed in an ongoing manner throughout the thesis.

Estonia as a small state acts as many other small states do, and seeks alliances and larger allies as a form of ‘shelter’ within the international system (see Thorhallsson, 2018, and Bailes et al, 2016). Since independence, Estonia vigorously pursued an internationalist agenda, seeking alliances with the West in the immediate aftermath of the Soviet Union’s collapse (Berg & Ehin, 2016). This has continued entirely uninterrupted until Estonia’s most recent election, held a month after the final interview of this thesis was conducted, in March 2019. This election saw the emergence of EKRE, a nativist, far-right party whose positions have been noted to include anti-immigration, Islamophobia, and sympathy for Neo-Nazism (Braghioroli, 2019). EKRE more than doubled their vote share and their seats in the Riigikogu (the Estonian Parliament), leading to a coalition being formed with them by the governing Keskarakond (Center Party, a centrist political party traditionally favoured by Estonia’s Russian speakers who sit within the ALDE liberal wing of the European Parliament) and Isamaa, an economically liberal-conservative party, created from a merger of two similarly minded conservative parties: Res Publica and Pro Patria. As of early 2021, this government has now collapsed, and the damage it has caused is yet to be fully assessed, although early analysis has suggested it has harmed Estonia’s international reputation as well as caused domestic ruptures. In particular, it has furthered an existing urban-rural divide and fostered grievances among those who feel ‘left behind’ by the direction of modern Estonia (McNamara, 2021). Additionally, EKRE, while now out of government, still have a strong electoral and polling position.

This modern cleavage has been something of a departure from the consistent, centre-right, technocratic governance that has been seen to define Post-Soviet Estonia, which some critics blame for the current rise in populist sentiment (Kattel, 2020). The nativism which EKRE exploit has been simmering for some time (see Petsinis, 2015) and Estonia’s identity politics have consistently tapped into identity-driven Ethnopolitics (Petsinis, 2019) as much as they

have pushed the internationalism of e-Estonia. Arguably the two have been a house of cards for some time and the balancing of nativism with technocratic internationalism was inevitably going to lead to controversy or a clash between what modern Estonia should be (Kattel, 2020). Estonia has used its e-governance and cyber security expertise to foster public trust in institutions. Kattel & Mergel (2019) argue that Skype was huge in building trust in Estonian technological expertise. Its founders, coming from working-class backgrounds, also provided an advert for how Estonians could benefit from technology, and how private sector innovation, in particular, was trustworthy and a platform for Estonians to market themselves to the world.

Kattel & Mergel also argue that Estonia's digital success has also been shaped by a convenient convergence of history and context, namely both events such as private citizens creating Skype, but also historical context such as the Soviet past, which created an acceptance of a governmental oversight (or what they call a 'guiding hand'). However, they also note that the introduction of key governance principles, which gave citizens a degree of ownership of the e-State, was key to ensuring trust in e-Estonia's institutions. This can be evidenced in the Küberkaitseliit (Estonian Defence League's volunteer-driven Cyber Unit), which asks for patriotic technology experts to volunteer their time to help fortify their nation's cyber defences (Kaitsellit, 2019).

Existing research has also suggested that public trust is central to the functionality of e-governance (Jun, Wang & Wang, 2014) that operates on the basis of a consensual relationship between citizens and government institutions. Many conclude that Estonia has been relatively successful in building this trust, such as Runnel et al (2009) who note the country benefited from a boon of 'soft' or more 'idealistic' values in the period before and immediately after independence, and that a period of national awakening created a boon of trust in both national institutions but also the private tech industry. However, even in 2009, Runnel et al noted a failure to restructure the economy appropriately as a potential problem for Estonia going forward. Those failures, at least in some small part, can be seen to have fuelled the grievance agenda that has driven EKRE as a political force and disrupted the Estonian house of cards, finely balancing nativism with technocratic internationalism. This clash, along with the 2019-21 coalition government, has led to declarations of nervousness from those within Estonia's tech industry (Duxbury, 2020) concerned that Estonia's internationalist image was now tarnished and that this could harm international recruitment.

Trust is integral both to Estonia as a state but also to e-Estonia. Yet the type of trust involved is inherently different. One is borne of patriotism, yet another functions based on informed consent and active trust-building. Until recently, Estonia and e-Estonia could not be considered at odds. Yet as times change, so do politics. Chapter 6 in particular explores these concerns in further detail.

2.9 Conclusions

This chapter has sought to illuminate how Estonian cyber security concerns reflect wider geopolitical narratives. From the extensive literature assessed by this chapter, it can be concluded that the common cyber security concerns of Estonians can be seen to be informed by multiple factors, including Estonia's modern history (both Soviet and

Post-Soviet) and Estonia's smallness. It has also been argued that contemporary geopolitical narratives are crucial in shaping perceived cyber security threats, much as they influence non-cyber threat perception. The chapter has also highlighted the importance of trust, noting Estonia's high levels of trust in governance, and how this extends to e-Estonia and notably to Estonia's ubiquitous e-governance. In this regard, digitalisation is seen as a means to preserve trust in the state but equally represents a risk.

This chapter has also highlighted that Estonia and e-Estonia are, at times, in competition with or contradict one another. e-Estonia, since its inception, has been an internationalist, neoliberal project concerned primarily with service provision, albeit with some notable, human-centric features for citizens. While Estonia and e-Estonia do converge in many policy areas such as conventional and cyber defence and the narration of a common international adversary – Russia – domestically there are political movements, such as a rise in populist right sentiment, which are at odds with e-Estonia. As Baldacchino & Wivel (2019) note, small states often need to choose between nationalism and cosmopolitanism. The latter was undoubtedly the choice of every Post-Soviet Estonian government up to 2019. It remains to be seen if this approach is the will of the Estonian people going forward.

For the purposes of this chapter and the wider thesis, it is crucial to ascertain what we can infer from this research and the wider implications for Estonian approaches to cyber security and e-Government. To establish the value of this, the research should have both conceptual and contextual value. Whilst the conceptual value (grounded within existing geopolitical and security research) is established in Chapter 3, the contextual contribution is addressed in this chapter. Namely, what is the value of an Estonian case study, which body of existing literature and knowledge does it provide a unique contribution towards, and also is there a more wide-ranging contribution beyond this? Whilst both the introduction and Chapter 3, to some extent, establish the author's position as to why Estonia matters, this section aims to establish further how the study of Estonia can enlighten wider debate in both cyber security, regional and international security debates.

3. Cyber Insecurities, Ubiquitous Connectivity & the Sociotechnical

3.1 Introduction

This chapter explores some of the conceptual ideas behind the thesis, and seeks to answer the question: *How are everyday cyber insecurities linked to sociotechnical relations?* In order to answer this question, this chapter conducts a comprehensive literature review of existing conceptual research focusing on the idea of security itself, cyber security, information security, everyday security, and the sociotechnical. The chapter argues that everyday cyber insecurity and sociotechnical concerns are urgent and growing areas of enquiry due to the growing ubiquity of connected services and devices within everyday life, particularly in Estonia, given these devices are used to access the ubiquitous online governance systems.

The chapter establishes the theoretical basis of ‘sociotechnical’ and ‘everyday’ security research and its relevance to this project. The chapter subsequently discusses the merits of different approaches to complex interdisciplinary concepts, including assemblage (see Dittmer, 2016 or Collier, 2018), and hybridity (Mälksoo, 2018 & Lanoszka, 2016) as useful theoretical vehicles to better understand the complex relationships between human and non-human actants. The chapter goes on to argue that connected devices and broadened ideas of what cyber security entails are crucial in understanding how e-Estonia is secured. It argues that the sociotechnical and the everyday are inextricably linked due to the complexity of contemporary challenges. Consequently, insecurities are complex, and closely linked to devices and mundane interactions, but also informed by politics and geopolitics.

3.2 Security and the Sociotechnical

Security is a fundamentally contested, and vitally important concept. It has been noted that it is impossible to make sense of world politics without it (Williams, 2013). Yet security is more than a vehicle through which to make sense of the power politics of international relations. Security, it has been suggested, is primordial (Booth, 2005), rights-based (Mitzen, 2006), community-based through narrated, shared commonalities (Giddens, 1991) grounded within rights and ethics (Browning & McDonald, 2012) a maternal relationship between protector and protected (Neocleous, 2007) and derivative from wider social and cultural phenomena. (Vaughan-Williams, 2011). Intrinsicly, security is interdisciplinary. It is not owned exclusively by one academic discipline, but rather shaped and moulded by multiple factors. A central tenet of much security logic is the assumption that there must always be something tangible to be protected, often termed the referent object (Cavelty-Dunn, 2009). Frequently, data or hardware is treated as the referent, although this is being progressively challenged. It has been noted that people are frequently the greatest threat to information security (Von Solms & Van Niekirk, 2010). Yet, this has been countered by Adams & Sasse, who rebutt such claims, arguing that users are ‘not an enemy’ to be countered, but instead a vital aspect of security solutions, to be understood and appreciated (Adams & Sasse, 1999). Increasingly it is argued that research should be

attentive to the socio-historic factors that influence how we perceive risk within an information security context (Hall, Heath & Coles-Kemp, 2015).

Information security approaches are often neglected within wider social science research, although this is changing, as illustrated by work such as Hall et al (2015), Coles-Kemp & Hansen (2017), and Robinson & Martin (2017), which have shown closer collaboration between the social sciences and information security. As a discipline, information security has traditionally been interested in the protection of data and favoured approaching problems in a quantitative, scientific manner. Information security also is often driven by the principles of data integrity, availability, and confidentiality (see Whitman & Mattord, 2011). However, it has been argued this can neglect the social, political and cultural aspects of security (Bødker & Greenbaum, 1993). The following chapter subsequently seeks to explain some of the different approaches to security, a history of its development as a research area, and outlines contemporary developments.

New research has begun to focus more explicitly on the 'sociotechnical', i.e. the social aspects of technical objects and security processes (Coles-Kemp & Hansen, 2017; Malatji et al, 2019; Haddad & Binder, 2019). These social aspects include individuals' attitudes towards technology and the ways in which technology changes those attitudes. Haddad & Binder (2019: 131) argue that this 'nexus' between digitalisation and society requires further exploration and that the sociotechnical involves everything from 'careless users, unaware citizens... devices, databanks and vital infrastructures' and that these are all 'sites of potential harm and insecurity to society as a whole'. Digital-material objects have become more prevalent and researchers have drawn upon wider object-orientated philosophies and their development across the social sciences. Geographers in particular have noted the inherently material character of virtual spaces and have sought to explore how these increasingly complex relationships may be further understood (Kitchin & Dodge, 2014). The concept of 'technicity' has been suggested to be an appropriate vehicle of analysis, which is defined as the qualities of the co-constitutive relationships between the human and the technical (Kinsley, 2014: 366).

Sociotechnical approaches have been a growing area of theoretical research for some time. They may be broadly defined as 'the study of processes in which the social and the technical are indivisibly combined' (Vojinovic & Abbott, 2012). The connection between the sociotechnical and feelings of insecurity has been made by Volkamer et al (2015) who highlight the poor security relationships citizens often have with their phones. They argue that citizens frequently view their data as unimportant, and instead of that the device itself, rather than the data contained within, is the primary security risk. They also note that the poor usability of security software made research participants less likely to bother with appropriate security for their phones data. Sociotechnical studies into the diverse security challenges posed by ubiquitous e-governance are relatively in their infancy. Existing research in India has observed the 'transactional effectiveness' and 'service efficiency' benefits of sociotechnical approaches (Kompella, 2020), while Kosenkov et al (2019: 493) argue in their exploratory analysis that 'sociotechnical approaches provide a reliable basis for sys-

tematically responding to existing problems and challenges to e-governance'. However, there is a relative lack of existing work in this field.

3.3 Studying security: Varied Approaches

The origins of security studies are found within the field of International Relations, where the subject began as a sub-discipline driven by IR scholars concerned with the role of security in shaping International Politics. Perhaps the most influential school of Security thinking within this sub-discipline has been Classical and Neo-Realism. Classical realists argue the roots of their thinking can be traced back to antiquity, and that its reasoning is primarily driven by power politics (Williams, 2013). This neorealism was classically espoused by Kenneth Waltz, who argued that states live in a state of nature, and all act in their national interest, ultimately driven by their survival. As states cannot be sure of the intentions of other states, a lack of trust between them drives the security agenda in increasingly militaristic ways, as a means of ensuring their national security. Such beliefs hold that security is *of the state* and can only be achieved *by the state* through military power (Waltz, 1977) and that states live within an international, anarchical society (Bull, 1977). This influential strand of security thinking has long held the state as both the ultimate provider and guarantor of security. However, such approaches have been critiqued as too state-centric, and that security is more nuanced and complex than the protection of state infrastructure alone (Browning & McDonald, 2013; Booth, 2005).

Furthermore, realist interpretations of security itself hold it to be integral to world politics, the international system, and the nation state. This has received notable attention from classical scholars. Locke believed that states and governments were created by individuals to protect themselves from one another and that it was a fundamental principle and duty of governments to minimise conflict and protect their citizens from harm, thus forming a social contract. This drew upon the writings of Thomas Hobbes, who proposed a similar social contract, albeit with an absolute ruler or monarch, rather than a Lockean government. This consent to be governed, both Locke and Hobbes theorised, was given by citizens, to their ruler, in exchange for the guarantee of security. Hobbes theorised this power be placed in the hands of absolute rulers, whilst Locke argued that failure to provide such security gave authority to citizens to overthrow their rulers. Rousseau, another social contract theorist, on the other hand, suggests governments are sovereign and created individually by the people, for their people, and are thus socially and culturally shaped by said people. In this sense, Rousseau might be considered a constructivist (Der Derian, 1995).

However, it is vital to note that much of this literature and theory was not written in a time concerned with cyber security matters, and Eriksson and Giacomello (2006) note how realism has struggled to account for cyber threats beyond a strategic level, which does not account for the everyday realities cyber security challenges can pose. Waltz (1977) and Bull (1977) for example, had no comparable equivalent of a destabilising cyber-attack to theorise. They could not envision the ability of a smaller power such as Estonia to elevate its international standing through digital means. Realism is less able to theorise how smaller powers might disrupt the international order through cyber means as it is more theoretically rigid and primarily concerned with more conventional means of warfare – although some (Craig & Valeriano, 2018) have argued that the online world has been said to resemble the 'anarchical society' – a classic realist

interpretation of the world based upon Hedley Bull's (1977) argument that all nations live within a chaotic international society where the biggest and most powerful make the rules. Similarly, realism is less attentive to social and cultural factors.

Constructivism is a common, alternative approach to the study of International Relations, with wider influence in social theory, which suggests that nations will act in a way that is socially constructed and shaped by different cultural, social and historical contexts, which in turn inform individual national security logics (Browning & McDonald, 2011: 248). Constructivist security research has largely been shaped by International Relations scholars utilising constructivist social theory. Very broadly defined, constructivist theory approaches security from an assumption that security, as with politics, is shaped and informed socially, and is differentiated in different locations. In itself, security can also be an articulation of core values and a means of their protection (McDonald, 2012). Similarly, constructivist securities hold the notion that insecurity may also be a social, historical construct (Booth, 2005: 38). This approach, in turn, rejects realist security theories as being too much of a 'one size fits all' approach. Within a security context, this approach suggests that people are likely to address the same security concerns differently in different places.

When discussing security, we must also consider the power of liberal, and particularly neoliberal approaches. Security has been said to be a cornerstone of modern liberalism since the time of Hobbes and Locke (Barnett, 2015: 266) and liberal approaches to security countered realism before and until the 1980s. Debates raged between neorealism and neoliberal institutionalism to explain the security environment. (Floyd, 2007: 334) The collapse of the Soviet Union and the end of the Cold War bred alternative approaches in the search for defining and understanding security in the late 20th and early 21st century, leading to a period of neoliberal dominance. Neoliberalism is argued by Klein (2014) to encompass the 'privatisation of the public sphere, deregulation of the corporate sector, and the lowering of income and corporate taxes paid for with cuts to public spending' and is somewhat different to conventional liberalism but maintains some of the social aspects. The dominance of neoliberalism within western politics also shaped a new, neoliberal logic of security. This was in part a product to counter the negative, realist logic inherent within security thinking, which held that all were subject to the whims of the great powers of global politics. This neoliberal approach was attractive to smaller states, who alone (conventional realist logic suggests) cannot guarantee their own security due to their limited capabilities or resources and must seek to ally with others (Hey, 2003, Crandall, 2014, & Thorhallsson, 2016). Consequently, these small states sought to build closer security ties based on subscribing to a neoliberal logic of security that the alliances they sought to join demanded – for Estonia, this meant both NATO and EU membership.

These developments also fitted the foreign policy goals of the large western powers, who consolidated their power – and particularly America, who developed a hegemonic world leadership in the late 90s and early 2000s. During this time, Russia in particular suffered a traumatic fallout from the collapse of the communist regime – harsh economic reforms mired many in poverty and corruption was rife while state assets were sold off (Sakwa, 2017). A common critique of neoliberal security logic is that it is simply another way of securing western interests on a global scale, or in-

deed that it is driven by the whims of capital rather than the interests of those it is supposedly securing (Neocleous, 2007 & 2016). This approach came to characterise the post-cold war era, but its theoretical grounding has much earlier origins. Immanuel Kant's model of 'Perpetual Peace' considered the growth of liberal institutionalism and the spread of democratic society. According to Kant, the only acceptable form of governance is a 'democratic, republican government'. He argued that perpetual peace would be achieved through global liberal governance, as liberal democracies are inherently predisposed not to make war upon one another (Williams, 2013).

However, as with some of the critiques of neorealism, neoliberal security is similarly critiqued for its one size fits all approaches to security. Recently, liberal institutionalism has come under increasing threat. The election of a NATO sceptic to the White House⁶ and indeed the Brexit movement in the United Kingdom is seen to threaten the order of institutions such as NATO and the European Union, once seen as vital guardians of alliance/collective security (McNamara, 2017). This might be seen as a return to the origins of security, often characterized as inherently conservative, protectionist, and self-interested rather than collective (Huysmens, 2002). Conversely, it has been suggested that liberal security logics have also allowed more in-depth consideration to develop of the human, the political, and the cultural aspects of security (Nunes, 2012: 346) and that some of the critical and human approaches which have emerged in recent years have grown in response to the era of neoliberal hegemony.

One notable departure from the conventional neorealist / neoliberal security paradigms has been the turn to human security – a human-focused critique of the failure of states to provide for the well-being of their populations. Human security may be conceived as an attempt to reformulate security beyond basic physical survival, with its focus on the rights and needs of people set within a universal human rights-based framework (Browning & McDonald, 2011). Thérien (2012) argues that human security means the protection of a 'way of life', i.e. the perpetuation of a particular set of customs and beliefs. Human security thinking developed primarily in the post-Cold War era, a time defined by NATO expansion and neoliberal hegemony. A notable contribution to human security thinking was the ideological embrace of humanitarian intervention (Wheeler, 2000). This was institutionalised, to some extent, in the United Nations charter as 'The responsibility to protect' (Bellamy & Wheeler, 2008). However, such interpretations have also been seen by some as merely an extension of neoliberal security logic and the attempted implementation of universal (western) security logic (Sparke, 2006 & Morrissey, 2011). The logic of humanitarian intervention was deeply damaged by failed interventions by western powers, leading to considerable public backlash in both the west and indeed those nations affected. Other powers such as Russia expressed doubts and later hostility as to how humanitarian intervention by the western powers morphed into calls for regime change (Sakwa, 2017). The Syrian crisis might be interpreted as an example of western powers and Russia clashing over when and how to intervene in a worsening civil war and regional security crisis. Meanwhile, Russian interventionism in South Ossetia, Georgia, is often justified by the Kremlin as a parallel event to western interventionism. These events continue to cast a considerable shadow over Russian geopolitical reckoning and strategic thinking to this day. (Sakwa, 2017 & Toal, 2017).

⁶ US President Donald Trump has repeatedly attacked NATO allies for not fulfilling their spending commitments, and bemoaned the United States unfairly shouldering the burden for the alliance financially

There is an argument that western Interventionism has made Somalia, Libya, and Iraq arguably less secure for normal citizens than ever (Peoples & Vaughan-Williams, 2014). This argument is also made by the Kremlin, with President Putin himself arguing that the events of 2014 Ukraine were driven by ‘western interference’ in Ukraine’s domestic affairs that led to the Maidan ‘coup’ which overthrew a democratically elected government (Putin, 2021). This argument can be expanded to claim that despite the stated emancipatory goals, ‘interventionism’ has successfully hijacked by a western-dominated, neoliberal security agenda that is more about geopolitics than the advancement of human security. It has been noted by Kremlin critics that Russia utilises this argument to justify its own geopolitical actions, yet often also lacks the consent of the parties it is supposedly fighting for (Kuzio, 2019 & Galeotti, 2020). More holistic interpretations of security might instead be more beneficial, drawing upon the everyday experiences of citizens, as opposed to those driven by larger geopolitical agendas. Critics have long suggested that human and national security have an uncomfortable coexistence (Hudson, 2005: 155). This can be evidenced in the dominant human security logics that came to define the immediate post-cold war era, which have led to the development of securities of exception. Such arguments of exception suggest that ordinary norms can be suspended in favour of moral interventionism. This might be notably characterised by the US/UK-led invasion of Iraq in the early ‘00s, which ignored the norms of international law in favour of a moral argument for removing a tyrannical dictator. This was then extended to arguments of development – such as building a better life for the Iraqi people (Peoples & Vaughan-Williams, 2014 & Morrissey, 2011) It has been argued that to make human security fit for purpose, more radical approaches are needed, which go beyond the above examples of neoliberal-driven security projects. These radical approaches can highlight areas where there is a disparity between citizen concerns and elite security agendas, and through an increased focus on everyday life we can bring to light the fundamental social aspects to cyber security (see Hyndman, 2008 and Peoples & Vaughan-Williams, 2014)

An additional key security concept developed in recent years by the Copenhagen School of security studies has been that of ‘securitisation’. Securitisation, roughly explained, is the process whereby a particular issue is subject to intense public interest, and due to emotive discourse surrounding it, is consequently depoliticised as a matter of consensus, thus rendering it beyond perceived reasonable discussion and subject to the political move of claiming it as a security issue. The political move typically takes the form of a speech act that thus creates a social construction of security⁷. A contemporary example might be the debates surrounding terrorism which have come to characterise mainstream security debates in the past decade. Compared with many security issues, terrorism has received disproportionate focus and intense public debate for what is, fundamentally, an unusual and infrequent occurrence when compared to other security threats. Yet, as the discourse around terror attacks has been so heavily securitised, non-normative approaches are stifled (Buzan & Wæver, 2009). This has fundamentally changed both how we think about, but also how we discuss (or rather do not discuss) security concerns relating to the causes of terror attacks are frequently attacked as being ‘soft’ on terrorists (Jackson, 2013). Further studies utilising securitisation theory as a theoretical

⁷ See Wæver, 1993 for the original conceptualisation as above, as well as Browning & Joenniemi, 2016 for ontological security debates, and Mälksoo, 2012 for a contemporary debate on securitisation of the Soviet past

vehicle have explored the deep securitisation of non-Jewish Israeli citizens (Abulof, 2014) and the securitisation of historical memory of contentious events (Mälksoo, 2012 & 2015). Of critical influence is Hansen & Nissenbaum's (2009) research on the securitisation of cyber security that explores the 2007 Bronze Soldier 'cyber war' on Estonia. Contextually, given Estonia's digital dependence and reliance on the e-state, the 2007 Bronze Soldier attacks took on special significance and obtained a securitised narrative. Furthermore, Hansen and Nissenbaum (2009) note that this narrative was deployed with great effect internationally, alongside geopolitical narratives which cast Russia as menacing to cyber security, and also Russian-speaking Estonians as a menace to security within Estonia domestically.

Critical scholars have been intensely critical of this process of securitisation, arguing that it only serves to limit debate around matters which are intensely and inherently political, and is an intense political solution that only serves to benefit 'the few' (Floyd, 2007: 342). Securitisation consequently has the power to project previously neglected issues to prominence through the suggestion of imminent emergency (Buzan, 2007), and a process where issues are made into matters of security. This, it is argued, places them 'above' politics, and makes exceptional state interference acceptable (Barnett, 2015). Further geopolitical research has also been critical of how this process leads to an opportunistic suspension of the rules and standards of democracy, creating an ongoing public culture of emergency (Neocleous, 2007 & Amin, 2012) and the institutionalisation of expeditious decision making (Aradau, 2008).

To address some of the concerns elaborated above, some scholars have chosen to adopt more radical ways of thinking that challenge hegemonic, neorealist, and neoliberal security thinking. Thus, we have witnessed a critical turn perhaps best illustrated by 'everyday security' as a means to challenge powerful narratives by empowering everyday voices (Vaughan-Williams & Stevens, 2016). Much critical security thinking has responded to the perceived erosion of civil liberties and freedoms neorealist and neoliberal securities have been responsible for (Morrissey, 2011). Arguably, both neoliberal and neorealist securities have been built upon a perceived consensus that there is a balance struck between individual freedoms and the quest for security. The oft-quoted and infamous Benjamin Franklin quote - often utilised when addressing matters of securitisation - of '*Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety.*' frequently serves as an inspiration to both critical security thinkers and libertarians alike. Social contractism, (whether the Lockean, Hobbesian, or Rousseauian interpretation), shares a roughly similar premise, and there is an implicit assumption underpinning the idea of the social contract that individuals accept the trade-off between liberty and individual safety (Der Derian, 1995). Consequently, critical security research has sought to dismiss this willing relationship, and the notion of balance as a 'myth'. Some go as far as to condemn the idea of security in itself, dismissing it as a product of neoliberal ideologies (Neocleous, 2007) whilst others have suggested that security itself only makes sense if individual human beings are the referent (McSweeney, 1999: 208).

As a general tone, critical security research has hence sought to make *emancipation from* security its chief concern. The core contentions of many is that only through *emancipation from* the core concerns of orthodox security, can true security be achieved (Vaughan-Williams, 2010 & Wyn-Jones, 1999). Whilst Neocleous rejects the very idea of secu-

ity, most critical researchers are in fact rejecting the process of securitisation. This might be evidenced in a shared commitment toward the re-politicisation of security (Wyn-Jones, 1999; Neocleous, 2007, Nunes, 2012). This stands in stark contrast to the process of securitisation, which is supposedly a fundamentally de-politicising process, in that it takes matters, presents them as matters of security, and thus makes them beyond political discussion, as they are instead a security matter. This, it has been argued, can lead to human-focused, ‘everyday’ solutions (Stevens & Vaughan-Williams, 2016).

3.4 Cyber security, Sociotechnical Interactions, and the Everyday

In the interests of this project, it is important to define the term ‘cyber’. The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) defines cyber as “Relating to or characteristic of the culture of computers, information technology, and virtual reality” (CCDCOE, 2017). The origins of the term are believed to be drawn from the idea of cybernetics, which in turn borrowed from ancient Greek terminology concerning governors and government (Unwin, 2014), and was further popularised by William Gibson’s science fiction novels such as *Neuromancer* and *Count Zero* (1982 & 1984). Whatever the origins of the term, it rose to prominence in the post-war era in relation to machinery. Now it is commonly used to discuss connected devices. It has also been suggested that this tendency to prefix ‘cyber’ in front of terms, creating terminology such as “cyberspace” and “cyberwar” has been a cynical process to make processes seem more tech-savvy and edgy, as the world came to terms with the increasingly ubiquitous computing in modern society, and has led to a rather lazy grouping and overuse of the term (Graham, 2013 & Rid, 2016). Others have preferred to utilise different terms, such as ‘digital’ or ‘augmented realities’ (Rose, 2016, Graham, 2013, Ash et al, 2018). However, if picked apart, we could come to similar conclusions that these terms are used interchangeably for modern digital technology.

Given this criticism, why does this project use ‘cyber’? A chapter could be spent discussing the relative merits of ‘cyber’, as opposed to ‘digital’. Whether we should discuss ‘data’ or ‘the technical’. This research uses ‘cyber’ primarily due to the ubiquity of the term. Rightly or wrongly, ‘cyber’, ‘cyberspace’ and ‘cyber war’ are widely recognised if often misunderstood. They appear in governmental legislation and in the terminology of private companies alike. Quite simply, despite considerable academic resistance to the term, it has stuck within the wider global public conscience. As this research concerns itself with the ‘sociotechnical’ and everyday interactions, it consequently makes sense to use a term with which the public is most likely to be familiar. ‘Cyber attacks’ and ‘Cyber warfare’ are also firmly embedded in the public conscience and popular culture. A recent season of the popular Netflix TV series *House of Cards* (2013-2018) featured a ‘Cyber’ attack, which amongst other things, caused a train to derail. The Andy McNab novel *Firewall* (2000) features a ‘Cyber’ war. These might all be considered contributory to a wider culture of ‘cyber’ as a term. Shires (2020) notes how cyber security in popular culture is frequently depicted as unknowable and inherently sinister, involving shady actors behaving in an unethical manner. Furthermore, he argues that these popular culture depictions of cyber security actors as operating in morally dubious ways consequently shape real-world actions in a negative way, and can embolden or encourage questionable behaviour and attitudes among cyber security professionals. Popular culture is suffused with references to dramatic events involving critical infrastructure breakdown and the threats

posed by cyber warfare (Shires, 2020). Even long-standing movie series such as the *Die Hard* franchise has been updated to take into account the changing capacities of criminals to wreak havoc on digital societies. One research participant (Participant N) even cites *Die Hard 4* (2007) as an example of cyber attacks and hacking in an interview conducted for this thesis.

The advent of a vast swathe of new technologies and the growing big data revolution has led to an increased interest by geopolitical scholars in the cyber. Many scholars claim we are in the midst of a 'digital turn' within the wider humanities (and particularly within geopolitics), with research citing the ability of many new technologies to transcend and remake space (Ash et al, 2016 & Graham, 2013). One key development relating critical geopolitics to digital technology has been the evolving role of ethics and responsibility in the digital world (Jackson & Valentine, 2014). This has led to an academic inquiry in the area of governmental surveillance, infrastructure, big data, and the creation of networked or 'coded spaces' (Kitchin & Dodge 2011; Zook & Graham, 2007; Cohen, 2007). This research has contributed to the changing conceptualisation of 'cyberspace', a term which has become slightly less fashionable following earlier research, and wider enthusiasm for an imagined, otherworldly space. This is problematic in terms of the law but also misses vital material components without which an imaginary cyberspace would not function. Without material storage, devices, or human to operate those devices, there can be no cyberspace. Upon reflection, John Perry Barlow's 1996 declaration of the independence of cyberspace has been superseded by more contemporary sociotechnical work outlined above (Barlow, 1996).

Cohen (2007) suggests that 'cyberspace's' use as a space-based metaphor for the supposedly virtual cyber realm has fallen into disuse, it may be resurrected as a term to make sense of emerging networked spaces inhabited by users. The cyber increasingly affects everyday lives and shapes society and lived spaces. Human Geographers have explored these spaces, coining them 'Digiplace' or 'Code Space' (Zook et al, 2004 & Kitchin & Dodge, 2011) respectively. Their arguments suggest that the 'digital', or 'code', is generative of different spaces, and transforms society. Additional research has also discussed the airport as one such site, where spaces and mobilities are tightly controlled through coded space (Adey, 2009).

We are seeing the emergence of ever more 'everyday' coded spaces. The Uber taxi, for example, is an everyday space created entirely by digital means. The user enables this space by ordering a car through the Uber application on a smart device. The Uber taxi consequently becomes a distinctly material form of cyberspace. Concerns of Uber have been linked to a wider concern of data security, and in particular, the location services which exist and operate constantly within the application. There is also a human security aspect to using the Uber service. We can consequently see the emergence of security which is both material and digital alike, where one concern is tied to another. Existing research has sought to outline the security and ethics of these sociotechnically created interactions (Kamais, 2019) as well as highlighting the exploitative economics of these new spaces (Graham, 2020).

It has also been argued that there is no longer a clear separation nor a singular merged entity of the social and virtual spheres (Valentine & Jackson, 2014: 201). Instead, there exists a complex assemblage: a hybridity forged by multiple actants, both human and non-human alike. The conceptualisation of ‘cyberspace’ as a separate realm is increasingly dated, as demonstrated by existing research which has highlighted the increasingly socially, culturally, politically, and materially embedded nature of cyber matters within our everyday (Hansen & Nissenbaum, 2009 & Ertan et al, 2020). The everyday, the cyber, the material, the social and the technical are all intrinsically interlinked (Amoore, 2018). Finally, it can be argued there is a power dynamic involved in the term ‘cyber’. As previously noted, the term is utilised by governments, and within popular discourse to describe potential cyber warfare. It is omnipresent in the security concerns of Estonia, the subject of the study, due to the nation’s embrace of digital technology, as well as its fearful relationship with neighbouring Russia (Crandall, 2014). However, it is relatively less cited in individual and everyday contexts. It is a powerful and emotive term, drawn from state-centric discourse. Nevertheless, despite its multiple interpretations, and the inherently state-centric nature of the term, it remains the most sensible and commonly understood terminology we currently have.

Some of the basic principles of ‘everyday’ cyber security might be drawn from the field of information security. Whitman & Mattord in ‘Principles of Information Security’ (2011) introduces many of the guiding facets of information security, and their utility to governments, businesses, and increasingly, to everyday users. They acknowledge the evolution of information security from computer security, and that security itself is the protection from danger. Information security, they subsequently define it, is the ‘protection of information assets’. The guiding critical characteristics of information are confidentiality, integrity, and availability of that information. Crucially, alongside hardware, software, data, procedures, and networks, they identify that people are a key aspect of information systems (Whitman & Mattord, 2011: 40).

Other information security scholars such as Martin (2017) have argued for a better understanding of how cryptography is increasingly relevant within contemporary society. Martin first establishes information security to be the protection of information and information systems, and then consequently argues for the everyday utility of cryptography, highlighting that cryptography provides many of the techniques which underpin information security technologies. Furthermore, and crucially, Martin notes that cryptography is increasingly everyday, as it is now deployed on devices found in the pockets of every consumer of technology, as opposed to in the past when it was largely a concern of governments (Martin, 2017: 4).

This leaking of security logics into everyday life is a key concern to many researchers who have sought to address this issue. The Copenhagen school suggest that security is, quite simply, ‘the pursuit of freedom from threats’ (Buzan, 1991: 18). The constitution of a ‘threat’ is variable and is discussed later in this chapter under the broader topic of security concerns (a concern is not necessarily always threatening, but might be a source of anxiety or unrest). To meet new challenges and to continue critical work, it has been suggested we need to radically rethink how we consider and approach the study of security (Vaughan-Williams, 2012). Previous normative conceptions of security have fre-

quently been object-oriented, i.e. something security itself is something tangible to be protected. The referent object is, most of the time, either infrastructure or data, not people. ‘National security’ very much emerges from these material visions of security, built upon the assumption that the state, or state infrastructure, is the referent (McSweeney, 1999). Meanwhile, it can further be suggested that ‘information security’ is very much driven by the idea of data as the referent (Coles-Kemp & Hansen, 2017). Security has always been an ‘essentially contested concept’, and even allegedly ‘timeless’ concepts such as national interests are always shifting, contingent, and ambiguous (Vaughan-Williams, 2010: 2).

Due to the ubiquity and everydayness of digital objects, we must consider approaches that are attentive to multiple and assembled factors that help constitute and reproduce everyday cyber securities. Adopting a constructivist approach that values social and cultural factors in the formation of security analyses is key, as well as an increased focus on the materiality of digital objects, and their potential to change security concerns in ways unexpected and unintended by design, as noted by Coles-Kemp et al (2018).

3.5 Critical Approaches to Cyber security

The growing securitisation of cyberspace is of key concern to many researchers, as well as how this can be challenged (Adey, 2009 & Hansen & Nissenbaum, 2009). Scholars have noted the growing list of exceptional powers granted under the guise of security, and how they increasingly apply to everyday citizens, leading to backlash such as the 2013 Snowden Wikileaks, highlighting abuses of governmental overreach in the digital sphere (Springer et al, 2012). Concerns of ubiquitous digital devices have inspired research regarding the utilisation of data and algorithms to produce ‘geographies of suspicion’ through the anticipation of uncertain future events (Amoore, 2009) whilst others have maintained a critical approach to the prospect of surveillance capitalism (Zuboff, 2015) and the utilisation of fear and capital to suppress public criticism (Amoore, 2009; Neocleous, 2016). Securitisation has been driven by the perception that dangerous actors may exploit vulnerabilities (Ackerman *et al.* 2006), thus leading to a fearful public (Pain et al, 2009).

A recent history of digital attacks has caught the public’s imagination. The cyber-attacks on Estonia in 2007, believed to have originated within hostile neighbouring Russia, were labelled as the world’s first cyber war. This cyber-attack, which effectively shut down a government, albeit for a brief time, served as a powerful reminder of the ability of a hostile neighbour to undermine the critical infrastructure of a nation via digital means (Warf, 2015: 90). Such an experience might be expected to influence the psyche of those who experience it (Graham & Shelton, 2013), and similarly contrast with those who have not. Yet cyber security need not be defined by such grand acts of supposed ‘cyber war’. Within an everyday context, for example, those who had been defrauded or had bank details stolen while using the internet will be more predisposed to being cautious of their everyday cyber practices in the future (Oravec, 2017).

The emergence of new cyberspaces (highlighted in the above uber case) poses fundamental questions about how we govern and secure the internet. The internet has been described as the largest experiment involving anarchy in human

history (Schmidt & Cohen, 2013) and a ‘Hobbesian wilderness’ by the Estonian President Toomas Ilves (Ilves, 2017). Geographical scholars have theorised cyberspace as an inherently public space or forum, to exchange and debate with others. This has been heralded for its emancipatory potential, given the inherently non-hierarchical nature of the internet (Valentine & Jackson, 2014: 201) but has the potential to unravel in a chaotic fashion. Issues such as cyber-bullying and the potential of the internet to act as a conduit for extreme views have become key concerns (Jackson, 2009). This sense of ungovernable lawlessness somewhat reflects IR scholar Hedley Bull’s “Anarchical Society” that he theorised as reflecting the international system (Bull, 1977). Not only is this undesirable to states (who wish to maintain security and power within their borders) but it is also undesirable to everyday citizens, who desire certainty and security when they log onto their computers, utilise their smartphones or scan their smart cards (Barnard-Wills & Ashenden, 2012).

Suggestions that ‘cyberspace’ is unknowable, inevitably threatening, inhabited by unsafe actors, and thus makes us unsafe have come to pervade popular political discourse surrounding cyberspace (Barnard-Wills & Ashenden, 2012). The modern world and the security challenges we face are constantly evolving, as illustrated by the connected nature of the digital and the everyday. There is a growing interest in how these cyberspaces are made, maintained, and engineered to further political and security agendas. Other examples of social cyberspaces include the portrayal of enemies in video games, such as Call of Duty and its portrayal of the Arab or Russian ‘other’, along with the narration of Anglo-American ‘good guys’. It has been suggested these popular geopolitical stereotypes can be perpetuated through play, as players immerse themselves in cyberspaces that re-enforce and reproduce ‘potentially racist landscapes’ and ‘geopolitical narratives of dangerous others’ (Ash & Gallacher, 2011)

In a non-gaming context, CGI is increasingly used to create virtual spaces. Virtual environments may have an agency of their own, capable of evoking individual or collective memory. CGI can be used to create an evocative idea or feeling through ‘seductive architectural marketing’ which can be used to stimulate memories of traditional heritage (Melhuish et al, 2014). The digital has increasingly begun to play an important role in the production and dissemination of cultural objects, creating cyber-culture that can also be backwards-looking (Rose, 2016).

Conducting sociotechnical research requires an understanding of ontological securities, particularly within a cyber setting. Ontological security, as outlined notably by Giddens (1991) suggests that ontological security is the kind of security human beings feel when they have a stable state of mind. These mental securities are supposed drawn from stable relations with others, as well as a sense of continuity and common and shared identities (Mitzen, 2006; Giddens, 1991). This idea is drawn from everyday life but is shared for example within international relations. In the Estonian context, ontological security might be drawn from the membership of the European Union and NATO. Membership of these institutions can be interpreted as a form of reassurance to Estonian citizens and the Estonian state alike, who, as this thesis illuminates, frequently feel insecure about their relationship with neighbouring Russia. In a cyber sense, the idea of ontological security might invoke the peace of mind users of everyday digital material objects require when carrying out their mundane, daily tasks. It means a commitment to further investigate the human pro-

cesses which underpin many interactions and transactions within cyberspace. This might be achieved through challenging securitisation processes (Croft, 2012) as well as re-enforcing positive security values through raising awareness of the positive arguments of security (Roe, 2008). Similarly, making effective security manageable and understandable to users of technology (as per Dourish, 2012) will ultimately be beneficial to citizens, and invaluable to governments and citizens alike, due to the many devices that enable everyday sociotechnical relationships between citizens, devices, and technology.

These devices and interactions are an increasing part of everyday lives in the 21st century. The everyday, a concept that found favour with distinguished writers such as Henri Lefebvre and others, and is increasingly being addressed within the humanities and social sciences, as a way of making sense of power and socio-spatial structures. Stuart Elden's interpretation of Lefebvre suggests that "the concept of "everydayness" [quotidiennete in Lefebvre's native French] stresses the homogeneous, the repetitive, the fragmentary in everyday life' (Elden, 2004: 202).

Furthermore, for Lefebvre, space is produced through everyday spaces, in mundane locations, where 'unglamorous' interactions are the most important. He also argues that for historians, these forms of everyday knowledge are more revealing than sensational events (Lefebvre, 1991: 135) as with them, they bring a greater understanding of life at that time. Lefebvre's 'critique of everyday life' is written from his perspective as a Marxist sociologist. He theorises that the everyday is ultimately where capitalism reproduces and maintains itself and believed through more attention and critique of the everyday, its hegemony might be challenged. As a Marxist, he is predisposed to the critique of capital. He suggests that capital has effectively colonised everyday life, exerting increasing influence through consumption practices and the erosion of freedoms this causes, often through technological advances. Lefebvre was not writing about cyber security, but his theories of the everyday and the importance of the mundane and banal have inspired swathes of research across the social sciences, not only for their supposed revolutionary potential but also for a wider commitment of scholars to critique dominant practices, as might be evidenced in both critical geopolitics and critical security studies (Elden, 2004).

Whilst philosophical approaches might sometimes be considered abstract, a commitment to the everyday has driven a movement to challenge securitisation processes through the study of everyday security practices (Aradau, 2008); to question the role of digital material objects such as drones in everyday settings (Shaw, 2013); and to highlight linkages between national and global power structures associated with traditional security studies (although there is a recognised and intrinsic link between the two). This has been termed as 'big-S' and 'small-s' security respectively (Philo, 2012). One of the emergent ways of investigating such connections between national and everyday (or small-s) security has been through a renewed focus on material objects. Security research has all too often concerned itself with the security concerns of either nations or private companies, with the state, infrastructure, or data as the assumed referent object. Yet through a focus on everyday materials and lived experiences, geopolitical researchers, in particular, have highlighted the sociotechnical security assemblage visible in television shows such as *The Wire* (Meehan et al, 2013) that shows the interplay between humans, mobile phones (albeit not of the smart variety), CCTV cameras and

the affective qualities those material objects may have in certain everyday social scenarios (In the case of *The Wire* [2002-2008], in West Baltimore). Further research seeking to explore the everyday materiality of security has suggested security as an idea is encountered as specific objects and techniques, rather than as an overarching phenomenon. However, there are collective security affects, such as panic or excitement, which are amplified by the atmosphere of crisis that the idea of security creates (Anderson, 2015: 273-4, Pink et al, 2018). This further suggests an interplay between everyday securitised objects and wider security narratives.

Deciding what is, and what is not part of the everyday is of course fraught with theoretical and methodological concerns. What to some is everyday, is to others exceptional. Objects may be affective by design and thus emerge as securitising actants (Ash, 2015), yet they may also be entirely mundane, and potentially securitising through sociotechnical interaction and security narratives which are present within everyday contexts. Increasingly, security and cyber concerns are embedded within the everyday, and investigation of these concepts requires further attention.

The opening sections of this chapter have hoped to illustrate that everyday cyber securities matter. While existing research has explored security (often within IR or the more technical Information Security – such as Kello, 2018; Vol Solms & Van Niekirk, 2013; Ashenden & Coles-Kemp, 2018), the everyday (often within geopolitical and security contexts – such as Stevens & Vaughan-Williams, 2016), and the Cyber (within geographical and security research – such as Buchanan, 2020), an approach that addresses all three as an interdisciplinary project may be deeply beneficial. Sociotechnical approaches are imperfect, but they provide the best means available to access complex research areas such as the digital-material, security narratives, and security concerns (Malatji et al, 2019 & Haddad & Binder, 2019). Whilst this sociotechnical research prioritises humans, it also acknowledges the power of other aspects of the wider security landscape, such as objects, devices, data, infrastructure and their agency.

Cyberspace is complex, constantly evolving, and contested. This comes with an array of security challenges that now litter daily lives. Whilst a simple identity card, or the contents of our pocket, on face value, may seem to not have the same agency as either computer games, CGI environments, or drones, it is fundamentally embedded within our everyday, and contains a myriad of security concerns and narratives attached to it. Such questions are inherently political and may frequently be associated with anxieties of surveillance (Leszczynski, 2015) something which Amoore, (2014) has suggested is driven by their incalculable, unknown nature to an often fearful or misunderstanding public.

3.6 Ubiquitous Connectivity: The Proliferation of Connected Devices

As these prior sections sought to illustrate, objects are frequently closely linked to security concerns. Furthermore, it suggests that in the 'information era', we live in an age of ubiquitous technology, which pervades our everyday lives, and reshapes our everyday environment, and consequently the security of it (Stevens & Vaughan-Williams, 2016; Dunn-Cavelty, 2008). A push towards the study of the Digital-Material draws inspiration from wider humanities. Lefebvre (2007: 402) suggests there can be no thought, no reflection, without language, and no language without a material underpinning. Geopolitical scholars have argued that by increasing focus on everyday objects, materiality can

link geopolitics and everyday practice (Dittmer, 2014: 386) while political and IR researchers have suggested that “things” can create, dispute, and solve political configurations. Ultimately, nations are composed of wider networks and assemblages of objects (Salter, 2016). This might be evidenced in social and political phenomena such as the 2008 Tunisian Revolution and wider Arab Spring, where social media (accessed predominantly from smartphones) helped coordinate widespread protests which eventually toppled the Tunisian government, as well as others across the Middle East, as seemingly mundane and everyday objects helped bring a networked public together as digitally-enabled citizens to topple an autocratic regime (Zayani, 2016). The phone itself thus became an elevated security concern, to the government and networked public alike.

Mobile phone technology has existed for some time, but moves towards near ubiquitous smartphone technology have been more transformative. These digital-material objects allow the public to connect to the internet anywhere they have a signal. The proliferation of smartphones is an increasingly global phenomenon. Ofcom’s ‘smartphone society’ study, based in the United Kingdom, concluded that more people use smartphones to access the internet than any other device and that over 90% of young people have one. (Ofcom, 2015). Smartphones have transformed many aspects of public life. We now use phones as banking devices, for contactless payments, as cameras, recording devices, navigational tools, and more. Researchers have sought to explain their complex role, embedded and interacting with their environment, noting they are subtle and complex devices, whose uses, agency and effects depend greatly on the assemblages in which they are actant (Chambers, 2016: 195). Others have utilised actor-network theory, as they express interest in this interaction between the digital, material, and social (Balzacq & Dunn-Cavelty, 2016). Others have focused on both data and the interfaces which make the interaction between humans and non-human data possible (O’Grady, 2015).

Of further interest is research into smart card technology. Smartcards are, much like smartphones, highly subjective, subtle, ubiquitous devices with complex forms of agency depending upon multiple factors. By their most simple definition, they consist of a card with an embedded chip, which functions either by direct contact with another device or through wireless short-wave contactless technology (Rose, 2016). Bank cards and travel cards both use smart card technology, transforming the environment around them by inserting capital into daily digital-material interactions (Cobbett, 2016). Similarly, ID cards utilise smart card technology and are frequently issued in many European countries as a mandatory requirement for citizens. Estonia’s identity cards are also digital identities that are an online, encrypted identities, allowing access to governmental documents and online services. Estonians can even vote online through this securely encrypted digital identity (*e-Estonia*, 2017). This technology has attracted considerable attention regarding the security of the cyber ballot (Springall et al, 2014), and the social and cultural factors which have allowed such innovation (Alvarez et al, 2009).

The most obvious digital material object of growing importance and concern has been the military drone, an object that has become emblematic of the war on terror and border security politics and practices (Shaw, 2013). Scholars across the security, international relations, and geopolitics disciplines have been concerned by how these objects blur

security debates, whether concerned with extrajudicial killing or how they transform landscapes with their digital material capacity. Their control is sociotechnical, with affective impacts upon pilots, those they target, and what impacts they have upon international law. There are also concerns about the use of drones in everyday spaces. This might be evidenced by Amazon's continuing push to utilise drones for delivery. Estonia also continues to pioneer autonomous vehicles in the public sphere and is enthusiastically funding self-driving vehicles in particular (Robinson, Hardy, & Ertan, 2022). Yet, such technology is often viewed by the public as associated with the military, or surveillance (Shaw, 2015 & Gregory, 2011). While the standard military drone itself is by no means a mundane or everyday object, the use of autonomous vehicles in civilian situations is steadily increasing (Jackman, 2016) and consequently, research exploring everyday cyber securities of such digital material objects should be of further concern to scholars in this area.

In the Estonian context, the most important digital-material devices are arguably smart cards and smartphones. Estonia's e-government systems utilise both smart cards and smartphones to function securely, via two-factor authenticated mobile and digital identities (*e-Estonia*, 2019). As the access to these systems increases, and the number of connected devices in daily lives proliferates, so does the number of potential attack vectors. e-Estonia, therefore, functions through, but is vulnerable to, the proliferation of smart devices. This vast proliferation of digital-material objects leads back to the debate of referent objects and the subject and objects of protection. In an age of ubiquitous digital material objects, our focus should not turn away from how these secure the state, infrastructure, and data, but should also focus on the human aspect. While existing research has explored the materiality of the digital in the sense of the physical storage of data, raising questions of data sovereignty and how that relates to the material aspects of the digital (Amoore, 2009) relatively little has explored the mundane, yet also exceptional digital-material objects which shape everyday cyber insecurities.

3.7 Insecurity, Sociotechnical Interactions, and Political Implications

The concept of insecurity is also of critical concern to contemporary sociotechnical research. Some scholars have chosen to investigate 'fear' as contributive to security environments, both on an international (Buzan, 1991) and domestic security level (Pain & Smith, 2008). Others have chosen 'Anxieties' as the focal word through which to discuss security dilemmas, noting how the modern security environment lends itself to generating anxieties of the danger of cyber war (Betz & Stevens, 2011: 130) or indeed anxieties of surveillance (Leszczynski, 2015). Yet some critics have rejected the emotive tone of such research, as being too general and which has supposed citizens to be too easily affected or overly driven by fear (Barnett, 2015) and not taking into account the possibility that some citizens can be well-informed and take calculated risks in their online interactions. Consequently, 'insecurities' might instead be a more appropriate terminology, as it is possible to be insecure about something without necessarily fearing it (Browning, 2018). For example, British citizens have insecurities about terrorism given the national legacy of the 7/7 terror attacks and a legacy of IRA republican terrorism. Yet to suggest they are fearful or suffer great daily anxiety is extreme. Whilst concerns peak and trough dependent upon world events, British citizens do not walk the streets in a state of fear (see Stevens & Vaughn-Williams, 2016). This thesis consequently suggests that 'insecurity' is a more

appropriate term to use in order to interrogate digital professionals' sociotechnical relationships with e-Estonia. To draw another example, Estonian citizens might be insecure about the potential of cyber-attacks from Russia, following the cyber-attacks of 2007. However, to suggest they are either fearful, or anxiety-ridden by the possibility of something which for most citizens was an inconvenience, is too hyperbolic, or overstating the problem (Hansen & Nissenbaum, 2009). However, that does not demean the importance of those insecurities, nor mean that they underestimate the readiness to prepare for the worst.

It has been observed that security narratives (i.e. common tropes relating to current political events and security) have fed insecurities, as has been highlighted by many security and geopolitical scholars. (Buzan, 1991; Hansen & Nissenbaum, 2009, Pain & Smith, 2008). This suggests a clear link between insecurities and security narratives, driven by elite actors, either governmental or via the popular media, that are felt by everyday citizens. Bill McSweeney (1999) has previously suggested the essence of everyday security is a situation where individuals feel safe and secure going about their everyday activities. This is somewhat disconnected from narratives of impending cyber attacks, hacks, leaks, and scams. If we accept that the digital and the cyber are every more interlinked with our daily lives, by consequence how secure we feel in our daily lives will be closely connected to our sense of personal security. It is difficult to visualise closely connected data and code which increasingly shape our daily interactions. This makes security concerns difficult to make relatable to the everyday, especially when much security thinking has been developed around notions of the protection of referent objects (Aradau, 2011). Data visualisation is regarded as an important tool in the detection and prediction of risk and vulnerability (Hall, Heath & Coles-Kemp, 2015: 93). Such visualisation provides clarity and illustrates that much security is relational and fundamental to everyday experiences of security. Recognising the need to better explain cyber security concerns to a non-technical audience should thus be a priority of sociotechnical research.

Such sociotechnical research might be more positive (Roe, 2008), culturally sensitive, and appreciate the complexity of mundane security assemblages, and the human relationships which may define them, which may often not feature within traditional security literature. Examples utilised in existing research include that of a granddaughter utilising a grandmother's online accounts (Coles-Kemp & Hansen, 2017). Other research has also highlighted the importance of human trust relationships, in relation to cyber security interactions (O'Grady, 2015).

Security narratives and insecurities are informed by wider discourses surrounding security (Hansen, 2013). These are said to be informed by popular geopolitics and security discourse perpetuated by governmental sources and the popular media. Hansen's (2013) research on the discourse that surrounded the Bosnian war had the effect of driving security narratives that portrayed an ordered west and a disorderly and uncivilised Balkan 'other'. This, Hansen argues, perpetuated security narratives that fed governmental policy, whilst also perpetuating narratives to the public, that in turn shape security concerns. Examples of narratives surrounding the potential of 'cyber war' have been condemned as 'overstated' (Rid, 2016) yet the possibility of 'cyber war' might shape everyday concerns cannot be discounted.

Dunn Cavelty & Suter (2009) suggest that the assumption of much security literature relating to the cyber is that infrastructure is the key referent object to be protected. They define infrastructure as being ‘systems or assets so vital to a country that any extended incapacity or destruction of such systems would have a debilitating impact on security, the economy, national public health or safety, or any combination of the above’ (Dunn Cavelty & Suter, 2009: 1). This is despite a relative broadening of the wider Security Studies genre to include the likes of human security, as discussed above. Securitisation, at least within popular security discourse, has often been met with dystopian comparisons to George Orwell’s powerful political allegory *1984* as well as Phillip K. Dick’s *Minority Report* relating to the overreach of the surveillant state. This might also be perceived to feed insecurities and surveillant anxieties through the popular media (Rid, 2016). Whilst the desire of states to surveil their populace and enemies both domestic and international is nothing new, it has been noted that such distinctions are increasingly blurred within the realm of ‘cyber-space’ (Rid, 2016: 273) as well as enabled by the technological capabilities the digital increasingly provides. (Barnard-Wills & Ashenden, 2012)

The Copenhagen school suggests that speech acts often shape notions of the ‘referent object’. This may often be found within popular media and is then disseminated and becomes part of the popular discourse (Hansen, 2013). Once a subject is securitised it is thus considered beyond reasonable discussion (Neocleous, 2006). This securitisation has leaked into cyber security discourse. As illustrated by whistle-blowers such as Edward Snowden, leading to calls for more nuanced debate around digital security (Deibert & Rohozinski, 2010). This securitisation is distributed through the popular media. Critical scholars have suggested this creates a space of exception, whereby debate regarding digital security shut down, and extraordinary laws are implemented. These might be evidenced through laws such as the Patriot act in the United States. Thus, critical scholars suggest there is a need to reclaim the security debate. Dunn-Cavelty (2009) has suggested that infrastructure is often the referent object in terms of digital security. Similarly, much information security research favours data. (Von Solms & Van Niekirk, 2013). Reclaiming the referent as a human can lead to more balanced approaches, mindful of contemporary sociotechnical dilemmas which increasingly define modern cyber security challenges, whether relating to device security, e-governance, or beyond (see Malatji et al. 2019; Coles-Kemp & Hansen, 2017; Meijer, 2015; Kosenkov et al, 2019).

3.8 Cyber Insecurities, Sociotechnical Interactions

The contemporary study of cyber security and e-governance is complex, and this is reflected by the diversity of work that this chapter has illuminated. Much as concerns of ‘hybrid’ conflicts have proliferated, concerned by the mixing of the multifaceted security challenges, the study of everyday security is multifaceted. Security, international relations and geopolitical theories ranging from orthodox realism to human and critical securities, to the notion of cyberspace and everyday geopolitics are all fertile ground for exploration of everyday cyber insecurities and contemporary hybrid security challenges.

Assemblage theory is traditionally interested in the provisional, socio-material ordering of entities beyond one universal principle. It places all actors on an equal ontological footing and suggests that relations between them occur on an equal basis (Muller, 2015). Consequently, it provides a suitable theoretical basis to explore the importance of digital-material objects, and their interaction and interfacing with the human referent. This has been inspired by Deleuze and Guattari's assemblage research. As this chapter has highlighted, the material is of vital importance to the everyday cyber security assemblage. Deleuze and Guattari's (1987) 'a thousand plateaus' explores the organisation of material systems, but also extends their theorising to include social, linguistic, and philosophical factors. This has consequently shaped much of modern assemblage thinking.

Manuel DeLanda (2005) further progressed assemblage theory, noting some of the limitations of its prior usage, as well as misconceptions. He highlights that assemblage is not only the final product but also an ongoing process, believing this confusion to lie in the language. Furthermore, DeLanda is more critical of Deleuze and Guattari's reductionism to the assemblage itself in its totality, and instead places more importance upon the individual aspects, rejecting the idea there is a 'seamless whole', but rather how micro and macro events can all, to differing levels shape the wider idea of an assemblage. Fundamentally, his argument rejects 'totalities' and differs particularly from Deleuzian approaches in that it is less reliant upon the Marxist approach to capital. Others have emphasised the 'Hybridity' and flexibility this approach has allowed, particularly within International Relations theory, and how it allows the complexity of material, biological, social, and technological components to be considered as intrinsically linked, as opposed to strictly categorised frames of analysis, which have not adequately explained the intertwined nature of many of the above in creating modern political challenges (Acuto & Curtis, 2013: 2-3).

To further engage with the embedded nature of cyber security challenges in e-Estonia, it is necessary to understand the complex, interlinked relationships between the human and non-human. Thinking about security in 'hybrid' terms may also be beneficial. The Baltic states are supposedly uniquely challenged by hybrid threats posed by Russia (Radin, 2017, Galeotti, 2016, & Mälksoo, 2018). This is often seen to encompass the more human aspects of cyber security, such as disinformation. As such, the complexity of these challenges might be seen to require new approaches to the interface of the human and non-human (O'Grady, 2015). That might also include a focus on material objects and the insecurity they can generate (Aradau, 2010), which seems an appropriate consideration, given the growing proliferation of connected devices, and the importance of connected devices in Estonia

Digital interactions have taken on an increasingly important role in the production and dissemination of cultural objects and form a constituent part of a complex digital and material relationship. An approach mindful of the complexity of these relationships might hope to better understand the impact of cultural and sociotechnical influences (Rose, 2016). Existing sociotechnical research has sought to utilise assemblage theory to understand sociotechnical relationships, including the work of Jeremy Crampton (2015) who has explored the codependence between private and public security firms and the political economy of intelligence data. Others have sought to explore notions of privacy as an assemblage (Elwood & Leszczynski, 2013) or the organisation of critical infrastructure and the importance of

material objects in security assemblages (Aradau, 2010). Similarly, there have been micro-level studies of sociotechnical security assemblages in action, such as within the airport (Adey, 2009 & Schouten, 2014) or the city (McFarlane, 2014).

If hybrid warfare is a problem, as suggested by the likes of Mälksoo (2018) and Galeotti (2016), then hybrid security challenges require hybrid solutions. Whilst assemblage theory is a heavily theoretical vehicle for thinking about multiple challenges, it has also been critiqued for being widely adopted yet loosely interpreted – that many simply use the theory as a means of saying ‘it’s complicated’ (Buchanan, 2015). Similarly, the concept of ‘hybridity’ might also be critiqued as being entirely focused on creating a new term for referring to what is simply the modern means of warfare (Paul, 2016). On balance, whilst assemblage and hybridity are referenced within this thesis, these are ostensibly terminology denoting the complexity of contemporary cyber security and the challenges Estonia and its e-governance faces.

3.9 Conclusions

For the purposes of this chapter and the wider thesis, it is crucial to ascertain what we can infer from this research, and what the wider implications are for Estonian approaches to cyber security and e-government. To establish the value of this, the research should have both conceptual and contextual value. Whilst the conceptual value (grounded within existing geopolitical and security research) is established in Chapter 2, the contextual contribution is addressed in this chapter.

This chapter has mapped the conceptual space for this thesis, addressing the research question: *How are everyday cyber securities linked to sociotechnical relations?* From the comprehensive literature review undertaken in this chapter, it can be concluded that everyday cyber security is linked to sociotechnical relations because mundane sociotechnical interactions underpin everyday cyber security. While geopolitics matter, as established in chapter 2, contemporary cyber security concerns are inherently shaped by mundane interactions and ubiquitous connectivity. Broadly speaking, this chapter has also sought to negotiate the challenges of an interdisciplinary thesis. It establishes the future direction of the thesis, establishing terminology such as ‘everyday’, ‘everyday security’, ‘cyber insecurities’, and the ‘sociotechnical’. Additionally, it notes the relationship between everyday cyber insecurities and sociotechnical relations – that both are linked due to the challenges of ubiquitous connectivity. They are also influenced by issues such as securitisation, and might best be conceptualised as a confluence of human and non-human factors. The chapter has also highlighted the importance of non-technical, and human-centric cyber research, noting the significant growth of such research in recent years. It also identifies cyber insecurities and sociotechnical relations as being crucial to this study and our future understanding of complex human-cyber securities.

4. Research Design and Methodology

4.1 Introduction

The goal of this chapter is to set out the methodological approaches utilised by the project and the individual methods that were chosen to answer the project's research questions. This chapter outlines the methods of data collection and describes how these meet the research questions (As seen in both 1.2 and below in 4.2). To justify the choices made when putting together the research design, this chapter also draws upon some empirical examples from existing research and highlights the relevant key methodological concerns and debates. The chapter covers the project's research questions and outlines the methods and methodological considerations when undertaking fieldwork. It draws upon examples from existing sociotechnical and social science research and notes how these have influenced the methods chosen by the author. The chapter then moves on to discuss semi-structured interviews in 4.4. This section describes in detail both the methods and the rationale for sourcing and conducting the interviews, including approaches to sampling and research ethics as well as detailing how the interviews were undertaken. The chapter then describes the use of MAXQDA and coding (4.5) and subsequently details some of the ontological and theoretical debates that were considered when conducting/writing up the research. The chapter also outlines the strategy of anonymisation used in the thesis and also features the anonymised details of participants and their professional roles in order to offer some context to the reader. Finally, the chapter makes some critical reflections and conclusions on the research process, noting the organic nature of undertaking large research projects and how the project evolved over time.

As this thesis was interdisciplinary, the chapter discusses approaches utilised by scholars of security studies, information security, and geopolitical researchers, as these are the primary research areas to which the thesis seeks to contribute. It illustrates the benefits of the different philosophies and methodologies which have informed the analysis within this thesis. The importance of qualitative, 'thick description' (i.e. the importance of social and cultural context, motivations, and richness of data in explaining issues, as outlined by Geertz, 1994) to the project is also noted. The benefits of such qualitative approaches are outlined. The positionality of the researcher is also mentioned as an important ethical consideration to acknowledge and is discussed in 4.3.

The conceptual focus of the project relates to everyday cyber securities and sociotechnical approaches. This interdisciplinary research area has been developed within the earlier literature-based chapters of this thesis [2–3] and the context of this thesis is based upon the conclusions of those chapters – namely that geopolitics matters to Estonian cyber security concerns and those everyday insecurities are closely linked to sociotechnical interactions. As an interdisciplinary research project, the thesis employed a somewhat flexible approach, utilising mixed qualitative approaches in order to answer the research questions (outlined in 4.3 and in 1.2 of this thesis). This includes the use of semi-structured interviews and ethnographic analysis, supported by qualitative analysis. This meant findings are supported by existing literature regarding the role of everyday material-digital objects, critical security, critical geopoliti-

tics, and literature specifically relating to the context of Estonia, as well as the wider Post-Soviet space, and contemporary debates surrounding cyber and European security. Chapters 2 & 3 have provided an overview of this existing research, which is also utilised to support argumentation in Chapters 5–7.

As the project concerned itself with how citizens engage in matters of cyber security in their everyday lives and explores their concerns and how effective governmental and popular cyber security narratives are, it was important for the research to select appropriate methods to illustrate engagement with citizens. This was a considerable challenge when we consider that cyber security itself is a notably slippery concept with diverse and constantly evolving interpretations, as illustrated in Chapter 3. Cyber security, in terms of this research project, is not considered a discipline in itself but instead straddles security studies and information security in particular. This project also heavily draws upon the notable contributions which have come from geographers, interested in the transformative, spatial aspects of cyber security (such as; Amoore, 2008; Ash et al, 2016). As such, the project was mindful of the geographies of the research and aimed to explore how Estonia's innovative approach may be useful in creating the conditions for an improved digital security environment, as well as increased digital engagement beyond Estonia. These contextual factors all informed the methodological choices discussed later in this chapter. The rationale for focusing upon everyday, sociotechnical cyber securities has been driven by the author's hypothesis that existing research on e-Estonia has not been attentive enough to the challenges and insecurities of ubiquitous connectivity, nor has it thoroughly investigated the role of the digital professionals who curate it in such detail.

The research hypothesises that much of the existing discourse is insufficiently attentive to social, cultural, and political factors which shape citizens' attitudes to their cyber security and that a disparity exists between cyber security discourse, wider security narratives, and the everyday concerns of individuals. There is also a significant and undervalued link between cyber security and geopolitics. This project seeks to address this research gap. Furthermore, the research chose to investigate the practical exportability of the Estonian model in terms of managing everyday citizens' tensions between privacy and security. This was driven in part by the explicit claims made by Estonian public figures who suggest that the Estonian model is reproducible, or indeed the government-sanctioned e-Estonia website, which makes similar, bold claims.⁸

4.2 Research Questions

This research explores how geopolitical legacies have shaped current cyber security cultures in Estonia, contending that attitudes to cyber security are assembled in, and by, everyday engagements with devices, platforms, data, as well as human, social, cultural, and geopolitical attitudes. The research will investigate everyday security practices and intuitive behaviour, interested in how this is shaped by geopolitical experiences as well as different interactions with, and exposure to, the digital. This relates directly to the primary research questions and project title:

⁸ For further discussion, see e-Estonia (2019) as well as Reynolds (2016) for discussion of the exportability of e-Estonia, as well as President.ee (2018) for a statement from Estonian President Kaljulaid, stating goals of exporting the Estonian model and developing interoperable services in the Nordic-Baltic region

Securing e-Estonia: Challenges, Insecurities, Opportunities

The following have been identified as the key research questions the project poses, based upon the goals of the project, informed by existing literature in the prior chapters. These research questions (also found earlier in 1.2) in turn shaped the direction of the interview questions, which can be found in the annex of the thesis, as well as the interview transcriptions and other supporting data.

- **What, in the Estonian context, is the relationship between the state, citizen, and everyday cyber security?**
- **Are cyber security concerns changing wider geopolitical and security concerns, especially in relation to Russia?**
- **How does Estonia use its status as a digital pioneer to extend its influence?**

The above questions have consequently informed the methods and methodological choices explained further in the following section.

4.3 Methods and Methodology

It seems crucial at this juncture to discuss which methods and methodology the research has utilised to produce the findings it has, and how it has answered the above research questions. As in the prior chapter, the thesis discussed some of the theoretical, contextual, and disciplinary basis of the project. The primary source of original data for the research consists of semi-structured interviews undertaken by the researcher over the space of 18 months. This is supplemented by appropriate literature and policy documents where appropriate, as well as the author's reflections and field notes of time spent within Estonia. These are drawn from numerous events attended, and notable discussions on matters of cyber security and e-governance, and were recorded within the researcher's field notes over that time period.

These methods form the individual means of investigation, while the wider methodology situates these methods within an overall approach and justifies why the methods are suited to answering the chosen research questions. The chosen research methods are qualitative because they provide rich, in-depth narratives from a relatively small but rich data set. This might be seen as opposed to quantitative research methods, perhaps more suited to large sample sizes, but lacking the same investigative depth of participant's thoughts and feelings (Vanderstoep & Johnston, 2009: Figure 1.2, Geertz, 1994). Furthermore, such methods are far more suited to the 'everyday' aspect the research seeks to achieve because they give space to the individual voices of participants, allow for personal anecdotes and explanations of participants, and when combined with the adaptation of suitably critical approaches, they formed the basis of analysis for the project. The project is mindful of material objects also and reflects the methods encouraged by Dittmer & Gray

(2010) as well as critical security methodology literature Salter & Mutlu (2013) and Aradau (2015). While not explicitly concerned with materiality in its analysis, the project does heed the work of existing researchers and notes the importance of material objects such as smartphones and smart cards in exploring the project's research questions. This methodology was developed and utilised, reliant upon the identification of appropriate sources, the application of rigorous academic reflection, as well as suitable methodological justification, as this chapter seeks to illustrate. The primary means of data collection was through semi-structured interviews, explained further in the following section.

The primary method in this thesis is semi-structured interviews. Participants were sourced through 'snowballing' from key contacts established in Estonia, further detailed later in the chapter. This is a strategy common in qualitative research, although not without concerns which include the positionality of the interviewer, as well as the research being too dependent on a close network of contacts. As such, their success is heavily dependent upon the researcher successfully guiding the conversation, without interfering too heavily (Flowerdew & Martin, 2005). Caution is thus to be taken, and whilst the interviews were semi-structured to allow for more free-flowing discussion, they were guided by the questions attached in the appendix and discussed in 4.4. These were designed mindful of the research questions. In terms of positionality, it seems appropriate to acknowledge that as a white, British and native English speaking researcher from a UK university, I received a privileged welcome from both the professional and public institutions which welcomed me and engaged with me in English rather than the national language of Estonian and/or minority languages such as Russian. There was also a privileged welcome extended due to being from a London-based University and particularly from Royal Holloway, given the University's reputation for cybersecurity research. Many participants expressed that they were happy to discuss their country with a researcher from the UK. It is entirely possible that domestic researchers or those from less-privileged research backgrounds might not have received the same welcome nor access to elite professionals that I was fortunate to be able to negotiate.

In terms of research design, the research questions were designed to elicit answers from participants based on how they treat their personal cyber security concerns. The comments of participants were used to inform the arguments of the research, and were fully transcribed and coded (for more on this process, see 4.5). In addition, the researcher often framed discussion around smartphones and ID cards, using these items as discussion points in the interview due to their importance to e-Estonia. These were used to stimulate conversation around different ways people navigate their everyday cyber security insecurities and the challenges posed by e-Estonia. The research was also shaped utilising the qualitative methods recommended by King & Keohane (1994), who set out how to avoid bias. Furthermore, they suggest methods of descriptive inference and triangulation, with other qualitative methods, to best make sense of the results. Interviews offer the best opportunity to explore complex themes in further detail. As researchers have noted, confidence in interview data can be enhanced by increasing the size of the data set (Kidd & Parshall, 2000). The greater the data, the greater the understanding. The interviews have been designed specifically to address the research questions. Thus the questions relate to the research outcomes. The data gathered is supported (or 'triangulated') with existing research and further supported by the authors lived observations.

The choice of semi-structured interviewing was taken to allow participants the freedom to lead the discussion where they see fit, with the researcher acting as a guide to the ensuing conversation. It can be seen as providing a less formal experience than a fully structured interview and also allowed participants to contribute views that the researcher has potentially missed. A structured interview by contrast follows a set of prescribed questions. The structured interview is written with probes, transitions, and follow-up questions (Vanderstoep & Johnston, 2009: 225). Semi-structured interviews meanwhile offer structure without the same rigidity (Fontana & Frey, 2003).

This method also limits the ability of the researcher to effectively shape the entire interview through specific targeted questions, as is the nature of the prescribed questioning in a structured interview. This approach seemed better suited to the project, given the researcher's concern for everyday security issues, thus giving participants the opportunity and agency to shape the interview in their way, discussing issues that concerned them, or specific interests they relate to the topic. These, as can be evidenced in the analysis and attached transcriptions, ranged from issues about surveillance and hacking, disinformation and geopolitics, right through to pornography, and privacy.

It was the researcher's responsibility to ensure that these discussions remained focused and that the required data was obtained. This was not, as reflected in the later sections of this chapter, always perfect. Occasionally questions were missed, or discussion veered off-topic. Yet, every time discussion wandered and the information was not relevant to the topic, it was more commonly littered with additional insights which comprise some of the valuable quotations in this thesis. From the interviews, key themes were identified, coded via MAXQDA (available in the annex of this thesis), and consequently analysed using 'thick description' (Geertz, 1994), utilising the critical evaluative approaches outlined in this chapter by established researchers in the field of security studies and geopolitics. Such methods have been utilised by critical security researchers such as Salter & Mutlu (2013), whilst scholars of critical geopolitics have encouraged such approaches as a means to infer popular geopolitical narratives from everyday concerns (see Dittmer & Bos, 2019).

The collected data and transcribed interviews were analysed utilising a theoretical qualitative framework to provide structure and direction as well as minimising the researcher's bias. Further to this, from the emergent themes of the interviews, content analysis will also be conducted on appropriate documents to strengthen or illuminate the answers of the participants, as well as supported by relevant. This triangulated methodology has been chosen deliberately and was combined with theoretical reflexivity, as urged by Rose (2016), who suggested this ought to be conducted to reduce the researcher's own bias wherever possible. Similar justification can be found in the conclusions of Salter & Mutlu (2013) as well as Johnson and VanderStoep (2008), who concern themselves with the representativeness of research, case studies, and what 'everydayness' can be found in such research is grounded within these approaches.

Whilst qualitative methods are often noted for their general 'messiness' and vague nature, they are also suited to exploring emotions. Individual preferences are complex, detailed, and often not fully suited to quantitative approaches. It has been argued that qualitative approaches are better placed to explore complex social phenomena (McLean &

McMillan, 2009). However, it is important to mitigate concerns relating to how representative samples are and recognise the limitations of what can be asserted from the results. Through the care of the researcher, following the guidelines laid out as per the key research methods this project has adhered to (primarily Kuus, 2018, Salter & Mutlu, 2018 & Johnson & VanderStoep 2008), and attaching the transcribed interviews to the annex of this research, any concerns of misrepresentation should be mitigated. All interviews varied, and sometimes conversation wandered (occasionally questions were missed) but this format also allowed for a greater, and more constructive exchange. Due to the at times informal nature of these exchanges, participants often recommended colleagues or contacts to also speak with (furthering the snowballing technique of finding participants). The subsequent sections (4.4 and 4.5) address the contents of the interviews and the rationale for choosing digital professionals as research subjects.

4.4 Interview Structure & Questions

The full interview structure and questions are enclosed in the annex of this thesis. The questions in table 3 outline how certain key questions asked to the research participants addressed the research questions of the thesis/individual chapter research questions. It is important to acknowledge that this is illustrative. More questions were asked of participants (as can be evidenced in the annex) but as the project evolved these were sometimes discarded or became less relevant. Matching the questions exactly to the research questions is not a perfect process due to the messy nature of qualitative research (as argued by Salter & Mutlu, 2013) and also due to the way the project evolved over time. Nevertheless, Figure 3 highlights which questions generated the key data for each chapter. Meanwhile, further details on how primary data was interpreted via qualitative analysis and coding can be found in 4.6. Some of the questions from the table and other questions which were posed are discussed in further detail below.

	Interview questions sourcing primary data to address the research question	Chapter Research Question
Chapter 5	<p>What are the key threats to Estonia's cyber security?</p> <p>What are the common security concerns of Estonians (in your experience)?</p> <p>Do you think these are commonly linked to ideas of national security?</p>	<ul style="list-style-type: none"> • What, in the Estonian context, is the relationship between the state, citizen, and everyday cyber security?
Chapter 6	<p>What are the key threats to your own personal cyber security?</p> <p>What measures do you take to ensure your own cyber security?</p> <p>Do citizens have a role and responsibility in ensuring their cyber security?</p>	<ul style="list-style-type: none"> • Are cyber security concerns changing wider geopolitical and security concerns, especially in relation to Russia?
Chapter 7	<p>Is there something unique to Estonia or Estonian mindsets that makes technological innovation possible?</p> <p>What is the future for e-Estonia? Is e-Estonia likely to spread across the Nordic region?</p>	<ul style="list-style-type: none"> • How does Estonia use its status as a digital pioneer to extend its influence?

Figure 3: Key Interview Questions and Research Questions

Of particular interest might be the following questions, which elicited responses on what the challenges, insecurities, and opportunities posed by e-Estonia are. The replies to these questions often heavily shaped the direction of the analytical chapters, whilst some themes emerged from different questions. Of vital concern to everyday security processes, the focus of chapter 6, was the question

“What measures do you take to ensure your own cyber security? (For example, any procedures / Cyber ‘hygiene’ / everyday practice / VPNs in place)”

For this question, responses frequently discussed a variety of procedural or performative actions within their daily lives or related their security concerns to their everyday lives. Meanwhile, the discussion of key threats to Estonia as per the following question

“What are the key threats to cyber security in Estonia? (top 3 in importance, if possible)”

This encouraged participants to think about the national, or state-level security concerns of Estonia, and reflect upon governmental policies, and perceived threats. These concerns regularly contrasted with individual concerns which were highlighted by the following question.

Meanwhile, reflections on the uniqueness of Estonia are drawn from the following question;

“Can you describe the Estonian approach to cyber security? Do you believe there is anything unique? (after all, in many areas of security discourse, Estonians are considered experts in the field)”

This led to multiple reflections on the history of Estonia, the size of Estonia, and how the particular circumstances of Post-Soviet re-independence had fostered the development of the contemporary state, and e-Estonia. The above question, for example, is undoubtedly important but more generally applies across all analytical chapters rather than specifically addressing one research question.

Similarly, the following question:

“From your personal experience, what are the common security concerns of Estonians?”

led to participants observing the current state of national security in Estonia – a common theme throughout the entire thesis. This then led to discussions around the relationship between state security and cyber security. Whilst some participants echoed arguments of privacy and personal cyber security, others commonly linked ideas relating to state-level security, particularly how ‘fake news’, a popular political talking point at the time of research, was especially important. This was regularly related to the Russian language media available online, and broadcast within the country,

and how it might target the Russian language speakers of the country. This might be seen as a wider suspicion of this group, to be perceived as disloyal to the Estonian state, and shaped some of the analysis of chapter 6 which particularly focusses on the geopolitics of Estonia's security challenges vis-a-vis Russia. However, others opted to discuss the vulnerabilities of the e-state (which closely fit with the analytical theme of Chapter 5). As the interviews were semi-structured, dependent upon the role of each participant, discussion sometimes wandered, or additional, supplementary questions were asked.

4.5 Conducting Interviews with Digital Professionals: Sampling & Ethics

The primary data which has informed this thesis is drawn from detailed, semi-structured interviews with research participants. The decision to utilise interviews is outlined earlier in the methodology (4.3). The logic of engaging with digital professionals is explained in this section. All of the interviews undertaken involved technical experts and high-ranking officials from the public or private sector within Estonia. These participants were chosen as they offered both an expert-level insight into the e-Estonia ecosystem, but similarly, due to the research questions and the line of questioning adopted within interviews, they offered insights into the mundane, sociotechnical and everyday cyber security this thesis is concerned with. This study offers both a top-down and a bottom-up perspective to the study of e-Estonia by engaging with both elite-level actors and the everyday. This research utilises Kuus' work (2018) for guidance as she details the practice of undertaking interviews with high-ranking 'elite professionals' methodologically, citing examples and experience of personal, professional practice (in Kuus' case, research undertaken in Brussels). Kuus' focus on the everyday is vital to this project and notes in great detail the everyday applicability of her diplomatic research. She concludes 'Only through a careful qualitative analysis of the empirical context can one effectively situate practices institutionally and geographically' (2018: 12) and encourages the use of thick description and contextual evidence to support qualitative research. She also notes that any quote is only as strong as the assertions of the supporting argument.

Kuus (ibid) also extrapolates and emphasises how the everyday can find expression in the lives and working practices of 'elite professional' actors, who, as Kuus goes to length to highlight, are also average citizens, with their own everyday lives and lived experiences. While her research involves EU diplomats, who might be considered elitist in some regards, Kuus notes that these diplomats also have a daily, everyday life, and policies and interactions often take place and are shaped by their everyday interactions with others. This thesis argues that there is an everyday and sociotechnical aspect to high-ranking digital professionals' lives also, which remains unexplored, and a vital source of insight into everyday cyber securities. This thesis explores both personal and professional cyber security standards and procedures and encourages participants to mull over their own expertise. Frequently, participants of the research would compare and contrast with other, less technologically capable citizens, urging that while they might be considered experts in their field, these technologies are utilised by non-experts, and as such should be more accessible or transparent.

The project also involves qualitative analysis revolving around official policy documentation, and its connection to the interview data. Official governmental documents and discourse from official governmental websites will be analysed in a thorough, ‘thick descriptive’ manner, and utilised to support findings. All Estonian governmental documents and NATO documents are available in English. Similarly, some Russian documentation about wider security strategy and cyber strategy is available in English via the Kremlin website. Content analysis is also undertaken within this thesis on a qualitative basis and deploys the established guidelines of Timmermans & Tavory (2012) who emphasise that theory construction is a skill developed through repeated exposure and close engagement with both data and related examples of theory construction. Thus, all documentation when utilised is deployed with the support of established academic rigour and procedure, rather than cherry-picked to suit the author’s arguments. It is also analysed in a manner that supports the primary data of the thesis and supports the themes which emerged from the interview data.

Participants for the research were sourced by using contacts established over time – primarily from Tartu University but also by the research technique of snowballing (i.e. one participant putting the researcher in touch with another and so on). The researcher sent emails to identified relevant parties based on the criteria below. The author targeted a number of private and governmental institutions within Tartu and Tallinn, following networking, discussions in the department at Tartu University, based on local advice on the tech industry, and through personal contacts. The sampling took some time at first, and would often emerge in scattered groups. Sometimes sources occasionally went quiet, times for interviews could simply not be confirmed, or there was a lack of correlating free time for the researcher and participant to meet. Furthermore, some interviews were discarded as the scope of the research changed. Initial plans were to target young tech workers, yet this seemed more problematic based on contacts established. As the research transpired in the field, it became quite clear it was possible (with relative ease) to interview established and often senior-level digital professionals for the research. These participants are detailed in section 4.9 and the amended scope for their participation is explained also.

The research specifically sourced experts within the field and/or associated with the fields of cyber security or e-governance within Estonia. There was no particular age group, although the author, in the interests of both balance and good practice, sought to establish a gender balance among participants. Whilst a perfect 50/50 distribution was not possible due to the way interviews were sourced, the distribution was 11 male and 9 female participants. The rationale for the targeted participants was informed by the literature review in chapters 2 and 3, which suggested that Estonian’s wider geopolitical narratives are likely to impact their cyber security concerns, and that their everyday cyber insecurities are linked to sociotechnical relations.

Given these findings, the research targeted individuals working in public bodies (either working for them, or in private companies with close links to the public sector via public-private partnerships) and working with technology. All participants can be considered as experts within their field, would have a good understanding of the challenges of cyber security, and might be classified as ‘tech-savvy’ – i.e. ‘Digital Professionals’. These digital professionals utilise modern technology in their daily lives. These professionals were at that time employed in a public or private institu-

tion in some way connected to the e-Estonia ‘ecosystem’ including think tanks, universities, private tech developers, governmental departments, and/or were volunteers with the EDL (Estonia’s famous Defence League Cyber Unit).

As the research is concerned with the extent of historic and cultural factors that inform attitudes toward cyber security, all participants were based in Estonia and had significant lived experience in the country. Thus, the questions the research poses in regards to social and historic political narratives and experiences and their role in shaping contemporary attitudes around cyber security issues (particularly relating to surveillance) are understood and participants are able to discuss matters based on their personal experience. Consequently, nationality was not considered an issue due to the above criteria. All three non-Estonian participants (nationalities anonymised) had lived within Estonia for some time and due to their professional subject positions were recognised as experts in the field. The final two participants listed below (Participants U & V) did not participate in full interviews but instead specifically provided comments relating to international e-governance collaboration as it related directly to their occupations. These were of particular utility to chapter 7 of the thesis.

The research was undertaken over two lengthy periods in Estonia, whilst on departmental visits visiting the Johan Skytte Institute of Political Studies, under the supervision of Professor Eiki Berg. This was enabled by the DORA mobility programme, which supports the mobility of incoming doctoral students interested in conducting research within Estonia. The initial visit was undertaken between January and April 2018, with a return for the following academic year in 2018-9 as a research fellow funded by the Estonian Research Agency. Thus, the author by the completion of the project had spent around 18 months embedded within the Johan Skytte Institute of Political Studies in Tartu, as well as living in Estonia. During this time, the author actively participated in research events pertaining both to political science, but also prominent cyber security events held in public and private institutions around Estonia.

Interviews conducted

Below is an overview of research participants, organised by date from earliest to latest. Private companies have been redacted, however, further details of employment (suitably anonymised) can be found in the thesis anonymisation section (4.8)


Participant	Date	Place of Employment
Participant A	1.2.19	[REDACTED]
Participant B	08.3.18	[REDACTED]
Participant C	14.2.18	[REDACTED]
Participant D	20.3.18	Estonian University
Participant E	6.4.18	[REDACTED]
Participant F	6.4.18	[REDACTED]
Participant G	9.4.18	RIA (Estonian Governmental Department)
Participant H	3.4.18	[REDACTED]
Participant I	29.3.19	RIA (Estonian Governmental Department)
Participant J	26.2.19	Estonian Defence League - Cyber Unit
Participant K	27.3.18	Estonian University
Participant L	31.10.17	[REDACTED]
Participant M	7.3.18	[REDACTED]

Participant N	26.2.19	Estonian Defence League - Cyber Unit
Participant O	6.2.19	NATO CCDCOE
Participant P	11.4.18	MKM (Estonian Governmental Department)
Participant Q	10.4.18	MKM (Estonian Governmental Department)
Participant R	1.3.18	[REDACTED]
Participant S	1.3.18	[REDACTED]
Participant T	27.2.18	[REDACTED]

Minor Interviews by Email (Further details below)

Participant U	14.12.18	Nordic Institute of Interoperability Studies
Participant V	17.12.18	VRK (Finnish Pop. Registry & E-Govt Dept)

The data was collected, as stated above, through semi-structured interviewing. All interviews were recorded using an audio recorder application using the researcher’s smartphone. These were then securely stored by the author and backed up on Royal Holloway University servers. All interviews have been transcribed and are included in the thesis annex. The semi-structured nature allowed for participants to take interviews off track slightly in a natural way, adding additional personal insights. All participants were given the right to withdraw at any time and have been provided with a full copy of this final thesis.



ROYAL HOLLOWAY, UNIVERSITY OF LONDON
ETHICAL APPROVAL FORM

For staff and student research projects involving data collection from research participants (observations, interviews, questionnaires, group discussions, recordings, video etc).

As the work involves human participants, ethical approval must be sought in advance. All data will be stored securely on the University database. All research has been approved by the project supervisory team (Prof Klaus Dodds & Prof Lizzie Coles-Kemp), and also through the Department’s internal approval procedures, and is bound by the College code of ethics in research.

To be completed by the participant (delete as appropriate)

1. Would you like any data related to your contribution anonymised? YES/NO

2. Would you like a copy of the final project and any papers utilising your contribution? YES/NO

3. Are you happy for your comments to be utilised within the research? YES/NO

As a participant, you have the option to withdraw from the project at any time. This can be done by notifying the researcher (Alex Hardy), if you do not wish your contribution to be included.

The working title of the research project is:

Everyday Cyber Securities: A comparative study of the UK & Estonia

I am fully aware of the research project, and furthermore am happy to proceed to contribute.

Participant Name (print below): **Signature:** **Date:**

.....

Figure 4: A copy of the ethics form provided to, and agreed with all research participants

Throughout this research, the author's position and potential bias are to be considered at all points and thus reflected within the choices of analytical framing as well as focus analysis. Furthermore, all research will be passed through the university ethics committee, in full compliance with guidelines and procedures. This is supplemented by the right for individuals to withdraw from the research at any time and guaranteed the anonymity of participants. Additionally, the researcher carried out a full departmental risk analysis to ensure the safety of the researcher, the participants, and the integrity of the University was protected and adequately catered for at all times. A preview copy of the ethics form that was issued to and authorised by every participant in discussion with every participant can be seen in Figure 4 above and is also included in full-size in the annex of this thesis.⁹

4.6 Utilising MAXQDA for Qualitative Analysis

As can be seen in the annex of this thesis, all interviews that were undertaken with the digital professionals discussed above were fully transcribed. This not only provides analytical utility for coding but also exists as evidence that quotations were not taken out of context. The transcribed interviews were consequently analysed by the researcher, and ten codes were assigned, based on common patterns within the data, as well as areas of interest within existing research, identified by the author in the literature review chapters of this thesis (Chapters 2 and 3 respectively). These codes identified patterns or common narratives relating to a specific issue. Those issues and subsequent codes were: 'identity' (or the idea of e-Estonia being an integral part of the contemporary Estonian identity), 'fake news and disinformation', 'national security', 'everyday security' (or issues pertaining to personal data, or 'cyber hygiene'), recent 'Soviet and Post-Soviet history', 'Trust', discussion of 'smallness or collaboration', the acceptance of 'risk', 'insecurity' and finally issues related to 'Russia'.

Instances, where these themes were mentioned by research participants, were highlighted by uploading transcriptions to the MAXQDA software and were subsequently analysed (an overview of using such analysis for qualitative research can be found in Christians & Carey, 1989, and for more support of the specific use of MAXQDA to display research findings, see Guetterman et al, 2015 & Cresswell, 2015). This software allows the researcher to apply multiple codes to blocks of text, where more than one description might be applied. For example, take the following quotation:

"I think this is you have to be knowledgeable about things and understand what's possible when something happens... and I lost my card.... but some costs benefit more... so it's for me as I think for many Estonians... It is pretty convenient.... My life is smooth and nice using Digital Services and much value more than my privacy or possible threats will what would happen."

(Research Participant E, 06.04.2018)

⁹ Author's note: This was the working title of the thesis at the time interviews were conducted - hence this is an accurate copy of the form provided to participants, although the title of the thesis was changed - the thesis was originally envisioned as a comparative study. Furthermore, all participants will receive a copy of the thesis prior to finalisation of the thesis. All participants expressed that they were satisfied by the process, and indeed that this was more thorough than they were used to. Furthermore, all participants were contacted for clarification once again before submission of the final thesis. It was subsequently decided that the thesis should be fully anonymised for ethical reasons.

This quotation was coded as discussing everyday security (for example, the discussion of lifestyle and convenience) but also of risk, and the acceptance of that risk (noting that there is a cost of lessened security through having digital identities). Through the application of multiple codes, and extrapolating across all of the data (some 30 hours of interview data, which transcribed amounts to over 70,000 words), it becomes possible to evidence connections between codes. This coding and the results of that coding can be seen within the annex of this thesis, under the subsection 'MAXQDA coding'.

The connections between these codes subsequently informed the direction of the analytical chapters of this thesis, as they highlight intersections between the different codes for further analysis. Consequently, the analytical chapters of this thesis (5-7) are dedicated to the different aspects of e-Estonia commonly identified by research participants and are informed by the research questions identified earlier in this chapter (4.2). Those chapters address relationships between Estonian citizens e-Estonia and everyday cyber security, the geopolitical concerns of research participants (particularly relating to Russia), and how Estonia utilises their status as a digital pioneer to extend its influence. These research areas might be evidenced in the visual displays and dominant codes displayed in the annex [Annex p5]. Whilst a qualitative research project, more interested in thick description and analysis (see Geertz, 1994), the coding undertaken helped to guide the direction of analysis within the wider thesis.

4.7 Ontological and Theoretical Approaches to Qualitative Analysis

It is important to emphasise the flexibility with which the project was approached. As noted earlier in this thesis, cyber security is an interdisciplinary subject, not fully embedded within a set discipline and furthermore is constantly evolving. As such, the methods and conceptual framing were set within the formative stages of the research to allow for changes in the field, some of which are reflected upon later in this chapter. As explained in chapter 3, the research will be taking an 'everyday' approach to research, committed to the concerns of normal citizens. A qualitative approach is beneficial to this research as it allows exploration of everyday security relationships in mundane settings, and the interplay between technology and everyday security (Aradau, 2015). The research rejected positivism and is instead guided by critical security research methodology, as set out by Salter & Mutlu (2013), who note such rigidity is inappropriate to understand the complex nuance of situated case studies, regarding multi-faceted and contemporary security challenges.

This research is further grounded theoretically in Foucault's poststructuralism. This poststructuralism has largely held that discourses are not simple reflections or representations of reality, but that they may create new, subjective truths through their spread (Foucault, 1970). This approach, as with much qualitative analysis, may seem muddled, yet also allows us to make sense of the study of micro and macro-scaled problems (as noted by Dittmer, 2010), and allows for fuller, critical analysis of the power structures involved. Thus, this approach is fitting to demonstrate the link between everyday security and national security concerns. This critical approach to power structures is inherent

to the critical security studies sub-discipline and has been established by the work of Neocleous (2006) and McSweeney (1999), and further emphasised by Johnson and VanderStoep (2008), who argue that such approaches are vital in the study of 'everydayness'.

This research draws considerable influence from these works and extends the application of their theoretical approach to the study of cyber security. As the research treats cyber security as woven into everyday life, reflecting its Estonian case study, it engages with material philosophy in its analysis (such as Meehan et al, 2013) when discussing Estonia's ID cards, mobile identities, and smartphone usage. However, such material approaches are complimentary rather than central to the analysis of this thesis, which values critical approaches and discursive reproduction. The project is thus mindful and analytical of the reproduction of everyday insecurities (see Vaughan-Williams & Stevens, 2016 for more on this concept, albeit in a conventional, non-cyber security setting).

The methodological ground for such critical approaches is evident in Salter & Mutlu's critical security methods, as they note that such approaches are:

"useful for demonstrating the impact of language on discourses and practices of security; not only highlighting the linguistic origins of insecurities but also demonstrating the impact of competing narratives in shaping them." (Salter & Mutlu, 2013: 2)

This approach also draws some inspiration from constructivist theory, often utilised by International Relations and security scholars (such as the Copenhagen School often associated with Barry Buzan, Ole Weaver, and Lene Hansen) which suggests that such political views and security perceptions are shaped socially. Thus, security narratives and insecurity may be reproduced linguistically, and geographical location can influence the reproduction and reinforcement of such views. Consequently, the research values both the reproduction of linguistic and discursive tropes, but also draws upon qualitative approaches and occasionally, material ontologies (Aradau & Huysmans, 2013: 2) This allows for the structuring of research discussions themselves, which are to be undertaken using conventional qualitative methods, and analysed later utilising thick description (as guided by the work of Geertz, 1994). The methods themselves are a reflection of the tools for organising empirical material and practical research design.

Research question 1 (What, in the Estonian context, is the relationship between the state, citizen, and everyday cyber security?) makes some limited engagement with security objects that permeate everyday life in Estonia. To answer this, the interviews asked what the participants believed were the common cyber security concerns of Estonians and used ID card and smartphones as prompts in order to discuss these objects and their relationship to national security. Question 2 (Are cyber security concerns changing wider geopolitical and security concerns, especially in relation to Russia?) engages the data of participants with research from the fields of critical geopolitics and security studies to better understand how cyber security concerns reflect geopolitics in the Estonian context. Question 3 (How does Estonia use its status as a digital power to extend its influence) similarly engages with both primary data and supports its argumentation with relevant research in the field of small states and e-Governance. This question also engages with

official policy documents and government statements to support and supplement the findings from the interviews conducted.

Mutlu (2013) suggests a mixed methodological approach of discourse analysis and auto-ethnographic observation to observe the chosen security issue in its surroundings. However auto-ethnographic observation represents a myriad of problems, including the tendency of the researcher to speak on behalf of the subject of research. Engagement with participants, through interviews, is a preferable way to understand everyday cyber security engagements and understandings. Nevertheless, whilst not formally nor fully embracing an ethnographic approach, the thesis does represent the product of considerable reflection by the author (given the considerable time spent embedded in Estonia), and utilises field notes from events, meetings and informal discussions to generate additional insights. These form the basis of some aspects of an ethnography¹⁰, but in the context of this project are simply meant to compliment the other original data the project substantively produces – predominantly in the form of semi-structured interviews, and instead form part of the qualitative evaluation of the project as vital forms of reflexive, qualitative analysis of the research (Patton, 2002).

The research consequently adopted a position that it was preferable that participants were to discuss their everyday experiences, rather than the observant researcher speaking for and of them. The methods used by this research are a more conventional qualitative approach, such as outlined by Patton (2002) and Kuus (2018). This approach is also sympathetic to the methods of everyday research outlined by VanderStoep & Johnson (2008), who suggest that triangulation of methods is an appropriate manner to conduct qualitative field research. The critical analysis of many of the other chapters draws inspiration from Salter & Mutlu (2013: 2), whose research adopts four postures of critical inquiry, which are thus;

“1 Social and political life is messy: our analyses must reflect our belief that we cannot identify any single unifying principle in social and political life; methodological pluralism is a hallmark of this belief.

2 Agency – the capacity to act – is everywhere: it can be found in individuals, groups, states, ideational structures, and non-human actants.

3 Causality is emergent, rather than efficient: analyses set out the conditions of possibility for a set of politics, identities, or policies, rather than a single or complex source.

4 Research, writing, and public engagement are inherently political: we understand politics in its broadest sense to mean questions concerning justice, power, and authority; critical scholarship means an active engagement with the world.”

The research design and critical evaluation are consequently guided by such principles. The choice of semi-structured interviewing with a selection of policymakers, security practitioners, and digital professionals is best suited to meeting

¹⁰ An ethnographic approach was considered by the author in the formative stages of this project, but the means to produce any ethnographic study were considered too prohibitive to contribute the sole, primary data for the project. The author’s understanding of ethnographic research was informed largely by the critical methods laid out in Salter & Mutlu (2013).

the demands of the research questions and forms the dominant means of primary data for the thesis, which is consequently supplemented with additional resources such as field notes and appropriate, literary source data to support the qualitative evaluation of the project (Patton, 2002).

4.8 Thesis Anonymisation Guide

All participants willingly consented to participate in this research. However, in the pursuit of ethical research, these participants have been anonymised. This section briefly introduces the anonymised background of the research participants. This research follows the guidelines and advice of Mauthner et al (2004) as well as Horner (1998), suggesting that the loss of privacy in published research can be extremely problematic ethically and may hold potential repercussions for those participants involved, who so generously gave their time to provide their input into the project.

Individuals' positions, where possible, have been left suitably vague as to make identifying individuals difficult whilst also attaching suitable gravitas and value to their claims. Many of the research participants, as outlined in the methodological chapter of this thesis, are high-ranking digital professional actors within their field and hold senior positions of influence. Whilst it may be possible from the details below to identify individuals, these details have been disguised as much as practicable. For example, Non-Estonian workers are identified as such, rather than as specific nationalities which might identify them more specifically. Nevertheless, there is an inevitable limitation of conducting research in a small country, within a small community.

As such, the work references the work of Clark (2006) out of both a sense of pragmatism but also academic rigour regarding research anonymisation. Clark argues that while anonymisation is an important aspect of research, he also carefully argues that the blanket anonymisation of all background information should not be undertaken, lest the value of some of the data be lost. He instead urges a reflexive approach where the author makes decisions based upon the perceived sensitivity of the data at hand. He further notes that anonymisation always runs the risks of a participant becoming identifiable unless data is so obscured it loses value, and thus the researcher must act with care and diligence to identify things that should and should not be anonymised, given the sensitivity of that data and also personal information. Given that little of the data within this thesis could be considered overly sensitive (the focus is, after all, on mundane cyber security and sociotechnical interactions). Consequently, this seems a balanced approach for this thesis to take, which works both within ethical guidelines whilst also being acutely aware of the limitations to the extent that anonymisation can be achieved without the value and gravity of the participant's input being lost or rendered meaningless.

Below, the anonymised individuals are introduced. Companies and governmental bodies are introduced by utilising how the company or departmental websites describe themselves, as opposed to being explained by the author. Individual positions were collected by the author from the research participants themselves at the time of the interview. Some positions have been obscured slightly, mindful of the above discussion upon anonymisation, in situations where without such anonymisation an individual would be easily identifiable. Descriptions of individual companies are in-

cluded, but those companies' names have been obscured. Due to Estonia being a small nation, individuals could most likely be identified this way, as often some smaller companies might only employ a handful of personnel in senior roles. Similarly, Universities have been anonymised, although it is pertinent to note that Estonia only has three Universities (Taltech, Tallinn, and Tartu respectively). Genders are also invisible, in the interests of anonymity. Government departments are visible (MKM, RIA, and the Government Office respectively) as public sector workers' profiles and contacts are not publicly available, unlike private-sector workers, making identifying those participating based on the information in this thesis impossible.

- Participant A [Page 164] (01.02.2019)

Participant A works in a senior position for [REDACTED]. [REDACTED] is a joint company established by two well-known Estonian cyber security and cyber solutions companies [REDACTED] and [REDACTED]. Both companies have 50% share in [REDACTED]. [REDACTED] was established to develop and commercialize specific cyber security products by combining the expertise and experience of two founding companies.'

- Participant B [Page 169] (08.03.2018)

Participant B is non-Estonian and works for private Estonian firm [REDACTED] who, in their own words are: *'a research and development intensive ICT company that develops and sells mission-critical software systems and products, maritime surveillance and radio communications solutions. [REDACTED] has been an active counterpart in developing critical e-Government systems, such as the Estonian X-Road, i-Voting, e-Customs and others. Today [REDACTED] delivers its systems to across 35 countries in the world.'*

- Participant C [Page 178] (14.02.2018)

Participant C also works in a senior position for [REDACTED] (the same company as Participant B).

- Participant D [Page 183] (20.03.2018)

Participant D is an established Non-Estonian professor of e-governance in a leading department at an Estonian University.

- Participant E & F [Page 189] (06.04.2018)

Participant E works in a senior position at [REDACTED]. This interview also featured Participant F, a less senior employee of [REDACTED]. [REDACTED] is an IT management and consulting company. *The core service provided by the company as a client representative is to ensure the operation and development of the client's information system. We help our clients become smart and skilled when it comes to managing your IT matters. Quoting one of*

our clients, “HLP is one of our men in our boat.” Our good practices, the simplicity and conformity of results, and the transparency of our activities, all work to your advantage. Our experts have 5 to 20 years of experience in the fields of IT, development and data protection management.’

- Participant G [Page 195] (09.04.2018)

Participant G is a senior figure at RIA. *The Information System Authority (RIA) coordinates the development and administration of information systems ensuring the interoperability of the state’s information system, organises activities related to information security, and handles security incidents in Estonian computer networks. Information System Authority is within the administrative area of the Ministry of Economic Affairs and Communications.*’ (e-Estonia, 2020)

- Participant H [Page 201] (03.04.2018)

Participant H is senior staff at [REDACTED]. [REDACTED] is a non-profit organisation which lists its priorities as ‘1) To support the collection, preservation and distribution of educational, scientific, cultural and historical data available under a free license, especially in Estonian and Võro languages and make more freely licensed information available about Estonia in other languages. 2) To support and promote projects which are managed by [REDACTED] [REDACTED], a non-profit organization in the United States.’

- Participant I [Page 208] (23.09.2018)

Participant I is a senior figure at the Ministry of Economic Affairs and Communications specifically concerned with Cyber security. *The objective of the Ministry of Economic Affairs and Communications is to increase the competitiveness of Estonian companies and thus the prosperity of people.*’ (e-Estonia, 2020)

- Participant J [Page 212] (29.02.2019)

Participant J is a technical volunteer at Küberkaitse Liit (The Estonian Defence League Cyber Unit). *The Estonian Defence League’s Cyber Unit (EDL CU) is a voluntary organisation aimed at protecting Estonian cyberspace. The Cyber Unit’s mission is to protect Estonia’s high-tech way of life, including protection of information infrastructure and supporting broader objectives of national defence. The Cyber Unit includes specialists in key cyber security positions in national critical infrastructure, patriotic individuals with IT skills, including youth who are ready to contribute to cyber security, and specialists in other fields that concern cyber security (lawyers, economists etc).*’ (Kaitse Liit, 2021)

- Participant K [Page 216] (27.03.2018)

Participant K is a Professor of Cryptography at an Estonian University.

- Participant L [Page 222] (31.10.2017)

Participant L is a senior figure at [REDACTED]. [REDACTED] is a non-profit think tank and consultancy organisation: a joint initiative of the [REDACTED]. [REDACTED] We create and transfer knowledge and best practice in the area of digital transformation: e-governance, e-democracy and national cyber security. [REDACTED] can expertly empower your central and local government decision-makers to lead digital transformation programmes to create smart, sustainable and effective e-government, e-democracy and cyber security solutions. We make this happen through consultancy, training, networking, research and assisting you in the implementation of your e-government technical solutions.’

- Participant M [Page 225] (07.03.2018)

Participant M is a specialist researcher at [REDACTED]. [REDACTED] is the leading think-tank in Estonia specialising in foreign policy, security and defence issues. We aim to be the regional knowledge hub of first choice for the security and defence communities of Estonia, its allies and partners.’

- Participant N [Page 229] (23.03.2019)

Participant N is a volunteer technical expert for the Estonian Defence League Cyber Division (same as Participant J)

- Participant O [Page 232] (06.02.2019)

Participant O is a senior figure at NATO CCDCOE, Tallinn. *‘As the NATO-accredited cyber defence hub we support our member nations and NATO with cyber defence expertise. CCDCOE embodies and fosters cooperation of like-minded nations’* (NATO CCDCOE, 2021)

- Participant P [Page 235] (11.04.2018)

Participant P is also a senior figure for the MKM, as introduced above.

- Participant Q [Page 240] (10.04.2018)

Participant Q is a researcher for the Government Office of Estonia specialising in e-governance and Cyber security. The Government Office *'supports the planning of the government's work, organises and coordinates country's strategic planning, prepares the government's programme and coordinates its implementation'*. (e-Estonia, 2020)

- Participant R & S [Page 247] (01.03.2018)

Participant's R and S are both senior staff at ██████████ in Estonia. *'Founded in 1976, ██████████ is among the largest IT and business consulting services firms in the world. Operating in hundreds of locations across the globe, ██████████ delivers end-to-end services and solutions, including strategic IT and business consulting, systems integration, intellectual property, and managed IT and business process services.'*

- Participant T [Page 258] (27.02.2018)

Participant T is a senior figure at ██████████, a private tech firm in Estonia. In their own words, *'We were founded with the mission of creating a world free from the burden of trust.'*

'The cost to the global economy of managing human trust can be measured in the trillions of dollars per year. A whole range of industries (audit, compliance, cyber security, inspection, certification) exist that try to narrow the uncertainty associated with trusting others. However, they fail, with rising cost. ██████████ replaces trust with digital TRUTH - mathematical proof of the correctness of data, networks, system and processes. Our technology enables applications to be built with truth inherent in their design, delivering value wherever there is digital.'

- Participant U completed an email interview focusing specifically on cross-border e-governance. They are a senior figure at NIIS (The Nordic Institute of Interoperability Studies) located in Tallinn. (14.12.2018)

'Nordic Institute for Interoperability Solutions (NIIS) is a non-profit association with the mission to ensure the development and strategic management of X-Road and other cross-border components for e-government infrastructure' (NIIS, 2021)

- Participant V completed an email interview focusing specifically on cross-border e-governance, specifically relating to Finnish collaboration with Estonia (17.12.2018). They are a senior figure at the Finnish governmental department VRK (*Väestörekisterikeskus*).

'VRK is a Finnish government agency, which provides demographic information services for Finnish citizens, public administrations, businesses and communities, as well as polling services for elections' (VRK, 2021)

4.9 Methodological Reflections and Conclusions

The research of the project overall was organic, and required consistent adjustment throughout the project, as it developed over time. The fieldwork was undertaken over two broken periods, based on funding to visit Tartu University, and the targets of the interviews changed gradually. The research frequently involved flexibility, as well as persistence to meet senior professionals. What became apparent was the value of being situated within Estonia, and Tartu University specifically. Many interviews were obtained organically by snowballing from contact sat the university, informally through friends, attending events, and generally relying on persistence. This did often mean interviews were conducted in spates, around events attended, or by chance dependent on a new contact being made.

It took considerable persistence to obtain interviews with the Estonian Defence League Cyber Division, for example, but then the offer of four interviews came within a day or two, as one contact passed an internal email around. Similarly, it took some months to get an interview from NATO CCDCOE. Many more fell aside. Originally, as reflected upon also in the conclusions of this thesis, there was a hope to conduct focus groups. Regrettably, the practicality of this made such research impossible. As a bizarre quirk, from the many enquiries sent to tech companies in Tartu and Tallinn, those met with a reply or an offer to meet were often with high ranking staff rather than ordinary workers. The decision to conduct interviews with high-ranking digital professionals consequently became a conscious adjustment, rather than an original goal. The research was ultimately complex and messy, as often characterises extensive fieldwork overseas (Hay, 2010), and was also largely conducted towards the end of the project, due to the availability of funding.

It is also important to note that in the planning stages of the project, there was a plan to focus more heavily on object-centred ontologies as outlined by the likes of Aradau (2015). This featured in the original research design, with interviews utilising smartphones and ID cards as discussion points (the logic being that those smart devices were integral to the everyday access of e-Estonia). In the process of writing up the research, an overt focus on objects was largely dropped, having previously been the focus of one of the analytical chapters. Nevertheless, this work is important, as there is such a close relationship between the e-state and smart devices. This can be seen in both 5.6 and 6.4 where research participants mused upon how the security of their connected devices posed represented a challenge for the e-state and a source of insecurity for citizens. Despite object-centred ontologies not being a strict methodological approach for this thesis, the thesis does utilise literature focusing on devices and also contains rich data discussing their importance (as evidenced in the annex of this thesis).

This chapter has chiefly explained the how, what, and why of this project. It has explained how the research was undertaken, through the explanation of the specific methods involved in data collection via semi-structured interviews and the consequent methodical critical analysis, as can be evidenced in the rest of the thesis. It has detailed the journey through each stage of the project, explained the research questions, and demonstrated how the chosen methods address those research questions. Additionally, the chapter has highlighted the importance of researcher bias, ethical

practice, and the conduct which guided the fieldwork undertaken. It has also demonstrated the researcher's knowledge of potential methodological pitfalls which informed the project. Finally, the chapter offered some critical reflection of the methods employed, whilst potential alternatives are discussed in the concluding chapter of this thesis (8).

Finally, the research was subject to some methodological limitations. Firstly, it was solely carried out in English, due to the author's lack of Estonian language skills. Fortunately, the vast majority of professional Estonians speak excellent English and this is amplified in the tech sector where English is the working language. As such, despite some early concerns, a translating assistant was not necessary. Secondly, it is perhaps notable in the research that there is an underrepresentation of Russian minority groups within Estonia, who it has been noted by other authors are often excluded from many aspects of public life (Raun, 2002). The research project, despite the author's attempts, did not access any Russian-speaking Estonians. Existing research has noted that many Russian-speakers from both Estonia and neighbouring Latvia often opt to migrate to the rest of the EU for work (Cheskin, 2015), which might go some way toward explaining the lack of Russian speaking participants. Furthermore, being based in Tartu was also a factor, given Tartu has a relatively low Russian population, as opposed to Tallinn and Narva (although the author did travel to Tallinn for a number of interviews, notably with government officials). Thirdly, it is also important to note that while the research also focuses on the 'everyday', claims to 'everydayness' are limited to the everyday lives of the digital professionals – although it has highlighted that wider lessons can be extrapolated from those opinions and experiences, as existing methodological research has highlighted. All conclusions made by this thesis are consequently made in context of these methodological limitations.

5. e-Estonia & Post-Soviet Estonia: Contemporary Challenges

5.1 Introduction

This chapter explores how the Estonian state has actively cultivated Estonian citizens as responsible, secure, cyber citizens, utilising a unique blend of nation-building narratives that construct e-Estonia. This chapter argues that e-Estonia is a popular narrative developed through the performative construction of e-Estonia by both the Estonian government and the tech community. Indeed it might be considered closely tied to the identity of the modern Estonian nation. This chapter responds to the first research question of the thesis: *What, in the Estonian context, is the relationship between the state, citizens, and everyday cyber security?*

The chapter reflects upon the social, cultural, historic and political challenges that Estonia faced upon its re-independence in 1991. It examines the role of notable consequent events, such as the 2007 cyber attacks in shaping the relationship between citizens and the state. It develops the notion that e-Estonia now forms an integral part of the contemporary Estonian identity, and this is performed and reproduced by digital professionals. Whilst e-Estonia has been an economic success story, the re-invention of Estonia as a tech pioneer has not been uncontested. e-Estonia has been shaped by the unique socio-cultural and historic attitudes of the Estonian people (and those attitudes are framed through the Soviet past and feelings of geopolitical smallness) some feel less involved in the everyday reproduction of e-Estonia, as suggested by recent political developments. From the digital professionals this study engages with, this chapter argues we can evidence the (re)production of e-Estonia through empowered ‘petty sovereigns’ (a concept of Judith Butler [2006] explained in 5.3) drawn from the digital professional community. These are a small, but politically empowered community within Estonia, that has yielded impressive economic and technological results, yet is challenged by contemporary events.

5.2 Contemporary Estonian Politics

This research was carried out between January 2018 and early 2019, preceding the 2019 Estonian election. This was in the context of a growing global interest in the perceived threat of increased Russian influence, interference, or aggression toward other sovereign states (Kuzio, 2017, Giles, 2016). This is particularly notable within Russia’s ‘near abroad’; a term utilised by the Kremlin to denote former states of the former Soviet Union, often with significant Russian-speaking populations (Toal 2017).

The outcome of the 2019 election was something of a shock. Reformierakond (Reform), the dominant political party in recent decades, finished as the largest party, over-performing expectations. Keskerakond (Centre), the party of sitting Prime Minister Jüri Ratas slightly underperformed, finishing second (most polling at the time had the two parties close, but generally projected Centre to be the largest party). Perhaps most notable was the rise of EKRE (Eesti Konservatiivne Rahvaerakond – The Estonian Conservative People’s Party), who finished third with a big increase in their share of the vote. Also present were the Sotsiaaldemokraatlik Erakond (The SDE or Social Democrats) and

Isamaa ('Fatherland', a Christian conservative party). The election led to a 'controversial' coalition led by Centre Party and sitting PM Ratas with EKRE and Isamaa (Bult, 2019). In the aftermath of the election, as the largest party, Reform was permitted an attempt to form a government by the president. However, despite Reform and Centre both sitting within the Liberal ALDE (now rebranded as Renew) grouping in the European Parliament, Centre refused to countenance Reform leading a coalition of the two. While Reform refused to countenance negotiations with far-right EKRE (the only alternative was Reform could command a majority), Centre formed a slim Parliamentary majority with EKRE and Isamaa to keep Jüri Ratas as PM. To considerable outcry, those negotiations led to a far-right presence within the Estonian government for the first time since re-independence (Mudde, 2019 & Petsinis, 2019).

The values of EKRE in particular have been the source of much controversy (Petsinis, 2019 & Kasekamp et al, 2019), and are in stark opposition to the contemporary, neoliberal Estonia that has emerged in the past 30 years. Their electoral slogan 'Eestlaste Eesti!' (Estonia for Estonians!) highlights their nativism, and 'Eesti Eest' (For Estonia!) is also a commonly utilised electoral slogan. EKRE's torch-carrying marches of growing size were a notable presence in both Tallinn and Tartu during the author's time in Estonia and have also been highlighted by international media such as *The Telegraph*, while others have noted the 'sinister' appearance of the procession (Bult, 2019). Vilson (2021) notes that Estonia has always been a somewhat 'pragmatic' European anyway, and the 2019 coalition has been a more 'reluctant' European nation, affected by a growing domestic populism and nationalism. The rise of EKRE is roughly tracked to 2015 and it has been argued that EKRE has thrived by utilising identity politics as well as exploiting economic inequalities. Furthermore, they have utilised a unique Post-Soviet anti-refugee angle, arguing that Estonia might be 'colonised again' by outsiders – simultaneously also attacking Estonia's Russian community and inferring they are colonisers from the Soviet era (Petsinis, 2019 & Kasekamp et al, 2019).

e-Estonia on the other hand is detached from such nativism. Estonia brands itself as the world's first 'digital society' by offering unprecedented online e-governance services to citizens. Additionally, Estonia is particularly proud of its e-Residency programme. Launched in December 2014, the e-Residency programme is an initiative to offer non-Estonians the opportunity to become an 'e-Resident' of Estonia. While bold early claims suggested that e-Residency had the potential to 'redefine the nation state in the digital era' (Kotka et al, 2015) in reality, e-Residency offers willing international citizens the opportunity to buy an Estonian digital identity. Nevertheless, significant public diplomacy efforts have been invested in promoting a vision of e-Estonia as an open nation and a global community with equal access to e-services (Blue, 2020). However, e-Estonia should not only be conceptualised through the utility of public services. This chapter suggests that e-Estonia as an idea performs three distinct roles: first, it is a social and cultural signifier of a new Estonian way of life. For some, including the participants of this research, it represents a break with the Soviet past and is internationalist and inclusive. Second, it has become a tool of digital diplomacy for the Estonian government. e-Estonia is simultaneously a form of nation branding and soft power (Hardy, 2020). Third, it is an exportable commodity, perhaps further illustrated by the e-residency programme, as well as the modern e-governance visitor centre in Tallinn, which counts foreign dignitaries and investors among its many visitors (Mäe, 2017). As President Kersti Kaljulaid wrote in 2019, "Estonia is running its country like a tech company" (President.ee, 2019). Yet

it might also be argued that Estonia is an example of a nation rather too concerned about its international reputation when it could look to some of the social and economic problems at home, particularly affecting those beyond an affluent and privileged tech industry.

The e-Estonia brand casts Estonia as hyper-modern and culturally Nordic (Taampuu & Masso, 2016 & Mäe, 2017). This sharp contrast between modern Estonia and its Soviet past is exacerbated by continued poor relations with neighbouring Russia, as well as the significant Russian-speaking population of modern Estonia (c. 30% Russian-speaking minority), which contributes to a tense Geopolitical environment. This geopolitical tension is highly influential within Estonian politics and arguably permeates Estonian society. The goal of this chapter is to both illuminate some of the many contemporary challenges that advances in technology pose to Estonians, as perceived by digital professionals, exploring their relationship with the state.

5.3 e-Estonia's Digital Professionals, the State, and Independence

The development of e-Estonia has not been an overnight phenomenon, but a gradual process characterised by the relatively slow implementation of services. This might contrast with more sensational media headlines, which suggest that the Post-Soviet emergence of e-Estonia is a sudden phenomenon. For instance, Schulze (2019) claims 'fast track changes' shaped Estonia's Post-Soviet development, but as highlighted by the research of Solvak et al (2018), this was not the case. Instead, development was gradual and services were introduced slowly over time. The roots of e-Estonia stem from independence in 1991 and the moves were taken by the government in its aftermath to modernise the nation, as well as map a future direction for a small country with a limited budget. The development of e-Estonia was as much visionary as it was a necessity. The implementation of Operation Tiigrihüpe (Tiger Leap) from 1996 was seen as vital and is often most associated with former President Lennart Meri (whom Tallinn Airport is now named after) and Toomas Hendrik Ilves (who was then the Estonian Ambassador to the USA). This programme aimed to both educate and inform the public about new technology, particularly for public services. It aimed to provide the skills necessary to the next generation of Estonians to excel in the digital age and is widely considered a great policy success (Kattel, 2019). It focused heavily on education and laid the foundations for many young Estonians to move into the tech industry. The introduction of digital identities from 2001 was key to the development of e-Estonia. The Bronze soldier cyber attacks of 2007 have been characterised as the world's first cyber war in some commentaries (see Rid, 2011; Betz & Stevens, 2013 for example). These attacks illustrated the value of e-Estonia to the nation itself, but also its potential vulnerability. Frequently, participants in this research identified this event as a key departure, as illustrated later in this chapter.

The role of Estonia's digital professionals is vital to our understanding of e-Estonia. Digital professionals are uniquely empowered in Estonia, having been heavily involved in the development and implementation of Estonia's digitalisation (Margetts & Naumann, 2017). Yet relatively little attention has been paid to the impact of empowering such a group of workers in this way, and existing work has neglected to focus on the opinions of the digital professionals who

helped create and continue to maintain e-Estonia from re-independence through to the present day. This chapter utilises Judith Butler's (2004) concept of the 'petty sovereign' as a means to understand Estonia's digital professionals. A 'petty sovereign', as further explained later in the chapter, is a government official imbued with far greater power than is perhaps appropriate for their position and lacks proper oversight or regulation. Butler's original conceptualisation of the petty sovereign is overwhelmingly negative, something that this research does not suggest is necessarily the case in this study. Nevertheless, there are some cautionary lessons in handing influence and power to one small subsection of a population. Butler (2004) focuses her research on officials and bureaucrats imbued with managerial power to wield at their discretion. She suggests that petty sovereigns are a product of, but also themselves produce sovereign power. Of particular concern to Butler were immigration officials and those in charge of ordering detentions, stretching as far as workers at Guantanamo Bay (a very different environment to daily life in Estonia). Nevertheless, this idea can have utility beyond such extreme circumstances (existing research has explored the roles of petty sovereigns on topics as diverse as governing 'unruly space' in Darjeeling, India [see Wenner, 2016] and Nuclear policy in contemporary Japan [see Shindo, 2018]). In essence, each 'petty sovereign' is a conduit through which governmental decisions meet everyday life.

The Estonian government is at least cognisant of the possibility of power being concentrated in the hands of a potentially petty sovereign. Participant G highlighted this, stating the e-state is designed in a specific way to counter such concerns.

“Power is divided between different state agencies, and everyone's roles are specifically divided into what people can and cannot do. There is no, you know, all powerful person, or crook, who can control everything”

(Research Participant G, 09.04.2018)

However, the reality of the above is that while power is distributed, it is distributed among a small community of digital professionals who, this chapter illustrates, hold very similar attitudes to security, e-governance, and Estonia's place in the world.

Butler argues that in certain circumstances, 'petty sovereigns' actions can have serious consequences. 'Petty sovereigns abound, reigning in the midst of bureaucratic army institutions mobilized by aims and tactics of power they do not inaugurate or fully control. And yet such figures are delegated with the power to render unilateral decisions, accountable to no law and without any legitimate authority.' (Butler, 2006: 66) Butler utilises a specific scenario to caution against empowering petty sovereigns in such a way, with little oversight, and notes that at Guantanamo, this created a disastrous scenario, with little checks and balances on the powers of those individuals. Consequently, Butler argues that these petty sovereigns wield and reproduce the power of the state without sufficient accountability.

This chapter instead focuses on the idea of a more mundane ‘petty sovereign’. e-Estonia’s petty sovereigns do not wield such arbitrary nor hefty power as Butler’s example. Their power lies in the reproduction of seemingly mundane policy toward ubiquitous e-governance and digitalisation and the political implications of that concentration of power within the hands of one small section of the population. This has connotations of for the everyday security of all citizens, and their relationship with the state, despite the majority of citizens holding no influence over the decision-making process.

5.4 Post-Soviet Estonia

Since 1991, the Estonian security environment has most generally been defined by the country’s relationship with Russia, as well as its new relationships with the western powers. Estonia has sought to strongly commit to both the EU and NATO as a means to guarantee the country’s territorial integrity, which is often envisioned as threatened by its eastern neighbour (see McNamara, 2017 for a more detailed assessment of contemporary security dilemmas for Estonia and the Baltic States). A border treaty with Russia is still awaiting ratification, both in Estonia and from the Russian State Duma, and Estonia has been hesitant to ratify the treaty first, resulting in an anxious impasse (ERR, 2021). Estonian security concerns are also shaped by nervous insecurity regarding the significant Russian-speaking population, particularly in Ida-Virumaa county. Ida-Virumaa contains the city of Narva, which sits on the Russian border directly opposite the Russian town of Ivangorod. Ida-Virumaa county is populated with over 73 percent Russian-speakers, while over 95 percent of Narva itself is Russian-speaking. This led to nervous speculation in the time immediately following the annexation of Crimea in 2014 of how it might be utilised as a *raison d’être* for interference by an increasingly assertive Russian state, more willing to interfere in its own ‘near abroad’ than ever (Trimbach & O’Lear, 2016). Russia is also perceived to have acted with impunity in both northern Georgia and more recently, Eastern Ukraine, in the support of Russian-speakers (Toal, 2016). The collapse of the Soviet Union left many Russians and Russian-speakers scattered throughout former Soviet states. This is sometimes considered a product of the Soviet era, as workers were redirected from more populous Russia to other less populous areas of the Union.

However, it is important to note that there has been a continuous presence of Russian speakers in the Baltic States predating the Soviet Union for at least two hundred years. Before the war, the census indicated 5% of Estonians were Russian-speaking and numbers had fluctuated during Tsarist times (Kasekamp, 2017). Old images of Narva (available online at old.narva.ee) showcase the city before it was sadly largely destroyed during the war, taking with it a swathe of beautiful architecture. These images show numerous signage in the Russian language (alongside Estonian) evidencing the long presence of Russian speakers in Estonia (and somewhat diminishing populist suggestions that their presence is entirely a Soviet-era imposition). Integration for those Russian-speakers in Post-Soviet society in both Estonia and neighbouring Latvia has been problematic and sometimes met with hostility (Cheskin, 2015). This, along with the experience of Russian speakers in other Post-Soviet states led to the establishment of a key aspect of Putin’s foreign policy – the protection of these ‘Russian peoples’. Putin has sought to address Russia’s standing within the International system, in light of a perceived humiliation in the 1990s following the collapse of the Soviet Union, and one of the aspects of restoring Russia’s standing has been an unwavering commitment to the rights of Russian-speakers

beyond Russian borders and the idea of the existence of an ethnocultural ‘Русский мир/Russian world’ (Sakwa, 2017).

Estonia, and the wider Baltic states, look westward to NATO and the EU as guarantors of their country’s independence and security from Russian interference. This contrasts with many of the other non-Baltic CIS states, which have often looked to maintain closer relations with Moscow. Ideologically the Baltic states have aligned themselves away from Moscow and towards Europe since the Soviet Union collapsed. It remains to be seen whether these two alignments can ever be compatible with more positive relations in the future, but as of yet, this has not been the case, as European and Russian identities diverge considerably (Berg & Ehin, 2009). Elsewhere in the Post-Soviet world, many states have taken a different path to democratisation as evidenced in the Baltic states. Many (such as Belarus, Turkmenistan, and Azerbaijan) have seen an erosion of democratic rights and a lurch towards totalitarianism. This has also been evidenced in Russia itself, as Putin and United Russia have tightened their grip on domestic politics, while opposition has been crushed. This process has been named ‘democratic backsliding’ and is a common characteristic of many former Soviet states (Cameron & Orenstein, 2012).

The Baltic states, and Estonia in particular, have moved closer to Europe in terms of identity and values (although there remain some concerns with LGBT rights, anti-Russian discrimination, and the gender pay gap remains problematic [Kattel, 2020]). However, the same erosion of democratic rights as seen in other Post-Soviet nations cannot be evidenced. All three Baltic states are free, sovereign democracies, characterised by the rule of law, media freedoms, and free and fair elections (Freedom House, 2021). Further to this alignment with Europe, the Baltic states have been active contributors to NATO. Estonia, as one of the few states that meet their NATO spending obligations, is often happy to emphasise this (McNamara, 2017). The 2004 accession of the Baltic states into NATO is a critical departure. Whilst Estonia and Estonians (as well as the other Baltic states) might be assured of the protection of NATO in the event of a physical attack upon their territorial integrity, the decision of the Baltic states to overtly align themselves with the west militarily seriously aggrieved Moscow. Putin’s regime has consequently considered both the presence of forward bases in the Baltic Sea region, as well as the location of ballistic missile defence systems in eastern Europe, as a challenge and threat to Russia’s territorial integrity and as symbolic of western overreach. This has been identified by Toal (2016), Sakwa (2017), and Browning (2018) as one of the primary contributing factors to the Russian grievances which have come to define the post cold war era. Whilst the Baltic states have thus far been free of any of the kind of armed actions witnessed in Georgia, east Ukraine, and Crimea, they have been subjected to a series of coercion and soft power stemming from multiple sources, including Russian-language media outlets as well as cyber attacks and disinformation (Grigas, 2012). These actions, along with the cyber attacks of 2007 have driven Estonia to solidify its cyber defences, including the establishment of the NATO CCDCOE (Cooperative Cyber Defence Centre of Excellence). Closer ties to NATO have been central to Estonian security strategy since joining the alliance in 2004, and building closer ties to NATO is also based on cultural reasons, as noted by Research Participant H:

“If your interest is in International Affairs, I would argue they (Estonia) certainly lean West politically, you know along with the other Baltic Nations part of NATO and that’s... I don’t think it’s just a pragmatic security thing. There’s also a want to disassociate with Russia almost.. you know, the emphasis is that they are Western. It’s also even though the discussion about this USSR passed, it’s something that society as a whole has not really come over it somehow.”

(Research Participant H, 03.04.2018)

So, while Estonia is reliant on NATO for security and defence purposes, it is not just about defence alone. It is particularly striking in the interviews conducted that most felt while Estonia is reliant upon foreign powers for conventional defence concerns, the interviewees noted that cyber security was an equaliser, where Estonia could defend itself, and indeed lead as a ‘niche’ player in alliance politics, rather than be an economic and security burden to other larger nations within those alliances.

“security is always very important for Estonia, and people largely share that understanding. It’s different in other European countries. It’s also pride, national pride. I think that in Estonia we became this digital forefront... became a source of pride, and it dates back from the nineties, you know, why people want to do it... and it all links to the trust, but people enjoy Estonian, being the place where digital innovation is adopted because it was the thing that took us... well, when we became independent in the nineties we were lagging behind from Western Europe, but we very much wanted to be part, and at the forefront like... a civilised western country”

(Research Participant A, 01.02.2019)

A focus on cyber has given Estonia ‘its place’ in the ‘civilised west’, and Estonian security is intimately linked to this (and must be secured against the perceived uncivilised east). However, there is also a fragility to the nature of such security. Nearly all research participants suggested an acceptance that they could not ever be 100% secure in ‘cyber space’ and that cyber security involved an acceptance of insecurity. This was perhaps reflective of a general, national sense of insecurity (for instance, also noted by Herzog, 2017). The Estonian response to this insecurity has been a focus on transparency and accountability, even in the event of flaws such as those which impacted national identity cards in 2017¹¹ (RIA, 2018 & Research Participant G). Similarly, 2017 saw advance planning of the data embassy initiative – a means to secure the nation’s vital data in the event the territorial integrity of the country itself were to be threatened... in essence, ‘backing up the nation state’ (Robinson & Martin, 2017). The data embassy involves data storage itself being ‘backed-up’ in the embassy in Luxembourg, whilst others are planned to be hosted in Geopolitically friendly locations in the future. The data embassy is, in reality, a data centre, and an exploratory analysis suggests

¹¹ Notable flaws in the Estonian Identity Cards were discovered in 2017. These included several security flaws found in the ID card manufacturing process. In some cases, it was found that contrary to the security requirements, the ID card manufacturer had generated private keys outside the chip and in several cases, copies of the same private key had been imported to the ID cards of different cardholders, allowing them to impersonate each other. This has led to some strong critique of placing blind trust in manufacturers (see Parsovs, 2020 for a comprehensive analysis) although others have praised the Estonian governments handling of the crisis – in particular the transparency of the process, which maintained public trust (Korjus, 2018 & Hartleb, 2020).

that it would not satisfy the criteria of the Vienna convention to be treated as a full diplomatic mission under most contemporary understandings (Robinson et al, 2019). Nevertheless, the data embassy has been driven by the desire to ‘back-up’ the nation’s data and secure national X-Road driven e-services (mindful of the 2007 cyber attacks discussed earlier). The Data Embassy demonstrates Estonian contingency planning but also might be considered a trust-building exercise – reassuring citizens by ensuring the continuity of the state. The implied perceived threat to Estonia’s territorial integrity is, of course, perceived to be Russia.

Fundamentally, e-Estonia functions through a combination of technology, as well as the trust of its citizens, both in that technology, and trust in government institutions to maintain them and act in the interests of the country’s citizens. Whilst schemes like the data embassy might be dismissed as a ‘gimmick’ (Research Participant K: 27.03.2018), they also serve to reassure citizens that the government continues to innovate and evolve to protect e-Estonia (Robinson et al, 2019). How effective some of these measures will be as cyber threats continue to diversify remains to be seen.

The latest official Estonian Cyber security documentation (Estonian Cyber Security Assessment, 2019) identifies an increased public dependency upon digital services; a widening of attack vectors due to the growth of ubiquitous connected devices; an expectation that citizens must become informed security actors; and the threat of Russian disinformation as key cyber security concerns for the immediate future. This transformation of citizens as security actors mirrors developments in conventional security. Some scholars have suggested that the burden of everyday security is increasingly being transferred to ordinary citizens (such as Stevens & Vaughan-Williams, 2016). The consequences of such a situation range from a lack of preparedness or expertise for citizens to act in such a capacity, the anxiety it can inflict upon an individual, and even a sense of insecurity.

Everyday cyber security might also be understood as reflective of a wider environment of cyber securitisation, something which is fundamentally changing relationships between citizens and the state. While existing research on cyber securitisation has often focused on discursive reproduction through, for example, the media (see Hansen & Nissenbaum, 2009), this thesis instead argues that such securitisation is evident in the discursive reproduction of concerns and perceived cyber threats in daily life. Ubiquitous connectivity in Estonia inevitably turns citizens into cyber security actors. It alters the relationship between citizens and the state and turns digital professionals into ‘petty sovereigns’ imbued with the power to reproduce and reinforce the e-state, and even to forward e-Estonia as a political entity. The majority of ordinary citizens not linked to the tech industry hold no such power.

The decision to focus so heavily on the tech industry in Estonia upon re-independence and into the present day has made Estonia the most affluent Post-Soviet state. It has also made Estonia the sixth most unequal country in the world (Business Insider, 2017). Tech workers are paid good salaries by local and European standards while many other industries earn only a fraction of that amount (WorkinEstonia, 2020). This, alongside the close links between private tech industries and the Estonian government, has disproportionately empowered digital workers as integral to e-Es-

tonia and therefore Estonia itself. They are uniquely empowered to shape policy and the future direction of the country, being both the architects and reproducers of e-Estonia domestically (as opposed to the international visions set out in government policy and the English language branding of the e-state). Such inequality has been identified by Estonia's SDE party as a challenge to social cohesion, although this has largely focused on a growing urban-rural divide (ERR, 2016). However, the latest OECD report (OECD, 2019: 10) goes further, noting problems relating 'social disparities, including inequalities in life satisfaction or health outcomes, are high in some dimensions: between urban and rural, across regions, men and women, skilled and unskilled and citizens and non-citizens'. Digital professionals are largely clustered in Tallinn and Tartu and are considered skilled workers. Concerns about the gender pay gap have been addressed by Kattel (2020) and the tech industry is not sheltered from this. The subsequent section further explores some of these digital professionals' visions of how they see contemporary Estonia and the relationship between citizens and the state.

5.5 How Digital Professionals Understand Cyber Security in Estonia Today

All the research participants were asked what they felt cyber security was, or what it meant to them as professionals and citizens. The interviews and conversations took place in 2018, a year after a technical flaw in Estonian ID cards had been identified and addressed rapidly (BBC News, 2017). At the time, it led to local concerns that the Estonian digital state might not be as secure as it was once thought to be. Answers varied, ranging from a balance between state and citizen's responsibility, and also an acceptance of a degree of vulnerability, as illustrated below:

"Proper cyber security is only possible when you recognise you will not have a solution which will be secure forever, and that you can never be totally secure."

(Research Participant T, 27.02.2018)

Participant T's comment can be said to reflect the feelings of insecurity which characterise relations between some of the smaller former states of the Soviet Union and their contemporary relationship with Russia. A recognition that complete security from that threat is impossible and that you must simply do what you can 'with the neighbour you have' (Participant A, 01.02.2020). A crucial aspect of securing Estonia is based on Digital identities:

"For Estonia, I think we have taken a very logical approach, focused on citizens. We have provided the secure digital identity, as part of our compulsory ID scheme"

(Research Participant G, 09.04.2018)

However, the functionality of digital identities requires establishing and maintaining citizens' trust (both with the prerequisite ID cards and systems with personal data) as well as in terms of using them. What is a 'logical approach' for an Estonian digital professional is not logical everywhere, as noted by Research Participant T:

“I have a hard time understanding foreign countries that think in this way. it is unusual to us, and it isn't just the British. I mean, you share so much with so many service providers... google... banks... but you won't share things with your government!? I think I would trust the Estonian government as much, if not more, than these private companies”

(Research Participant T, 27.02.2018)

Whilst many western nations (particularly in the Anglosphere) display low trust in their government institutions, Estonia, as with many of its Nordic neighbours, maintains relatively high levels of trust (Høybraten, 2014). The aspect of trust emerged throughout the research, and whilst those interviewed felt that they perhaps did not like the government of the day, they did trust the institutions which maintain e-services and maintained the nation's cyber security. In short, they trusted their fellow Estonian digital professionals, and this, in turn, professionalised the state. Their trust consequently informed their willingness to utilise e-services. This suggests a quite comfortable relationship between citizens and the state, or certainly in so far as digital professionals are concerned.

“I can't speak for society as a whole, but I see the mindset in the cyber security community... and that's something... we all know those people that developed the foundations of the digital ecosystem... so you know them, or you know those who know them... it gives you that trust... it's something we made ourselves... not at a distance... and we have contributed to it. It validates and creates trust for ourselves... we have a sense that we know what we get, and we know what we have isn't perfect, but we know how and who put it together, and with what intentions... it's a huge aspect of trust, and it leaks into wider society as well”

(Research Participant O, 06.02.2019)

Fundamentally, trust underpins the operation of governmental services, and the functionality of e-Estonia more than any technology can, and as highlighted above, it is easy to see why trust comes easily among the digital professional community in Estonia. This research found that whilst people trust the secure digital identity programme, mobile identities, and the identification process involving national identity cards, these were not the only aspects involved in ensuring Estonian cyber security.

“these things are different in the UK and Germany for example... people see the government as something to oppose... here I think it's related to are geopolitical situation because we are concerned about Russia... so we tend to trust our civil defence forces or police, and even the Estonian Defence League, even if trust in the political parties themselves might be low... or lower”

(Research Participant M, 07.03.2018)

Implicit trust was placed in the individuals charged with maintaining the security of e-Estonia (both in the authorities and in citizen volunteers such as the defence league). This remained stable even when trust in the elected government was eroded. This is also reflective of a pattern that suggested that personal cyber security concerns did not always

align with national security goals. Issues that concerned participants included the integrity of their personal data, personal communications, the security of their financial details, and the security of smart devices they use on a day-to-day basis. This was noted by many including Participant K, who noted the disconnect between national security concerns and the perceived threats of ordinary citizens:

“Security and perceived threats and then actually what matters to, you know, everyday people... I think (there is) a bit of a divergence.”

(Research Participant K, 27.03.2018)

One way that Estonia is seeking to address these challenges is through regulation. Whilst this regulation is improving (at least across Europe, to some extent, with the introduction of GDPR) there is still work to be done to improve personal data security. This is arguably of increased importance to Estonia, given the ubiquitous connectivity it relies upon:

“Personal data is definitely a concern Estonians we have a medical data online for access to prescriptions etc... so in theory, this could be a concern right... having all of this data online... but we use blockchain technology to secure match of that data... so this is you know... mitigating it... secondly we don't have one server where all this data is held... so we have this distributed data storage system called the X Road... so we take care that everything is as distributed as possible. as a country we always have to be afraid... or aware of potential cyber attacks from other countries... so for one thing Estonia has secured themselves or ourselves against”

(Research Participant Q, 10.04.2018)

However, in general, concerns over personal data were lower than might be typically expected from a group of highly qualified and dedicated digital professionals. Existing research has suggested that leading digital professionals generally view themselves as significantly more security-aware than other lay users, whom they consider to be a security risk (Albrechtson & Hovden, 2009) This reflects the findings of Priisalu & Ottis (2017), who concluded that concerns over personal data in Estonia are relatively low. They argue that this is due to the systems of accountability implemented by the Estonian government – something frequently cited by participants in this research. Most participants involved expressed an acknowledgement of the fallibility of their personal and private data, and that they were prepared to accept this degree of risk for the services provided. Other concerns such as the security of financial services, of smart devices were less trusted and are discussed later.

Some participants expressed concerns surrounding smart card services, including contactless payment cards issued by private companies. However, they inherently trusted their state-issued ID cards and the system of digital identification. They also suggested that this attitude was generally reflective of wider public attitudes:

“Very few will tell you (be able to explain) the technology behind it, and how they know it is secure because of the encryption and the decryption process involved... I mean, you’re talking 0.01% of the population will be particularly familiar with this. So it comes down to trust”

(Research Participant C, 14.02.2018)

There was also some degree of agreement between participants about the identification of threats. Participants continually identified threats to national cyber security which closely mirrored those identified in official government strategies, with Russia the most frequently mentioned perceived threat. Participants also mentioned China and Iran as rogue actors with limited respect for privacy and norms, and also somewhat surprisingly, the United States:

“I think Europe has something of a reputation of being like ... sticking to some democratic values... it’s different compared to the U.S. or China or whatever... because China and I suppose in the U.S. It’s always this ideological deregulation....”

(Research Participant H, 03.04.2018)

This emphasised the importance of strict regulation in building trust with citizens and failing to do so endangered that trust. Other notable contributions cited the government’s handling of prior cyber ‘incidents’ had enhanced public trust. For example, the flaws identified in 2017 (BBC News, 2017) had done little to undermine trust in the security of the cards themselves and research participants often suggested the way the flaws had been handled by the Estonian government had actually served to improve public trust in Estonia.

“the way it was handled solved any concerns we had”

(Participant E, 06.04.2018)

“I don’t think we particularly suffered”

(Participant G, 09.04.2018)

However, one participant did suggest that e-Estonia has now reached an almost untouchable stage, where it is impossible to properly critique or seriously change track if you are invested in the e-state as a digital professional:

“Of course, people will try to make it as secure as possible, but it’s an impossibility to admit if you can’t do it, like if there’s a problem”

(Participant K, 29.02.2019)

Trust is high, yet there is a clear limitation to how much Estonia’s digital professionals can criticise the e-State. Estonia is undoubtedly somewhat unique in this regard. Additionally, others commented that while Estonia benefits from high trust in its governmental institutions, as many Nordic states do, it has a unique Post-Soviet political landscape,

which had perhaps normalised governmental surveillance in the past. Participants also favourably compared the current Estonian political climate to the Soviet era, emphasising their pride in self-rule, and how ‘anything’ would be better than the past experiences of Soviet / Russian rule. (Soviet and Russian were frequently used interchangeably within the interviews by participants). Russian meddling was also considered a threat that good citizens should be aware of:

“So once or twice a year, for example... this now goes back to the Russian neighbourhood... We are in the sphere of influence... or shall we say interest of Russian secret services. So once a year or so there is some kind of incident... so it’s definitely the case that the Russians are trying to fish around here. So... one thing that definitely should happen, is citizens should support incidents, and I hope they do”

(Research Participant C, 14.02.2018)

The Bronze Soldier cyber-attacks of 2007 were also frequently discussed, referencing the Estonian government’s reaction, and how this increased trust in the state to act in the cyber security interests of its citizens, mirroring the security flaws of ID cards in 2017 (Research Participant T, 27.02.2018). These attacks were seen as pivotal, and as a trigger for domestic action, but also further international collaboration (see chapter 8 for further discussion on this) in the pursuit of increased security. Furthermore, these attacks were seen to be of inconvenience for ordinary users and can be viewed as a departure from more normative cyber security approaches, and instead of a move towards more human-centric security. The importance of everyday accessibility was emphasised by Participant J as crucial to the uniqueness of Estonia;

*“The unique thing is that first, we do *everything* online.... as I’m sure you noticed from spending so much time here, is that Estonians are really closed people.... so whenever you can avoid talking to other people, you just find the alternative... and we go crazy if, for whatever reason, things stop working!”*

(Participant J, 29.02.2019)

The above speaks to the uniquely close connection between the Estonian state and its digital professional citizens. There is a marked top-down nature to these relationships in Estonia. In terms of influence, the state leads, followed by digital professionals, and then everyday citizens (who might even be considered a considerable risk to the security of the e-state by those digital professionals and wield the least political influence):

“I think bluntly to say stupid people are an issue ... a lack of common sense would be diplomatic”

(Research Participant R, 01.03.2018)

The comments by Participant J above emphasise the need for human-centric security, but also security that is accessible. Delegating cyber security responsibilities to ordinary citizens who are not comfortable with technology (or ‘lack common sense’ as put by Research Participant R who considered uneducated citizens as a key cyber security risk for

Estonia) is not ideal. This then becomes a security dilemma for the state. Nevertheless, despite these issues, e-Estonia has been concluded to be a notable ‘policy success’ (see Kattel & Mergel, 2019). However, as Kattel & Mergel also highlight, the political, social and cultural values of Estonia are highly specific and may be difficult to replicate in other locations – particularly in the anglosphere or other nations that do not enjoy high trust in public institutions.

5.6 Performing e-Estonia

Identity and nation branding is integral to e-Estonia, both domestically and internationally. It also seems pertinent to draw upon another of Butler’s conceptualisations, that of ‘performativity’ as a lens to explore the idea of e-Estonia. Butler’s research into performativity suggests that it is the act of reproducing elite-level speech acts through everyday conversation – the re-iterative power of discourse’ (Butler, 2010). Subsequently, these speech acts are reinforced through the norms of society. It might be further conceptualised as how practice and knowledge are articulated are performed (Barnett & Vaughan-Williams, 2015). In this context, Estonians might be seen as reproducing their identity as e-Estonians, re-enforced both by the assembled idea of e-Estonia as ‘the digital society’, but also as a performance of what they are not – the Soviet (or Russian) other. This re-enforces existing research that has suggested the Baltic and Soviet (or Pre and Post-Soviet Russian) identities fundamentally compete with one another and also crucially conflict in terms of historical narratives (see Morozov & Fofanova, 2016, for more). Other researchers have noted that e-Estonia and the e-residency programme, in particular, are a source of nation branding for Estonia. This markets the nation as outward-looking and inclusive, providing progressive and positive meanings as a marked departure from the negative Post-Soviet imaginary (Tampuu & Masso, 2018).

This might also be seen to highlight the socially constructivist nature of security. The fear of Soviet / Russianness is reproduced culturally, politically, and socially by Estonia’s digital professional class. It is not only a demarcation of modern Estonia but also an ontological security project for Estonians in the sense that it reinforces the value of Estonia as an independent nation, markedly different from the struggles of the past. It also highlights Estonia’s value to the wider international community. It has been noted, however, that this security may not be extended to all of Estonian society (Soll et al, 2015). Digital professionals’ attitudes to cyber security and their engagement with the digital in everyday life is informed by both the positive e-Estonia narrative favoured by official governmental discourse (that of course, many digital professionals are actively involved in creating professionally) and the negative, ‘othered’ image of Russia which is perpetuated digitally as well as through contemporary geopolitics. This negative discourse might be evidenced in the popular imaginary of Russians as threatening, sinister cyber hackers, a perceived hostile force willing to interfere in its neighbour’s affairs, or informed by the memory of the Soviet past. This is also somewhat shaped by the contemporary notion of the Russian minority in both Estonia and neighbouring Latvia as being problematic and unwelcome other inherited from the Soviet era (see Cheskin, 2015).

Performativity in this context is concerned both with how digital professional Estonians navigate-Estonia, but also with their security concerns. It is an expression of power as petty sovereigns, intertwining a popular geopolitical narrative with concerns of everyday cyber security. These interconnected factors, informed by multiple geopolitical, so-

cial, and cultural factors, shape everyday cyber securities. This performativity is a re-iteration of what e-Estonia is, but also what it is not. It is re-iterative and produces governmental security policy, media discourse and everyday geopolitics in daily life. In cyber security terms, performativity can be seen in the way people interact with their connected devices, and navigate (or choose not to navigate) the security concerns they present (Amicelle et al, 2015).

An additional performative aspect of e-Estonia, which became apparent during the research process, was an emphasis on collaborative, as well as individual security and the idea of ‘chipping in’ to the collective security of Estonia. This is personal but also emphasises a sense of responsibility for the participant’s immediate social circle. As noted below by Participant E, this security is performed through routine and personal responsibility, but also the act of ensuring those around you are also security-aware:

“To talk some more about security and threats... I think it is a very good way to control to educate your workers or employees, and to keep your work stuff secure. Mmh... through that some kind of confidentiality agreements and some kind of penalties.... You wouldn't use that within the public sphere though. So one of the key interests is now the this great push to make cyber so... you know, that citizens know the cyber security act isn't everybody's responsibility in some way or another. I was at a talk the other day, and one of the guys speaking said, you know, you're only as strong as your own social network because if you're speaking to someone you know, who is reckless with their personal data and you're sharing in some way yours, then you're only as strong as they are.”

(Participant E, 06.04.2018)

This sense of ensuring the security of others (and the nation) and being burdened by such responsibility echoes Butler’s petty sovereign research (2004). Instead of feeling a responsibility or a sense of empowerment for national security, Estonia’s digital professionals instead are cyber security actors. There is also a performative nature to Estonian cyber security policy and this is evident in the notion expressed by a majority of participants that citizens were, in some way, responsible for the collective security of the nation digitally. They also had a role and responsibility in performing actions securely in the cyber domain. Failure to act in such a way was, in the eyes of Estonia’s digital professionals is both risky and un-Estonian. Responsibility on the individual for security was the burden of the individual, or at last to be shared by individuals and the state:

“Of course...I think understanding.... it is pretty commonly held still that you are primarily responsible for yourself... and that applies online and in dealings in the digital space... and whether people are able to meet that obligation themselves... and how much is the cyber community doing to equip and assist people... there's awareness-raising initiatives fairly regularly to engage with regular citizens. On one hand you this thing that it's your life, you are responsible for it... whether it's the regular physical world, or online... but the other side

of that is that service providers and the state provides tools and education that enables that security online... and strengthens it when possible. But it's shared in this regard really. "

(Participant O, 06.02.2019)

This was not universal, however, and it was also emphasised that leadership on such matters must come from the top. Whilst Estonia was generally at the forefront of pushing reforms, there was still a need for stronger leadership and expertise from political leaders pushing notions such as cyber hygiene¹²:

"Well, I think... I think everyone does yes in this day and age... I think citizens do have a responsibility to be mindful of what they're saying and what they are doing online as we have moved into this weird era of fake news and of disinformation campaigns, we are getting more desensitised to these things, and I but we but we have to go but we need to stay on guard. So and I think that's at the personal level and but also I think that our leaders need to be they need to try to be more educated. You know, we're beyond... we're beyond the conversation where you know, the internet is a you know, a connective, you know tubes the inner tubes are all connected, you know, we should we should have moved beyond that but we still have leaders that still don't understand the basic concepts. "

(Participant B, 08.03.2018)

This comment might also be interpreted as support for more technocratic governance and a statement of belief that Estonia's political leaders should have at least an equivalent level of knowledge of Estonia's digital professionals. However, exclusively technocratic approaches have been criticised in existing research such as by Kurtz & Meyer (2019), who have noted the limitations of such approaches to conflict prevention. Meanwhile, Cianetti (2018) offers a robust critique of the 'hollowness' of Estonia's technocratic approaches to governance. Cianetti argues that such approaches have weakened civil society and failed to address domestic issues such as the political exclusion of the Russian-speaking community as well as issues of domestic inequality, instead overtly focusing on neoliberal economic policies which have only benefitted a narrow subsection of the population. These observations coincide with the findings of this research. There is a hint of elitism around the e-Estonia project, and technocratic approaches might most closely be associated with the electorally successful Reformierakond, although Keskerakond have continued such approaches in their coalition governments. Cianetti (2018) has suggested that the Post-Soviet era in Estonia has been defined politically by a succession of governments focused entirely on narrow, economically-driven goals. e-Estonia has been an extension of that, leaking into the everyday lives of citizens and altering the relationship between citizens and the state.

¹² Cyber Hygiene is fundamental cyber security best practices that practitioners and users can undertake to ensure the best possible security. The idea behind the term is that it should become routine or mundane, much as regularly washing hands and brushing teeth is conventionally hygienic

5.7 Connected Devices and Everyday Life in Estonia

Research participants also forwarded the idea of reclaiming agency as a means of navigating everyday cyber security concerns and whilst far from the norm, the refusal to utilise things like contactless payments (Participant C), the refusal to use a smartphone (Participant K) suggest that technological refusal as one way to take back control from the creeping influence of technology in everyday life. However, concerns over human agency are not always evidenced through technological refusal. Some participants wanted to distance themselves from technology altogether. Others had concerns with different connected devices and why they were needed. Whilst many appreciated mobile and smart card technology, and often the governmental e-services which could be accessed and enabled by them, they were sceptical of the need for, and vulnerabilities generated by smart homes and ubiquitous connected devices. Others performed everyday cyber security through the choice to attach camera covers to their devices, whilst some simply felt maintaining ‘cyber hygiene’ (as encouraged by both employers or governmental agencies) was enough. There was a separation made by digital professionals in terms of the necessity of certain digital services. Camera features and IoT devices in the home were optional but e-governance services were essential.

Security concerns with connected devices inform citizen engagement with e-Estonia, especially when these connected devices, specifically smartphones, digital identities, and identity cards are increasingly utilised in everyday life. Whilst ideas of an impending cyber war, or even the potential of hybrid warfare akin to Ukraine to occur in Estonia seem grossly overstated (see Trimbach & O’Lear, 2015 & Kasekamp, 2015), such concerns dominate cyber security policy, along with the protection of infrastructure and state assets (Robinson & Hardy, 2020). A general anxiety around the possibility of cyber or ‘hybrid’ conflict was identified by some participants:

“cyber war... or an attack... there are many definitions... These things have the potential to influence the population, which in turn has an influence on our international relations with other states. So it is a threat.”

(Research Participant C, 14.02.2018)

“we were the first to be targeted by a cyber campaign or cyber war in 2007, from Russia, so Estonia was the first to be attacked this way by a foreign nation, or at least it was the first really recorded or we made something of it”

(Research Participant N, 23.03.2019)

This evidence suggests that Estonia’s digital professionals are swayed by geopolitical concerns to some degree, and from their empowered positions they re-enforce these geopolitical visions in both their professional and day-to-day lives. Estonian policy meanwhile is growingly attentive to the need for the state to engage with the everyday cyber security concerns (see Robinson & Hardy, 2021), however, more can be done to engage with non-technical Estonians, particularly relating to securing everyday smart devices.

Another aspect of e-Estonia's performative cyber security is the spirit of volunteerism, which the research participants from the Küberkaiit (Estonian defence league cyber unit) were particularly happy to discuss¹³. This, for both Participant J and Participant N was what was unique about the cyber security landscape in Estonia, as well as the state-led encouragement to engage with e-services securely;

"J: Yeah, what else.... there's all government services, from the moment the ones in the last ten years, I can't recall one where you can log in with just a password and a username, or its limited functionality when you do that, so all our systems you need two-factor authentication... and to take the ID topic further, when we talk about encryption of emails and documents, where internationally you would use end to end so that the person you want to see it can only see it by decrypting it. So you take it from a national security perspective and Estonian defence league, where we have 26,000 volunteers who (sic - where?) by default, all the information relating to the association is sensitive, so if you send this information over the email, and even if the email account the person doesn't use two-factor authentication or someone is reading those emails, unless they have the ID card of the other person and they know the pin code then they cannot open any files... if there's malware in the computer already, then it's a different story of course"

AH: Do you think the existence of the defence league is very uniquely Estonian?

J: Ummm... in this kind of sense... when we have 26,000 people.... uhhh I did these sums during a masters course... but it's something like 2% of the population. So pretty high"

(Participant J, 29.02.2019)

"Also, the cyber defence league is one of its own... we're not the only country with such defence forces, but the first cyber, with volunteers. And as this cyber stuff is new, we were innovative... I'm not sure if that's unique, but it's interesting, and we're trying to get things started"

(Participant N, 07.03.2018)

This spirit of volunteerism has been vital to the foundation and maintenance of e-Estonia and is an example of a performed behaviour in an everyday setting (Butler (2010 & 2012)). Volunteerism might be seen to ease some concerns of e-Estonia elitism (as mentioned earlier), however, only the technologically capable can volunteer to defend e-Estonia (the less technologically gifted might instead be able to volunteer to the other kinetic branches of the Estonian defence league). This division of the technical and non-technical is trivial in terms of defence force voluntarism, but it is reflective of some significant cleavages in Estonian society, as explored further below.

¹³ The Estonian Defence League (Kaitseliit) is a voluntary organisation aimed at protecting Estonia. The Cyber Unit (Küberkaiit) provides reservist tech workers who give their spare time to contribute towards national cyber security. The Küberkaiit has won much international attention due to its novelty (see Cardash et al, 2013 & Valeriano & Maness, 2015)

5.8 A Tale of Two Estonias? e-Estonia and Post-Soviet Estonia

e-Estonia is something of a Post-Soviet economic marvel. Estonia is the most affluent of all Post-Soviet nations per capita and is notable for its rapid modernisation (OECD, 2019). This can be created to the continuity of stable, liberal democratic governance which has characterised post-1991 Estonia, where, in spite of who was President, Prime Minister, or within Estonia's governing coalitions¹⁴, the tech industry has been recognised front and centre as crucial to the future prosperity of the Estonian nation.

The future path of Estonia has received near-unanimous political approval, thanks to the economic benefits it has provided the nation. This was identified by the research participants, who noted the stability this had provided, but also perhaps a lack of political choice:

“We've been more or less governed by the same political party for the whole duration (of re-independence) if you look at the over the last 20 years.... the majority government... it's always been centre-right”

(Research Participant R, 01.03.2019)

The 2019 election changed things, as outlined earlier (5.2). Whilst Estonia has predominantly been governed by centrist-right, neoliberal parties since re-independence (most notably Reform, but also Res Publica and Pro Patria, which have now merged as Isamaa). The 2019 election is perhaps best characterised by the dramatic rise of EKRE (Eesti Konservatiivne Rahvaerakond, or in English, The Estonian Conservative Peoples Party).

EKRE fit the general mould of many contemporary far-right parties in Europe. They are largely defined by their outrageous views (by Western European standards). These include, but are not limited to xenophobia, racism, and homophobia. Yet they also, as with many European Populist right parties, engage in anti-elite, anti-intellectualism (see Mudde & Kaltwasser, 2017) to appeal to the 'left behind' classes within society. It has been suggested that EKRE has exploited some of the economic arguments that would often be more associated with left-wing politics. However, as with other nations in Central and Eastern Europe, because of the legacy of the Cold War era, left-wing politics has become so minimised, presenting fertile ground for the far-right to exploit (see Petsinis, 2019 & Kattel, 2020). This did in some way reflect some of the remarks of research participants regarding contemporary Estonian life, leading participants to note that many older people were struggling financially (Research Participant P, 11.04.2018). There was also a suggestion that modern society had eroded a sense of common national purpose that had existed, for example, during the Soviet era:

“a sense of collectivism and community isn't as strong as it was even 10-15 years ago”

¹⁴ Estonia's Riigikogu elections utilise proportional representation. No government has held an absolute majority under this format since independence was resumed in 1992.

(Research Participant S, 01.03.2018)

These reflections came prior to the 2019 election and whilst they cannot in any way be taken as an endorsement of EKRE's far-right populism, they do recognise some of the failures of the status quo, which EKRE sought to exploit in their campaign.

Critics have also attacked EKRE's anti-immigration stance as nonsensical as migration to Estonia is extremely limited, despite EKRE's outcry that refugees and migrants supposedly threaten the character of the Estonian nation (Petsinis, 2016). Consequently, in the absence of any meaningful statistics on migration, it has been noted that Estonia's populist right instead leans heavily on conspiracy theories and emotions to back such narratives and also reach out to the perceptions of rural Estonians, uncomfortable with the direction of modern Estonia, who feel disenfranchised, aggrieved or left out of the future direction of their country (Kasekamp, Maddison & Wierenga, 2018). Consequently, it can be argued there exist two Estonia's. EKRE, for right or wrong, speaks in some way to many of those who feel left out of the e-Estonia global vision. In 2019, EKRE took considerable support from rural Estonian-speaking areas (Talving, 2020). These areas, with low salaries and little investment, are a manifestly different Estonia when compared to the liberal and affluent urban centres of Tallinn and Tartu. This directly contrasted not only with the observations of some research participants but also ethnographic experiences in the field, which suggested a commonly-held belief by many Estonians that Estonia was a classless society, especially when compared to the author's native Great Britain:

(Discussing the immediate Post-Soviet era) *"we had very little separation between people and government was very small. We felt... and I suppose still do feel that we are governed by 'one of our own'... where as in England... you have this legacy of governors... being the same class for hundreds of years"*

(Research Participant T, 27.02.2018)

Existing research has challenged this particular narrative (of Estonia as a classless society), instead suggesting that widespread support for national emancipation did indeed enhance public trust, however, it glossed over class divides within society at the time (often between Estonian and Russian speakers) but also created new ones. This class divide, argue Hellemäe & Saar (2012), emerged in the generation 'active during societal change' and the consequences of these new Post-Soviet classes have yet to fully play out. This change was observed by one participant:

"everybody had an equal starting point in the 90s, but now we don't anymore... people want you to think that you can still get there purely through your own merit, but it's not really like that anymore... I think there was a research. I can't remember which... Cambridge or Oxford... that right before the financial crisis, Estonia was one of the countries in Europe that had the biggest wealth gap... Yeah, we have a very, very big wealth gap in this country"

(Research Participant S, 01.03.2018)

Whilst EKRE did not speak exclusively against a perceived internal, digital ‘elite’ in their election campaigning (they instead preferred a narrative attacking ‘Russians, refugees and Europeans’ or more specifically, a skepticism of EU institutions), they successfully cut through in their anti-elitist messaging (Kasekamp, Maddison & Wierenga, 2018). Again, while their ‘anti-elite’ attacks were not specifically directed at the tech industry, their conspiratorial approaches attack a silent elite that supposedly controls the country (which they have, somewhat strangely, continued to employ in government - See McKenzie, 2019), represent attacks on the status quo of e-Estonia. Thus, it might be argued that e-Estonia is at least a part of the ‘elitist’ or ‘globalist’ vision that so repels EKRE. e-Estonia is fundamentally European and Internationalist. It subscribes to a neoliberal worldview that is outward-looking and seeks to bring fresh talent, technology and ideas to Estonia (Cianetti, 2018). It is the antithesis EKRE’s vision of isolationism. EKRE’s vision of Estonia might thus be more of a ‘Post-Soviet Estonia’. Another Estonia also exists that is closer to the extreme Social Conservatism of Poland and Hungary (for a comparison of Jobbik - Hungary’s far-right - and EKRE, see Petsinis, 2019), and which has frequently been evidenced within Ukraine in the Post-Soviet era (see Mudde, 2014).

The disparity between incomes in Estonia is stark and has been capitalised upon by EKRE (McNamara, 2021). It is even openly advertised by WorkinEstonia, a website encouraging foreign workers to apply for positions in Estonia. They advertise that while the average salary in Estonia is €1,200 per month, the average salary in the IT sector is nearly double that, and indeed that a team leader could expect triple (WorkinEstonia.ee, 2020). They do not mention that the minimum wage is only €584 (Eurostat, 2020). This extreme wealth disparity was noted by research participants when talking about the risks of their smart devices and why these can now vary based on your income:

“I would prefer not to have one myself the contactless cards I think there is too much comfort ahead of security... I don't agree with the possibility that if someone finds one they can just use them and even the €20 limit in Estonia to a pensioner can be a lot of money”

(Research Participant P, 11.04.2018)

“in Estonia and I'm sad to say, that most of those elderly people don't have access to more than a couple of €100 in their bank accounts”

(Research Participant Q, 10.04.2018)

While contactless payments are far from limited to Estonia and are increasingly common across Europe, the amount of risk attached to their use increases for those on low incomes. As noted by our participant above, while such an amount may be trivial to some, it is a lot of money to many in Estonia. As noted earlier, Estonia’s average income is deeply divided based on industry. When the industry of affluence is also associated with some of the ideas diametrically opposed to those of the far-right, as this chapter illustrates, it may become their next target.

Indeed, Duxbury (2020) notes that the Estonian tech industry is already aware of the impact of the Estonian coalition government, which it is argued, made the country unattractive to foreign talent. McKenzie (2019) further notes that there are many Estonians who felt ‘left behind’ by the digitalisation of Estonia. They are excluded not only economically but also socially and politically. While the e-Estonia boom has arguably driven the transformation of the capital Tallinn and the nation’s second city Tartu (most noted as home to the country’s most prestigious University), many rural areas have not been so fortunate. This combined with a decreasing population continues to feed the idea of an existential threat to Estonia itself, or at least the Estonia that EKRE and their voters consider to be Estonia, which they argue has been, until now, dominated by the liberal, urban intelligentsia at the expense of ‘the people’. Thus, as already argued by Kolga (2020), it can be argued that there are two Estonia’s. There is e-Estonia, which has dominated popular international narratives (particularly within English language news outlets). It has won admirers across the west, as noted earlier in this article by many research participants, for its features but also its effective PR and public diplomacy. It is also dominated by digital professionals who hold disproportionate influence compared to ordinary citizens. In sharp contrast to the general positivity of e-Estonia, there is also a Post-Soviet Estonia, where salaries are poor and many of the benefits of e-Estonia are less felt. This is evidenced in this chapter both by some of the thoughtful responses of research participants as well as observations of the contemporary political environment of Estonia. Regular citizens, unlike the digital professionals who participated in this study, were not actively involved in the creation of e-Estonia, nor are they economic beneficiaries of the e-Estonia boom. Nevertheless, they are subject to the security demands and digital dependencies ubiquitous e-Estonia has created. This creates a fascinating and at times complex relationship between the state, citizens, and everyday security.

5.9 Conclusions

This chapter has addressed the relationship between the state, the citizen, and everyday cyber security in the Estonian context. It has been suggested that this is changing over time, as the e-state changes, and Estonia has matured as a democracy, citizens’ relationships with the state have come under pressure. This chapter has illustrated some of the unique circumstances which have led to the development of e-Estonia and the challenges of the Post-Soviet Estonia it stands in stark contrast to. This chapter has highlighted the privileged role of digital professionals in creating and curating e-Estonia from its creation to the present day, and the burden this at times represents. This chapter also highlights that e-Estonia forms a significant aspect of the modern Estonian identity, but this is not universal. There is an orthodoxy among Estonia’s digital professional class, who acts as its evangelists. Yet recent political events suggest that modern Estonia’s identity is contested politically – not everyone buys into the e-Estonia vision.

A notable challenge for e-Estonia is the relationship with neighbouring Russia. Nearly all research participants in this project demonstrated either an active or passive concern about the Russian state interfering in either the e-governance of Estonia or threatening the digital liberties of its citizens. Threats were generally externalised, yet arguably the biggest threat to the e-Estonia project lies within Estonia’s borders. This chapter notes that trust has been crucial to ensuring secure e-governance in Estonia, yet the rapid growth of a populist far-right which indulges in conspiracy theories (Kasekamp, Madisson & Wierenga, 2018) points to a less trusting relationship than the digital professionals

in this study suggest. The rise of EKRE is a new Post-Soviet cleavage in a divided society. Estonia's EKRE Government Ministers cast doubt upon their own country's electoral system (and particularly online voting), as being run by elites and a supposed 'deep state' (RT, 2020). This poses a significant challenge to e-Estonia's future.

This chapter also illustrates digital professionals' orthodoxy of thought pertaining to e-governance in Estonia. The matter has been almost entirely depoliticised according to the digital professionals this research engaged with. This can be evidenced by remarks about the government of the day not mattering (by research participant T) but also in the almost universal praise of a system they were either heavily connected to or actively created themselves. Digital professionals, as technical experts, enjoy power and political backing. This has yielded positive impacts on the living standards and freedoms of many Estonians to date. However, it has not benefitted everyone in a nation with a startlingly low minimum wage and a striking disparity in pay between different sectors of the economy. The biggest challenge e-Estonia may face is that there are two Estonia's. One, e-Estonia, a long-standing, sociotechnical project of ubiquitous connectivity, digitalisation, and e-governance. The other, is a Post-Soviet Estonia, marked by poor social cohesion, a growing far-right political presence, and significant inequality.

6. Estonia's Cyber Insecurities: Geopolitics & Russian Influence

6.1 Introduction

This chapter focuses on some of the geopolitical and everyday insecurities expressed by participants, and answers the research question: *Are cyber security concerns changing wider geopolitical and security concerns, especially in relation to Russia?* Everyday insecurities are said to be growing, and states are increasingly concerned about the growing hybridisation of threats. Various cyber threats are widely recognised as a vital component of such hybridisation (see Galeotti, 2016, Lanoszka, 2016 & Mälksoo, 2018). This chapter notes the unique vulnerability of Estonia to hybrid attacks and disruption, given Estonia's national dependence on digital services. The chapter reflects upon how Russia projects power and insecurity in the Baltic region, via increasingly different means, including soft power, perceived disinformation, and propaganda, which are also identified as aspects of hybrid threats. Estonia's digital professionals are part of the battle against hybrid attacks. This chapter also argues that Estonia's geopolitically sensitive location and ubiquitous connectivity heighten feelings of insecurity. It highlights that e-Estonia's digital professionals also consider connected devices to be a potential security concern as they are another attack vector through which the e-State can be threatened.

Estonia's ubiquitous connectivity poses its own challenges, as does the growing ubiquity of connected devices. Trust in Estonian self-governance, following the repeated occupations of the twentieth century, has provided a 'trust credit' (Research Participant P, 11.04.2018) to the Estonian government and enhanced public trust in e-Estonia. It has also allowed the ad hoc development of e-governance, which would come with sweeping human security concerns in other contexts. This ubiquitous e-governance and high levels of digital dependency have paradoxically created greater trust in Estonian national services and fostered a high level of distrust in private online enterprises. This manifests in the distrust of neighbouring Russia, characterised by concerns with disinformation and interference with Estonian sovereignty.

The Estonian approach to secure e-governance is informed by both conventional and everyday geopolitics. These, in an Estonian context, frequently cast Russia as a rogue actor in cyberspace, much as they also cast Russia as a conventional security threat to Estonia's territorial integrity and independence. Consequently, increased attention is required to maintain the integrity of e-Estonia, and to respond to these new 'hybrid' threats which spread insecurity.

Other notable new threats include 'disinformation' and connected devices. Opinions on e-Estonia's everyday security have been shaped by the experiences of others in Post-Soviet space in recent years – most notably Georgia and Ukraine, as well as the 2007 'Bronze Soldier' cyber attacks on Estonia. These experiences have bred insecure anxiety in Estonia which informs everyday geopolitics and also by extension influences attitudes to cyber security and e-governance.

6.2 Estonia & e-Estonia's Geopolitical Insecurities

Estonia, as reflected upon repeatedly within this chapter (and wider thesis), is a small country. Being a small country alone is often the cause of considerable security dilemmas, especially relating to larger powers within the global system (Steinsson & Thorhallsson, 2019). Small states are often reliant upon larger powers and alliances as guarantors of their territorial integrity. Furthermore, there is a long history of smaller nations being entirely subsumed by larger nations and empires, or being wiped from contemporary existence, through the progressive imposition of social and cultural norms of those larger powers, as well as language (for more on the challenges of small nations, see Thorhallsson, 2006 & 2012). There are also particular sensitivities in the Baltic region, given the troubled history of the area. A series of occupations represented a significant challenge to the individual identities of these smaller states, whose language and identity have been threatened by numerous occupiers, including most recently the Soviet Union. Upon the resumption of Estonian self-governance, significant value was placed upon the protection of Estonian identities, including language and culture as being distinctly Finno-Ugric. Such moves were mirrored across the Baltic states, as both Latvia and Lithuania also sought to protect their individual cultural identities, focusing on their unique Baltic nature to set themselves apart from the recent Soviet past¹⁵ (Berg & Ehin, 2009).

Consequently, from a security perspective, the continuation of the state as a unique cultural object and shared heritage has since thus been the defining thing which must be protected – especially from a threatening larger neighbour. This has also been exacerbated in Estonia's case by the declining birth rate among Estonian speakers (ERR, 2017) which has reinforced the narrative of an existential crisis or threat to the nation further. This is something that has also been seized by the populist far-right in Estonia, as highlighted in the prior chapter (see 5.2 and 5.7).

Significant value has also been placed upon finding 'uniqueness' and value in the wider international community so that Estonia is notable and offers something to the international community as a sovereign state. After all, plenty of non-sovereign countries exist within larger nations, and some with significantly more rights than others. (Notable examples around Europe include Scotland, Catalonia, and the Basque country). Whilst not independent states, each has its own distinct identity and many within these countries desire sovereignty. The past also demonstrates that nations and groups can fall out of existence. In the Baltic region, Livonian is now an extinct language, devoid of native speakers and only kept alive by a dedicated few¹⁶. A clear concern for many Estonians is the preservation of Estonian sovereignty, culture, traditions, and values, as well as the preservation of Estonia as an independent nation, lest it becomes another Livonia, a people and language now reduced to a novelty of the past. Existing research has established that population and demographic change are perceived as an existential threat to Estonia. Preserving the Estonian population and language is intimately linked to ideas of Estonian sovereignty (see Kuus, 2002 & Aalto, 2003). How-

¹⁵ Latvia and Lithuania identify both culturally and linguistically 'Baltic' as opposed to Estonian, which is instead 'Finno-Ugric' and most closely tied to the Finnish language. Other notable Finno-Ugric groups include Hungarians and the Mari and Komi minorities in Russia. (see Kuznetsova, 2020 for more discussion on the 'Finno-Ugric world')

¹⁶ Estimates suggest only around 200 Livonian speakers remain. For more on the history of Livonia, see Kasekamp (2010)

ever, there is a sense that Estonia is inherently fragile in this way, due to its small size (Crandall, 2014). Estonia has sought to assuage these threats by offering free language lessons to all new residents and has heavily invested in the digital preservation of the Estonian language (e-Estonia, 2017). This sense of preserving Estonia digitally is demonstrable in some of the discourse from interviews, as below:

“We can’t be big... but we can have influence... For Estonians, our e-governance... our cyber expertise... it’s about proving our worth... So we want to be the first with this and that... There’s this idea that we are threatened by our neighbour. There’s maybe a feeling that no one would care about Estonians if we were not important for some other things... So we want the world to remember us if anything were to happen!”

(Participant H, 03.04.2018)

What emerges is also a sense of fragility, and that for Estonia to survive, it cannot just exist but it must also actively proactively contribute and influence beyond its borders. This is also achieved by proving its value to its allies. This existential anxiety is sourced from the nation’s turbulent past, and also contemporary events across the Post-Soviet world, as highlighted further in the following section. The decision to adopt e-Estonia model can be seen as reflective of wider, non-digital fears of the vulnerability of the state (Aalto, 2003 & Kuus 2002). e-Estonia has also arguably made the nation more resilient, ensuring the protection of Estonian independence digitally through the data embassy (Robinson & Martin, 2017) and providing the nation with more ‘digital’ residents or ‘e-Estonians’ through the e-Residency programme (Kotka et al, 2015). More contemporary research meanwhile has suggested that Estonia has always been an anxious or reluctant European (Vilson, 2021). This does make some of the ‘borderless digital society’ and e-Estonia’s internationalism all the more surprising.

The Post-Soviet era, in much of the former Soviet Union, has been tumultuous, due to the legacies of that era such as the redrawn borders, the legacy of centralised governance, the democratic deficit, and the contested spaces left in the aftermath of the collapse of the union. Toal (2016) argues that such contested spaces in both Ukraine and Georgia (Crimea, Donbas, Abkhazia, and South Ossetia respectively), alongside tense political situations and geopolitical manoeuvring by the Russian state, have contributed to a fearful atmosphere within the wider Post-Soviet space. This fear is exacerbated by an increasingly assertive Russia. In this regard, Russia is perceived to be reasserting historic territorial claims, asserting the protection of Russian-speaking minorities (whose presence is often due to the legacies of Soviet resettlement policies) as justification for intervention into the territorial integrity of its neighbours. This argument is extended, to suggest those in the supposed Russian ‘sphere of influence’ may thus be subject to paranoia due to proximity. This is reflected also in arguments that Russia perceives NATO’s eastern expansion as encirclement, and such actions are justified (In the view of realist international relations) as means of reasonable defence (see Mearshimer, 2014).

Sakwa (2017) discusses a series of grievances that shape the Russian security and defence agenda, as well as Russia’s view of the world. Sakwa notes that this conflict stems from different ways in which Russia and ‘the rest’ perceive the

world. While the Western Powers pursue a Kantian peace (spreading liberal democracy as liberal democracies do not make war upon each other), Russia sees its security and the world system through a wholly realist lens, based on reciprocity and mutual benefit. Russia sees the advance of NATO not as the spread of liberal democracy and self-defence but rather as aggression which must be countered. Furthermore, Russian grievances are not limited to NATO expansion alone. Considerable value is also placed on the protection of Russian speakers as well as the preservation of the historic memory of the second world war (and particularly the role of the Soviet Union in defeating the Nazis). These issues have also soured relations between Estonia and Russia.

Russia has repeatedly accused Estonia of failing to address the rights of Russian-speakers in Estonia, has highlighted Estonia's refusal to acknowledge the Soviet war effort in defeating the Nazi's and even accused Estonia of overlooking Nazi collaboration among Estonians during the Second World War (Trenin, 2020). Estonia forcefully rejects these accusations and is an outspoken critic of Moscow, as it was during the latter days of the Soviet Union – a position which further angers Moscow (Liik, 2021). However, there is a semblance of truth in some of Moscow's grievances. Estonia has continually failed to address the memory of the Second World War and to this day contains several troubling monuments to Estonian SS legions erected since independence, something which Moscow views with arguably legitimate offence (see Weiss-Wendt, 2008 and Katz, 2010). Similarly, over 75,000 Russian-speaking Estonians still only hold 'grey' or 'alien' passports and are not full citizens of Estonia (ERR, 2019). The failure of Estonia to address some of these issues continues to shape the geopolitics of the region.

Elsewhere in the former Soviet Union, Russian grievances have spilt over into interventionism. Moscow views these actions as legitimate given the west's intervention in a number of conflicts, most notably in former Yugoslavia and treats criticism of those actions by the west as hypocrisy (Sakwa, 2017). Toal (2016) focuses his research on the 'near abroad'¹⁷ upon Ukraine and Georgia, highlighting the notion of 'Russian interference' in Post-Soviet space as being geographically disparate but geopolitically motivated. Moreover, he illuminates the everydayness of the Post-Soviet geopolitical landscape and illustrates the impact this has upon ordinary citizens. Other research has highlighted how everyday fears and insecurities of citizens can be linked to wider, macro-scale geopolitical narratives (Pain & Smith, 2008), and these are increasingly evident in this Estonian case study. Yet, as the interview data and existing research has established, these narratives are not new, albeit they have been exacerbated by recent events. The Estonian government has sought to counter these narratives by building trust with citizens. This is reflected in the focus on transparency and service-based design of the e-state. This is, however, coincidental rather than by design. Solvak et al (2018a) have demonstrated how service design was ad-hoc and developed gradually over time. Whilst, as identified earlier in chapters 3 and 5, Estonia, as with many of the Nordic nations it would happily seek to identify itself with, has a high level of trust generally in government institutions, this trust has not been developed in the same way:

¹⁷ The 'Near abroad' is terminology utilised by Toal (2017) which he has drawn from Russian policy to refer to the newly independent states of the former Soviet Union, including the Baltic states

On trust: *“We’ve been independent for such a short time, we’ve never known much different... and what was different before was worse... so maybe this will change over time. It’s different to Scandinavia. Maybe their trust comes from the welfare state. We don’t have that here”*

(Research Participant S, 01.03.2018)

Instead, trust has been established gradually, through implementation (often without consultation with citizens), but also Post-Soviet economic necessity. Some participants even suggested that initial trust was a form of blind patriotism that would be tough to replicate elsewhere:

“The people who have influenced and introduced these systems are our own... and we have no negative legacy in this regard.... so I can see how this would be difficult to introduce this way of doing things in a different country”

(Research Participant T, 27.02.2018)

The newfound patriotism upon the resumption of independence combined with the lack of historic problems (such as corruption) assisted in the smooth adoption of and acclimatisation to the e-state (Kalvet, 2012). This is distant from the citizen-centric views suggested by the official e-Estonia website (2018). Trust is imbued through a mixture of patriotism and pragmatism. The opportunity to exercise sovereignty and a fear of the alternative creates a unique environment where technological innovation has thrived. It has additionally created a distinct attitude to cyber security, e-governance, and ubiquitous connectivity. This attitude holds that it is both vitally important, and a matter of national survival, but also, is somewhat realist in its acknowledgement that Estonia has little else to set a nation of its size apart:

“it mainly has the e-Estonia narrative and that’s one day using very very effectively. And so that’s what makes Estonia you have a country that is actually branded as an ‘e-Nation’. You don’t find any other country that has it like that”

(Research Participant D, 20.03.2018)

It can be argued therefore that the e-state is intimately linked to Estonia itself, as it is what gives the nation renown and value on the international stage. Securing e-Estonia is also securing Estonia, and cyber security is more crucial for Estonia than most other nations. e-Estonia, like Estonia, is shaped by everyday anxiety of Russian domination and subjugation, but also an existential crisis. This is driven by a fear that Estonia could, like the Livonians, cease to exist if pragmatic sacrifices are not made:

“the population is famously shrinking as well. There’s some kind of feeling of inferiority that we are not that important and so on and probably the first instance when this digital approach was discovered for Estonia... so besides our existence, I think probably people buy into it as a way of validation of value”

(Research Participant H, 03.04.2018)

e-Estonia is then a form of digital resilience, reinforcing sovereignty, language, and Estonia's uniqueness. Accountability and traceability were also emphasised by participants as key to building trust in the technology of e-Estonia. However, based on this input, these were both a distinct second to nativist trust, i.e. a patriotic belief in innovation purely because it is Estonian. If a system was built by Estonians, for Estonians, to the ends of building and preserving the Estonian state, it is inherently good and trustworthy. This trust can also extend to levels that would be considered naive in other nations that are not a product of the same circumstance, as noted below:

"I think the Estonians do have less reason to distrust their administration... in part because they have the feeling that this is now their country... and if not to us, whom else shall we trust? So if we don't trust ourselves... well, we've got big of this big brother, Russia, right? and he's not always been the best brother... So we build our own country, and we trust the technology... we just build it so if someone abuses that technology, we can catch the guy who did the bad stuff! "

(Participant D, 20.03.2018)

This has also bred an orthodoxy of attitudes to matters of Estonia's cyber security and e-governance. As highlighted in chapter 5, politically, Estonia has been stagnant for many years (until the recent, growing challenge of far-right populism). Nearly all major political parties since the resumption of independence have subscribed to the vision of a neo-liberal, hyper-capitalist, flat-tax Estonia (Cianetti, 2018). It has been argued that the bland ineffectiveness of successive Estonian governments has failed to properly address many of the political challenges that Estonia faces, which stretch far beyond the e-State (Petsinis, 2019). The failure to address issues such as inadequate pensions, the gender pay gap, a growing urban-rural divide, and relations with the Russian-speaking community are all highlighted by research participants in this thesis and chime with existing research also. This is a problem that some critics have claimed has been compounded by an ideological obsession with digital progress. This has become tied to the contemporary Estonian identity to such an extent that criticising it is also critiquing Estonia itself (Kattel, 2020). Recent political events such as the 2019 election and the growing far-right influence in Estonia since 2015 should prompt some debate on whether the same civic culture can be maintained whilst balancing increasing demands on the e-state, such as the proliferation of smart devices and contemporary ubiquitous connectivity.

6.3 e-Estonia's Smart Devices

As established earlier in this thesis, the contemporary world is changing the relationship between citizens and their smart devices. In a world of increased connectivity and increased digital services, and the increased capability of devices, there is also an increased reliance on their functionality. Estonia is no exception. Of course, some devices are more ubiquitous than others. As this chapter is focused on the relationship Estonians have with e-Estonia, the discussion here focuses on the two smart devices most commonly used by Estonians to interact with their online services. They are also perhaps the most ubiquitous of smart devices (even beyond Estonia) – smartphones and smart cards. As

the capability of these devices grows, so does their role in a complex security relationship, with real-life, human consequences (see Coles-Kemp, Jensen & Talhouk, 2018 for more).

While devices can create a degree of positive security through empowerment in the security process, which in turn can enhance trust within e-governance (Roe, 2008), they more often than not generate negative feelings such as insecurity or fragility (Herzog, 2017). These might be seen as reflective of the wider Estonian contemporary security landscape. However, this insecurity is heavily individualistic and is typically closely related to conventional security concerns (Vaughan-Williams & Stevens, 2016) as well as everyday geopolitical influences (Hansen & Nissenbaum, 2009).

Many conventional security concerns are subject to geopolitical influences (see Pain & Smith, 2008), and connected devices can generate expressions of everyday geopolitical sentiments. As this section argues, this is influenced both by concerns about the sourcing of hardware and software, and the supply chain on which Estonia is reliant (and was highlighted by the ID card crisis of 2017 [Parsovs, 2020]). Furthermore, Estonia in the Post-Soviet era has strongly favoured deregulation where possible (The enforcement of regulation being reminiscent of the Soviet era, and consequently to be avoided at all costs [Cianetti, 2018]).

“We have this efficiency from the governmental side, which is our tax system... this is also a kind of a benefit for me as part of his nation that we have. Our government is doing a good job and is not losing money having paperwork or whatever other progressive rules to do my taxes.... it’s not wasting my tax money.”

(Research Participant F, 06.04.2018)

The idea of progressive taxes being a ‘waste of money’ does not fit the Nordic nation branding that Estonia has frequently pursued. However, branding is seen as a necessity also to attract businesses to Estonia (Mäe, 2017). Participants frequently mused upon Estonia’s relative size, and also noted that developing internal regulations is quite difficult, both because Estonia is such a small market, and also due to a feeling that regulations can stifle business innovation. In terms of devices, production is highly distributed internationally across a private sector driven by profit. Regulation, particularly in Estonia, which is heavily driven by technological innovation and free enterprise, would be difficult and unpopular to implement. Participant A mused upon some of the issues regarding the supply chain. Whilst ostensibly discussing the issues with Estonian ID cards in the 2017 incident, they noted the wider implications of Estonia’s size, and an inability to influence, to any great extent, private companies, even within Estonian borders, but also beyond

“the security of the supply line... that’s universal. But definitely also for Estonia... we had the issue concern us very concretely with the ID card crisis a year ago... this was a crisis of the supply line.... whether they consider the government of Estonia as a big enough client to inform (of a problem), I mean... Estonia might not be a big

enough part of the food chain, but the whole country is dependent on its ID / chip card... so there's that, but more generally, when we build larger departments... I'm thinking of NATO headquarters here... it's very difficult to keep on top of the whole supply chain"

(Research Participant A, 01.02.2019)

This also implies a certain feeling of vulnerability, insecurity or again, an acknowledgement that digital devices are difficult to secure because of the multiple factors at play in the design, manufacture and implementation process. This is also applicable to the smart device supply chain, which is often complex and utilises wide-ranging hardware.

Others noted the limits to what a government can do, in regards to the provision of absolute security. Ultimately, the answer may lie in cooperation and supra-national coordination which still, some participants felt, remained relatively lacking. Estonia, as a small state actor, has limited influence in such matters, although has wielded disproportionately large influence in shaping cooperation on a European and NATO level due to its specialisation in this field (Crandall, 2014 & Hardy, 2020). Yet, as Participant G discusses, it is difficult for Estonia to lead in this area:

"Well, I think this is almost a question of how far can a government go? It's.... uh... its not... it's a global, corporate vulnerability also. So you can't have a nation state solution to it. With a lot of these other issues it's the same. You can have European standards for example... but no nation state, particularly one of Estonia's size... probably not even a nation state of the UK's size alone, would be large enough to enforce industry standards by itself... so, it's not a nation state solution. It's an issue of products and services, and questions of accreditation, so we need a situation where you require certification and accreditation for that market. So America, or the EU can set standards for products to circulate within their environment, and if products do not meet these standards, they cannot be available for retail."

(Research Participant G, 09.04.2018)

Security collaboration at the European level represents an opportunity for Estonia to help coordinate standards in device security but also demonstrates a key vulnerability of e-Estonia – its smallness. The accomplishments of GDPR represent a significant step in terms of securing data, with emphasis on the security of citizens (Albrecht, 2016). Yet, not all software, much as hardware, could be trusted and this, Participant A, felt, required more significant action:

"It requires courage... and political wisdom... that it should be the policy... or good practice that government officials shouldn't use Yandex Taxis¹⁸.... we take a position on Huawei... or we take a position that we don't use Kaspersky Anti-Virus tools... so from one end its no nonsense, not to use Kaspersky tools if you consider Russia to be your prime security threat, but it's not down on paper anywhere"

(Research Participant A, 01.02.2019)

¹⁸Yandex is a private business which operates on a similar model to Uber (app based 'ride sharing', and also food delivery), but is headquartered in Moscow. It has received some criticism for supposed lack of data integrity, although the company insists it is fully compliant with EU regulations (see Bloomberg [2018] for more information)

The need for ‘courage’ and ‘regulation’ here held a distinct undertone of popular geopolitical visions, where the west and western technology is inherently good, and the Russians (and the Chinese) and their technology are automatically perceived to be bad or a threat to national security.

“If someone decides to do something... the Russians... or the Chinese or whatever. They’d probably still go for a denial of service attack, for disruption reasons.”

(Participant D, 20.03.2018)

While Russia is seen as the most likely source of any potential attack (largely due to political motivations or geopolitics aspirations in the region as discussed in 6.2) there is also an underlying feeling that Estonia is perhaps more aware of this than the rest of its allies. The comments of required ‘courage’ and ‘political wisdom’ hint that these might already exist within Estonian political thought, but could perhaps be more widely implemented amongst Estonia’s friends (for example, the participant also bemoaned lax Finnish approaches to Russia within this interview). Whilst this might be overly simplistic, it does infer a general characterisation that technological solutions are only to be found in the west and that private companies from the east were inherently less trustworthy because of their governments perceived hostility (Research Participant A also suggested that Kaspersky, a noted Russian antivirus software producer, should not be trusted by virtue of their location). However, this does highlight some of the inherently geopolitical concerns relating to connected devices and demonstrates the inherent geopolitics of cyber security.

6.4 Why e-Estonia’s Devices Matter

In Estonia, e-government systems utilise both smart cards and smartphones to function securely, via two-factor authenticated mobile and digital identities (e-Estonia, 2019). As the access to systems increases, and the number of connected devices in our daily lives proliferates, so do the number of potential attack vectors (see, for example, Capellupo et al, 2017 & O’Neill, 2016). This only serves to highlight the need for everyday cyber security, as citizens are increasingly connected and increasingly dependent upon connectivity to carry out their daily lives. It also highlights how different issues arise and notes how these can be mitigated (Such as Volkamer et al’s 2015 sociotechnical analysis of mobile phone and contemporary security threats) as well as how everyday security should be mindful of geopolitical factors. It is also worth noting that the participants in this research are experts within their field, and whilst from these concerns we can extrapolate insights into everyday life, it should be noted that these concerns are informed by education and/or professional expertise beyond the average citizen. This was reflected upon by some participants. Indeed, they noted that for the average citizen, some of these concerns might be elevated again, and that also, the security of the nation is less a concern for the average citizen, but personal security is instead something they can take more ownership of. Furthermore, the citizen using the device can be a security concern for security professionals, as well as the device itself:

“Most of the main problems that you see are really silly, mundane, human errors.... the sort of things that are totally preventable... so that’s our biggest challenge”

(Research Participant O, 06.02.2019)

“So... I think that personal cyber security is more of a priority... or, I worry about it more because I can do something about it... not a national level, I don’t really worry about it, because there’s nothing I can do about it”

(Research Participant R, 01.03.2018)

“It’s hard to speak for the average citizen... I can only say, based on what I deal with... or what I have noticed in ten years of cyber security training.... is that people are a common concern. People give away their own credentials too easily, and fall for phishing emails too easily... but that’s the same everywhere....”

(Research Participant J, 29.02.2019)

Citizens are a crucial aspect of the smart device security conundrum, and the interaction between citizens and their devices represented for the above research participants, and a new potential threat to the e-State. While some considered smartcards generally a threat, it was noteworthy that Estonian identity cards were more trusted than others. Thus, trust in the government and governmental institutions also stretched to participants’ connected devices.

(on smartcards) *“so... that’s one of the things I’m not really worried about... one of the reasons is that... well... my wallet only contains three cards... one of them my Estonian ID card, one my local shop membership card, and the third my bank card... sure, in terms of the contactless, where you beep your card onto the register, right... I do use that. As a computer guy, as a security familiar person, I do get paranoid about it sometimes... but I do have all the limits in place, so even if it were to go wrong... I wouldn’t miss more than my daily limit would allow... it’s a risk I’m willing to accept for comfort...”*

(Research Participant N, 23.03.2019)

Many participants also discussed ways they chose to mitigate the risks they felt this technology posed, however, it was noteworthy that every participant inherently trusted the Estonian state systems, and the Estonian ID card, despite the 2017 weaknesses which were exposed (Korjus, 2018 & Parsovs, 2020). Some responses had a distinctly geopolitical narrative. Participants were often prepared to trust their state (and the digital space it has cultivated) without question. Instead, they questioned the supply chain outside of Estonia and lamented its insecurity. Some suggested that Estonia has disproportionately benefitted from a ‘trust credit’ (Research Participant P, 11.04.2018) while others were simply incredulous that other nations did not function similarly to Estonia:

“I mean, I think this might also be getting a little bit paranoid... but then it’s different in different places. We have had these ID cards for 15 years now in Estonia... but in the UK, people don’t really like this idea, and don’t understand this”

(Research Participant E 06.04.2018)

The interviews highlighted a wider theme discovered throughout the wider research project that Estonians fundamentally trusted the services provided by their government, with very little critical reflection as to *why* that was. Indeed, as illustrated above, many participants felt it was unusual *not* to trust the government in such a manner. This trust is extended to smart devices which access such services, and also general internet access within Estonia – a kind of sociotechnical patriotism. Yet, as illustrated above, this is not always extended beyond Estonian borders, where concerns over surveillance increase, and consequently more care is extended to smart devices and access to online services. Estonia is a place where you can be more relaxed about your digital security and your devices:

“So I think if I were to go to if there was a country that I was little more suspicious about I might actually take it (more precautions) but coming back and forth to Estonia... I’m not so worried”

(Research Participant B, 08.03.2018)

Much of e-Estonia hinges on the acceptance, and the active participation of citizens. Yet many might argue that the imposition of this e-state has arguably been tantamount to an everyday securitisation to the ends of services and convenience, but also, as far as the state is concerned, money. Lacy & Prince (2018) outline several scenarios based on increasing digitalisation. The most negative includes a scenario where the digitalisation of services cannot be challenged and is increasingly insecure for ordinary users but financially beneficial to states and large corporations. Cost-saving and rolling back the expenses of public services were one of the prime motivators of the creation of the Estonian e-state (Heller, 2017).

The e-state is convenient, but it is also a necessity that pushes cyber security into daily lives and reforms citizens’ interactions with the state. Existing research has concluded that the e-state is popular among citizens (as Kattel & Mergel [2019] conclude), and the participants of this research concur. It also works with an ever-increasing number of users of connected services (Solvak et al, 2018). The ‘trust credit’ referred to by Research Participant P above is arguably non-renewable and the product of the particular circumstances of the immediate Post-Soviet era (see Vassil, 2015 for more on this time period). Instead, more contemporary events such as the cyber attacks of 2007 are used as a unifying moment to preserve e-Estonia as a ‘national idea and value’ (as discussed by Kerikmäe et al, 2019). Yet, as prior chapters have sought to illustrate, this model, off the shelf, is simply non-replicable elsewhere. As Research Participant Q further noted:

“We use or e-id’s, or mobile ID’s, or smart ID’ offered by the private sector, because we know that they are trusted... they’re provided by a trusted service provider, our government.”

(Research Participant Q, 10.04.2018)

This does beg the question of what would happen if trust in the state eroded to a point where this was no longer the case? Estonia has ridden a patriotic wave in its Post-Soviet era and has been relatively scandal-free. While future challenges like the ID card flaws of 2017 could pose problems, as of yet, trust remains high¹⁹. Mobile IDs are also every bit as crucial as smart cards and further illustrate the importance of device security to Estonia's everyday security.

6.5 Managing Risk in e-Estonia

As devices are closely linked to the future of e-Estonia and e-Estonia's security, smart devices consequently become a matter of managed risk for the Estonian state, and for Estonians navigating their everyday cyber security. An emergent theme within the research was also the geopolitically informed narratives that perpetuated decision-making processes. Some participants felt that their real-world location informed how they interacted with their connected devices. Many travelled for work and held views on services they would and would not use outside of Estonian space. For example, Research Participant T who works for Blockchain developers commented that he uses a VPN, but not all the time, and was less inclined to do so in Estonia. Furthermore, there is a clear delineation of the perceived everyday risk is low, in terms of personal security, but that company security is thus to be treated as a more serious concern:

"We do (use VPN)... I do if I need to connect to company services... but for personal reasons... actually I don't. But I have been travelling quite a lot with work, to let's say unusual places... and there I have needed the VPN to access 'normal' internet. In Iran, Sudan, Saudi Arabia... or places like that, for example. However ordinarily, day to day, no. However, the company policy is very strict that we do use it for work purposes."

(Research Participant T, 27.02.2018)

This suggests a clear Geopolitical angle and anxieties attached to perceived cyber threats. Others, placed value on the integrity of private messaging, and whilst the majority of participants mentioned using VPNs in some way, the discussion often referred to specific instances or security concerns that bothered them:

"Encrypted messaging yes, definitely... VPN, maybe not so much. It'd depend on where I was... like China"

(Research Participant Q, 10.04.2018)

Whilst other places (largely informed by a western everyday geopolitics) were not deemed trustworthy, Estonia is. Other research participants remarked that they would treat the security around their smart devices differently in locations they perceived as more threatening. In a discussion about RFID blockers, VPNs and other risk mitigation strategies for smart devices, another participant suggested that they were largely blasé about such risks in Estonia, but...

¹⁹ Korjus (2018) discusses the Estonian governments reaction to the ID card 'crisis' and the positive reception of its handling by the public

“Maybe if I were in maybe if I went to Russia, then I might be a little more inclined to take that. I mean, I’ve just I’ve been told like seriously lock everything down. If you go to some of these countries”

(Research Participant B, 08.03.2018)

Russia and Russian space and influence are thus cast as threatening to devices and the integrity and privacy of personal data, whilst e-Estonia is the opposite. Such trust is crucial, not only to the e-state itself but also to the technologies and means to connect securely with it, as Participant N of the Estonian Defence League remarked in an interview:

“One of the biggest threats to Estonia is actually a lack of trust.... if we don’t trust our ID cards and every security.... if that trust goes away... so for an example, something like Donald Trump happens. Now, because of him, many people trust the USA less, as a firm ally... we can’t rely on them as much as we did before, right? So, if you take that trust away from the card, or the system, either by just bombarding it with things like ad’s, making it not secure... so maybe like the thing with the ID cards last year? (Reference to the 2017 ID card vulnerabilities) So the cards were vulnerable to attacks, right? If that would keep happening, like a java update... then we probably couldn’t trust it as much as we do now.. to you know, run pretty much every part of the life of an Estonian... from drug store receipts, government stuff, elections...”

(Research Participant N, 23.03.2019)

What becomes apparent is that while participants were willing to accept certain security and convenience trade-offs, there was ultimately a key trust relationship or a socio-digital contract between the governed and the government. A failure of the Estonian government to maintain that trust could have potentially disastrous consequences against the backdrop of perceived menacing security actors. Those menacing actors were generally authoritarian states and perceived to have no values of digital privacy (such as China, and Iran, and always key to perhaps any Estonian geopolitical considerations, Russia).

6.6 Geopolitical Anxiety, Insecurity, and Estonia’s Nativist Trust

It has been argued that small and mundane everyday interactions are increasingly digitised, which in turn has fundamentally changed the cyber security landscape (Aradau & Blanke, 2015). Increasingly banal and mundane daily interactions are underpinned by cyber security concerns, and ever more services are linked to internet connectivity. Furthermore, the internet is increasingly politicised and an information battleground. A widening and deepening of what ‘cyber security’ entails has been emphasised by critical scholars for some time (eg: Hansen, 2009; Dunn-Cavelty, 2015, Kello, 2017), and is increasingly becoming recognised within governmental strategies to include issues including information and disinformation warfare, issues of human security and insecurity. These nuances are all extremely evident in modern Estonia and are reflected in the comments of research participants. Issues such as supply chains as well as broader geopolitical debates and how they influence digital security and decision making, and the geopolitical anxieties which inform Estonian mindsets are evidenced in examines of recent traumas such as the 2007 cyber war:

“Well... one unique thing was the aforementioned cyber war of ten years ago... it has been happening time and time again since then. So it happened to Georgia shortly afterwards too.”

(Research Participant C, 14.02.2018)

It has been previously argued that the 2007 ‘cyber war’ emerged from the context of a historical conflict (Sear, 2017). This research has echoed prior findings which have linked the conflict to wider geopolitical concerns. The 2007 ‘cyber war’ was far more than a digital conflict and was also ideological and linked to a clash of identities between Estonian speakers and Russian-speaking Estonians (For further discussion of those competing geopolitical identities which spawned the 2007 conflict see Ehala, 2009). Historic and identity-driven geopolitical values can be seen as shaping the threat perception of research participants here also. Additionally, speculation surrounding the events in Ukraine and Georgia should be treated as unique, rather than as models for supposed ‘hybrid’ conflicts or ‘Russian interference’ with a ‘one size fits all’ model. Each conflict, whether in the Donbas, Abkhazia, or South Ossetia is deeply rooted within the particular social, cultural, historic, and political conditions of those regions. and cannot be simply explained away as Russia interfering in the affairs of its Post-Soviet neighbours, no matter the assertions of some critics who would hold that Narva would be the next Crimea (an assertion discredited by Kasekamp, 2015 & Trimbach & O’Lear, 2015). While such situations are widely considered as not replicable in the Baltic states, they have still generated an emotive response from research participants:

“there’s foreign threats but they’re most likely going to be in conjunction with other hostile activities... something along the lines of Crimea”

(Research Participant N, 26.02.2019)

It is important to note that each Post-Soviet conflict is deeply contextual. Sasse (2016) argues that individual, empirical studies are vital in understanding various conflicts which are shaped by local geopolitics. Estonia is linked to Ukraine and Georgia instead through larger-scale geopolitics, where those nations have sought closer ties to the west, which Russia has in turn perceived as a provocation (Sakwa, 2017). This is also evidenced in the everyday geopolitics expressed by participants. What can perhaps be argued is that we are not seeing a new cold war (Toal, 2017) but instead seeing the birth of a new, information-driven conflict via other means, where contrasting regional narratives play out through disparate sources through the means of modern technology as a messenger. This can be conceptualised both as a form of deterrence defensively, and offensively as a form of coercion. Digital deterrence is indeed the terminology utilised by the Russian government (see Tsvetkova, 2020 for discussion of Russia’s new ‘soft cyber power), and arguably Estonia is at the forefront of leading in digital deterrence (Hardy, 2020a). These digital forms of deterrence and coercion increasingly target ordinary citizens and challenge how we should approach cyber security (Manor, 2019).

Most participants involved expressed an acknowledgement of the fallibility of their personal and private data, that this was increasingly linked to their smart devices, and that they were prepared to accept this degree of risk for the services provided. This reflects some of the risk-service benefit findings of smartphone security by Volkamer et al (2015) and smart card security from Poller et al (2012). The Estonians in this research strongly favoured services over security, which might contrast with other European and Western nations (Poller et al, 2012). Other concerns such as the security of financial services, of smart device capabilities such as cameras and microphones, were less trusted, and reflect the findings of Sicari et al (2015) who suggest that the security-service balance will be key for the future of IoT security. Some research participants expressed concerns surrounding smart card services, including contactless payment cards issued by private companies, however, inherently trusted their state-issued ID cards (Participant N). Where there was some degree of agreement was the identification of threats, with participants continually identifying perceived threats to national cyber security, which mirrored that of government documents.

Other notable contributions cited the Estonian government's handling of prior cyber 'incidents' which had enhanced public trust. For example, the flaws identified in 2017 had done little to undermine trust in the security of the cards themselves. Indeed, research participants often suggested the way the flaws had been handled by the Estonian government had served to improve public trust in Estonia. Furthermore, the same participant suggested that while devices were important...

"on a purely emotive level, this isn't about devices, or technology, but the trust in a democratic government"

(Research Participant G, 09.04.2018)

This re-enforces prior statements regarding the trust of government institutions over the technology itself. Some felt Estonia is somewhat unique in this regard, yet not as convincingly as some of the popular media discourse surrounding e-Estonia might hold, backing the suspicions of Drechsler (2018) & Kerikmäe et al (2018). Some commented that while Estonia benefits from high trust in its governmental institutions, as many Nordic states do. It also has a unique Post-Soviet political landscape, which had perhaps normalised governmental surveillance in the past (Research Participant D). Participants also favourably compared the current Estonian political climate to the Soviet era, emphasising their pride in self-rule, and how 'anything' would be better than the past experiences of Soviet / Russian rule. (Soviet and Russian were frequently used interchangeably within the interviews by participants).

6.7 Disinformation

'Disinformation', or 'information warfare' is commonly considered as an aspect of 'hybrid conflict' in much contemporary literature (see Galeotti, 2016 & Mälksoo, 2018 for more). It is explicitly identified as a leading security risk by Estonia's cyber strategy (Robinson & Hardy, 2021). Disinformation as a term has considerable baggage, particularly in the Post-Soviet world. Indeed disinformation was a favoured tactic of the KGB during the Soviet era (disinformation being the direct translation of 'дезинформация'). During the cold war era, such tactics were employed to spread

suspicion and distrust among western governments, and ‘information warfare’ (информационная война) was also similarly found within declassified Soviet-era documentation (see Snyder, 1997, Giles, 2016 & Lanoszka, 2016 for a western view of the history of Russian disinformation). So while disinformation or ‘fake news’ has become a contemporary political phenomenon, combatting mendacious or deliberately misleading information is nothing new in the Post-Soviet world.

Disinformation being utilised as a means for a foreign power to infringe upon fragile Estonian sovereignty, as outlined in this thesis is of critical importance. Feelings of fragility and anxiety which surround the continuation of the Estonian state can also be linked with the threat of systematic disinformation threatening the e-state and the state alike. The security of the e-state, but also the insecurities of those who use it is shaped by the potential for malicious actors beyond Estonia’s national borders, to conduct disinformation campaigns and cyber attacks to disrupt the security of the state in different ways:

"Stuff like targeted propaganda is important. It's harder to counter, and it's growing in importance... but I can't really suggest how to counter it. For sure, Russia is threatening in this regard"

(Research Participant T, 27.02.2018)

The potential for outside influences to consequently shape the political narrative in Estonia is thus a key concern for Estonian security. This is arguably an intersection where national security concerns, particularly relating to when international relations with Russia meet the everyday security of regular citizens. This is heightened in Estonia due to the significant Russian minority in the country, who, so it has been feared, might prefer leadership from Moscow than from Tallinn (Hoffman & Makarychev, 2017). The conflicting identities within the country thus shape and inform everyday security concerns and consequently play out in the cyber realm too. This interchange of security, identity, and the everyday is discussed further in the following section (6.8)

More emotive comparisons by participants even compared Estonia to Israel [Participant A], a state surrounded by enemies. This terminology is used to describe the use of various, non-conventional aspects of interference. Whether some of these constitute warfare or a continuation of foreign policy is open to debate, but commonly recognised aspects of this ‘hybridity’ are said to include: the appearance of legality or respectability; the exploitation of local tensions; the use of force such as ‘little green men’ (military forces disguised as civilian subversive forces – a term that was specifically named by Participant N); targeted disinformation and more. For a summary of this in Ukraine, see Reisinger & Golts, (2014) and Lanoszka (2016). This can also include less conventional methods to take advantage of weaknesses in civilian infrastructure such as power. The potential for this was discussed by one of the interview participants at length:

"I'm in charge of a working group in the Estonian defence industry association... we look at the threats... and there's definitely a worry if you look at Ukraine... Over the weekend, I had a heating failure at my flat in

Tallinn... so I ended up coming back to Tartu, to be warm... and when that happened, it made me think, what if we had a major grid failure... like happened over there... and whether, when it's -29.. what could we do, and how could we safeguard against that? As part of the working group, it's definitely a worry... even if it's nothing we can do anything about."

(Research Participant S, 01.03.2018)

This insight was based upon an individual interpretation of the cyber attacks on Ukraine in 2015 which crippled the power supply to around 250,000 people in December (more information on this attack and further reflection can be found in Zetter, 2016). These concerns highlight the weaving of an everyday concern (the availability of heat in the cold Estonian winter), with cyber security, and also with the everyday geopolitical narrative of Russia as threatening. The BBC called the event 'a cyber attack from Russia' and then President of Ukraine, Petro Poroshenko, labelled the incident as 'cyber war' (BBC, 2017). The potential of that being replicated in the middle of winter in the Baltic states would be of particular concern. It is worth noting this particular interview was carried out in February 2018 in Estonia, during a particularly cold snap, where temperatures frequently dropped below -20 degrees celsius. The consequences of the power being cut for a significant time in the middle of winter would have extremely dangerous consequences for the civilian population. The ability of cyber attacks to threaten such services should not be underestimated, and, as in Ukraine, many services in Estonia are digitally vulnerable, with online attack vectors which could potentially be exploited to take down critical infrastructure.

Disinformation is also one of the crucial aspects of any hybrid conflict identified by interview participants, as well as a strategic priority of the Estonian state (Thompson, 2019, Robinson & Hardy, 2021). This is often drawn from a distrust of the Russian media's influence within Estonia. It is also shaped by the possibility that Estonian residents (I.e. the Russian community – see Erbsen [2019] for an investigation of the role of Russian media in Estonia) might also be the 'citizen curators of disinformation'. Such a term has been used to describe citizens of Ukraine, where participants of disinformation are said to have been sourced from local Ukrainian citizens who felt more loyalty to Moscow than Kyiv, but also non-official sources within Russia, seeking to sow division (see Golovchenko, Hartmann & Adler & Nissan, 2018). This highlights to a degree how the agency of ordinary citizens can shape, and also be shaped by disinformation narratives, and the everyday security connotations of cyber security. This has also been developed by others such as Jenson, Valeriano & Maness (2019) who have argued that there is a growing power of coercion and subversion relating to the advent of ubiquitous connectivity. They cite both Ukraine and the supposed Russian interference in the US 2016 election. Whilst they argue this to not have fundamentally shaped the result of the US election (indeed the recent Mueller report [2019] draws similar conclusions), they suggest it did raise levels of confusion and selectively manipulate the debate. The potential for this in Estonia is a common suggestion of participants in this research and mirrors similar concerns found across the Post-Soviet space where Russian speakers are a significant minority (Cheskin & Kachuyevski, 2019 & Suslov, 2018) and are often found in geographically isolated clusters. This is also reflective of the wider political climate of the west at the time this research was conducted, where blaming Rus-

sia for the domestic failures of the west has been argued as being ‘in vogue’ since the Brexit vote and the election of Donald Trump (Trenin, 2019).

Others have noted a degree of hypocrisy in such critiques. Indeed, the ‘hearts and minds’ aspect of any conflict long predates the age of ubiquitous connectivity and has characterised modern conflict for some time. Mejias & Vokuev (2017) note as such in discussing these tactics. They also suggest it is easy to point to parallel tactics utilised by democratic regimes in numerous conflicts and that both democracies and autocratic regimes participate in such disruptive tactics. These are both key challenges to citizens’ everyday securities, going forward, and illustrate further how geopolitics are inseparable from cyber security thinking.

Others have urged a more robust counter approach. Giles (2016) argues that the Russian state and associated non-state actors have exploited history, culture, language, nationalism, and more to carry out cyber-enhanced disinformation campaigns with much wider objectives. Giles’ critique is endorsed by NATO and suggests a more calculated and controlled approach than is perhaps accurate, given that it has been almost impossible to definitively identify that many attacks, such as those on Estonia in 2007, can be attributed to the Kremlin itself. Disinformation might be associated with certain, Kremlin-sponsored media outlets (Sputnik is Kremlin-sponsored, and also publishes not only in Russian, but Estonian too, whilst RT is widely spread across Europe) but the news is enthusiastically shared and distributed by many willing citizens who have nothing to do with the Kremlin (Tsvetkova, 2020). Moreover, such critiques remove the agency of individuals. Whilst research on the existence of troll factories and data manipulation remains in its infancy, the ability of click farms to sway public opinion needs further exploration. It has been suggested that these can have the potential to influence public politics by playing on everyday insecurities (Jones, 2019) but it is extremely difficult to determine who is behind specific bots and to quantitatively measure their impact. The narrative around Russian interference has also largely rebuilt the idea in the west of a powerful, subversive Russia as a continuity of Soviet, cold war era information warfare (Sakwa, 2017), albeit with a new, and relatively unknown cyber twist. Participants were also aware that such action is in its relative infancy, suggesting that Ukraine has been a ‘training ground’ for such techniques:

“Russia is using Ukraine as a cyber warfare training ground... research from these attacks have suggested they could have gone much, much further in the damage they caused... but it wasn’t done, they stopped... but various different tactics and techniques are being tried out to see what will happen.”

(Research Participant S, 01.03.2018)

This suggests that Russia might, having honed these skills, deploy them in the ostensibly more resilient, NATO-aligned Baltic states in the future. Given the inherent insecurities and fragilities of the Estonian security landscape. In such an event they would meet a more prepared adversary than Ukraine five years ago and Georgia in 2008. Nevertheless, Russia, the memory of the Soviet era, and other conflicts in the Post-Soviet world continue to cast a long shadow over Estonian security concerns. These are reflected in the online world, and in the daily, connected lives of citizens,

reflecting prior research which notes that these have inherently shaped Estonia's conventional security approaches (Kuus, 2002 & Crandall, 2014).

6.8 Everyday Cyber Geopolitics and Russia

Research participants were asked what they considered to be the main the common security concerns of Estonians and if they thought that these are commonly linked to ideas of national security. From this, participants frequently identified not only the types of threats faced by Estonia today but also who posed those threats:

“Conventional warfare today (targeting Estonia)... is probably not that smart an idea.... there are about ten different nations here (part of the NATO enhanced forward presence in Eastern Europe)... so there would be problems if you crossed the border... cyber is less like that though... you can just say it wasn't us, what are you going to do”

(Research Participant N, 23.03.2019)

As previously alluded to, in both the cyber and conventional security realms, Estonia's security environment is often defined by the country's relationship with Russia. This is shaped by the Soviet past, significant events since Estonia re-established autonomy, and now by a complex digital relationship. What emerged throughout the interview process, and is evident in both media outlets also, is a form of everyday geopolitics expressed by research participants that define national relationships with Russia, Estonian citizens' perception of Russia, and subsequently, perceptions of Russians. They form part of an Estonian everyday cyber geopolitics that informs perceived threats, and Russians were considered by participants the most likely to pose a digital threat:

“if they would like to attack us... the Russians... They'd probably still go for a denial of service attack, for disruption reasons.”

(Research Participant C, 14.02.2018)

The above notes a pattern of recent events such as the 2007 cyber attacks on Estonia, but also the continued poor relations between Estonia and Russia (see Utkin, 2021, who further analyses those poor relations). They also follow a pattern of Russian interference in its near abroad, something noted by multiple participants. The idea of everyday geopolitics can be seen to shape both public perceptions, and also in turn shape governmental policy. This can be driven by multiple factors including media discourse, perceived security concerns, popular culture, or reactions to political initiatives such as immigration or security policy (see Dodds & Dittmer, 2009; McFarlane & Hay, 2003; Williams & Boyce, 2013). This in turn often casts one group as either an 'other', a sinister or menacing 'enemy'. It reflects securitisation research, a process whereby something identified as a security concern is repeated until it becomes an accepted norm. It has been suggested this can happen at both macro and micro levels: i.e. relations between states, but also in daily life (Buzan & Waever, 2009).

Interviews also suggested that Russia is a source of cyber paranoia or at least some form of anxiety for many Estonians. Those working in the public sector were particularly concerned that their work accounts would be targeted by Russian agents, seeking access to classified information. Similarly, workers in firms that supplied technology to government institutions held similar concerns, that their firms might be targeted by either hackers seeking access to private information or that simply they might be targeted due to their association with the Estonian government. One participant (B) felt concerned about travelling to Narva, due to the proximity to the Russian border, did not trust Russian mobile networks, and felt the potential for Russian mischief-making. This reflects other work that has noted that Russia utilises cyber tools to disrupt the world order (Pigman, 2018). This is a narrative evident among participants:

“We’ve also seen different types of threats too, occurring more and more, are open manipulation attacks using social media, paid content in Russian-speaking media for instance... this has become pretty big recently. So the Russians are very good at using propaganda. Some people call them political campaigns, others call them brainwashing...”

(Research Participant C 14.02.2018)

“Trolling and social media is a threat I am increasingly concerned about”

(Research Participant A, 01.02.2019)

Consequently, as evidenced above, the spectre of a malicious Russia interfering in its neighbour’s sovereignty features heavily within the everyday geopolitics of Estonia. Participants in the research project frequently identified Russia as a threat to their cyber security, on a state level, and also on a personal one. There was also often a great pride in the idea of e-Estonia, being a signifier of a modern country, removed from the recent past:

“Being digital means not being Soviet... something like that”

(Research Participant L, 31.10.2017)

Many identified the idea that Russia was a source of cyber insecurity through the spread of ‘fake news’ or information that specifically pushed the political objectives of the Putin regime. Arguably, Russia has successfully weaponised disinformation in this way, and undermining public trust, through a multitude of state-owned, Russian language media outlets, as well as utilising social media, through both official accounts as well as supposed ‘Troll factories’ which supposedly flood popular social networks with Kremlin-funded propaganda (Galeotti, 2020). Not all research agrees with research participants on this matter, however, noting that the west does not need Russia to descend into infighting, nor is it particularly in Russia’s interests to widely undermine sovereignty when that is what the Kremlin values to the most itself (Sakwa, 2020).

Nevertheless, such is the level of concern in Estonia that such matters are explicitly mentioned as being of key importance in the Estonian cyber security review published by the RIA²⁰ (Estonia Cyber Security Review, 2017). Participants frequently identified the potential for this disinformation to sway internal political matters, as well as the possibility that it negatively affected and specifically targeted the Russian-speaking minority within Estonia, thus threatening national security (Participant S). The changing nature of cyber security as a conventional security concern emerged through this research, as participants identified multiple ‘real world’ aspects of cyber security. In particular, the Kremlin-sponsored Sputnik was identified as particularly troublesome, as well as other, less abrasive Russian language outlets available in Estonian territory (Participant G). These serve to feed long-standing concerns of Russian language media outlets as a source of disinformation in order to shape the geopolitical views of Russian-speaking Estonian citizens:

“A third of Estonia lives in a different media space... you can see this on a New Year’s eve in Tallinn... some of the city celebrates at 11pm: new year on Moscow time... and they (the Russian speakers) tend to live in a very different information space “

(Research Participant S, 01.03.2018)

These Russian language and Russian state-owned media outlets also pursue Russian foreign policy goals in the region, namely that of protecting Russian speakers in the ‘near abroad’ (Toal, 2017). Meanwhile, those more hawkish on Russia have suggested that Russia’s security is enhanced by the insecurity of its enemies (Giles, 2019). Yet it is equally arguable that the counter-narrative informs the everyday geopolitics of Estonians as much, given the near uniformity of views aired by participants in this project.

As previously mentioned, the ‘hybridity’ of the Russian cyber threat is written into official governmental recognition, featuring prominently in contemporary strategy (Robinson & Hardy, 2021). This further illustrates how cyber security concerns are influenced in Estonia by geopolitics. Contemporary research has observed perceived Russian notoriety in this field, utilising sophisticated disinformation campaigns to further political and strategic goals, and suggested that virtual weapons are a persistent irritant to international order (Mälksoo, 2018: 378). Arguably, this narrative has been weaponised by both sides, to further domestic political agendas. However, the Russian government apparatus conversely takes great glee in its social media outlets and political statements in suggesting and ridiculing the idea that Russian disinformation even exists, let alone is as powerful as its opponents often suggest. The general Russian stance, which is frequently perceived as both dismissive and aggressive by western nations (Manor 2019 & 2020) has bred nervousness in the Baltic states.

As established earlier, the Baltic states fear to some degree the replicability of the Crimean annexation and value the preservation of their independence above all else. There are considerable NATO forces now deployed in the Baltic region, including a British battalion in Tapa as part of the NATO Enhanced Forward Presence (McNamara, 2017).

²⁰ RIA (Riigi Infosüsteemi Amet) is the Estonian Information and Data Department.

Furthermore, as a NATO member, any perceived attack on the Estonian state would trigger a response by all NATO members and the enhanced forward presence is seen as a further guarantor of that security. This might also be seen as mirrored digitally by the presence of the NATO CCDCOE (Cooperative Cyber Defence Centre of Excellence) in Tallinn. Russia is aggrieved by this perceived expansionism of the west, especially into the former Soviet Union which it considers to be within its sphere of influence, but is not an irrational actor set on military confrontation with NATO (Sakwa, 2019), leading to the present geopolitical stand-off, that is hostile, but unlikely to turn into a full, kinetic conflict.

It is debatable, given some of the interviews conducted, that Estonia also benefits from this narrative of a threatening Russia. This geopolitical narrative has a continual, unifying effect regarding governance, as whatever the Estonian government of the day does, is considered preferable to the fear of domination from its neighbour (Cianetti, 2018). This echoes much analysis of the political benefits Russia receives. Some of the ideological basis of Putin's foreign policy goals are drawn from the narration of Russia facing an existential crisis, of Russian-speakers (or 'ethnic' Russians) under threat in the 'near abroad' and the perceived menace of NATO expansionism into the Russian sphere of geopolitical influence (Leichtova, 2014, Toal, 2016). Estonians meanwhile face a different existential crisis. A low population and declining birth rate were also mentioned by participants (such as Participant H), who noted the idea that the Estonian state could grow instead in the cyber realm. Thus, Estonians identified with the idea of e-Estonia as an everyday geopolitical symbol of the continuity of the Estonian state.

Crucial to 'hybrid tactics' is the potential of plausible deniability of state-level involvement. Russian state-controlled news outlets, as well as official governmental sources, such as the particularly undiplomatic Russian Embassy UK Twitter account (@RussianEmbassy), frequently extol the lack of proof as a means of casting doubt upon accusations of Russian cyber interference, as well as frequently sarcastically mocking any negative news stories as being the fault of mythical Russian hackers (Manor, 2020). The Russian Embassy of Estonia account (@RusEmbEst) frequently shares the tweets of other embassies as well as state-sponsored news outfits such as Sputnik, pushing Kremlin-backed foreign policy. The @Russia_MFA and @RussianEmbassy accounts have both been noted by Manor (2019) as "drivers of disinformation". Capitalising on the problem of attribution being difficult within cyber contexts, these accounts are used to spread doubt and question dominant western narratives, which invariably are labelled 'Russo-phobic'. These 'softer' cyber security issues can destabilise and disrupt international relations, geopolitics, and domestic politics alike. 'Hybrid warfare' akin to the conflict in Ukraine is not replicable in Estonia, and there was little suggestion from the interviews conducted that this is a genuine public fear. Nevertheless, some of the tactics find their way into the everyday concerns of Estonians working with technology:

"We have the neighbour we have... Russia is often malicious (to it's neighbours)... but Estonian security, not only in a cyber sense, are often more security-aware than others... We're like northern Europe's Israel... we feel our freedom is not guaranteed. We have to fight for our freedom. It's not an open war, but it's done by other means"

(Research Participant A, 01.02.2019)

Comments such as the above evocatively equate Estonians to Israelis and connect to an everyday geopolitical narrative of Estonia as uniquely threatened geopolitically and existentially. Israel famously claims to be surrounded by enemies wishing to destroy it, and this has led to many Israelis having a heavily securitised geopolitical identity, where security matters above all other matters (Abulof, 2014). This renders political discussions on matters of security and potential alternative approaches nearly impossible. It might be said that the idea of Estonia has been securitised in a somewhat similar way, whereby Russia is to be considered ‘the other’ or ‘the enemy’ seeking to destroy Estonia’s fragile independence. Any question or critique of the prevailing economic and security approaches of the government is roundly critiqued and hounded as ‘non-Estonian’ (see Kattel, 2020, who discusses such difficulties in his thoughtful critique of ‘Estonia as an idea’ as well as the attacks on President Kersti Kaljulaid for suggesting Estonia ought to maintain relations with Russia where possible). Moreover, Estonian technological exceptionalism ran through the opinions of research participants. Whilst other nations are also threatened by malicious cyber actors, Estonia, in the opinion of the research participants, is better prepared or more resilient to threats:

“although the Georgians, the French, the Italians to a degree... you will notice they have this fetish for technology, without properly thinking about what it means... But for Estonia, there is very little that you can’t do digitally.”

(Research Participant C 09.04.2018)

This digital exceptionalism reflected both Estonia being ‘better’ at cyber security but also highlights just how reliant Estonia is upon technology to set itself apart. Furthermore, there is also a sense that Estonia is both vulnerable but also better placed than most to navigate contemporary security challenges posed by Russia. This was, however, not a view shared universally. Discussing the matter of Estonian uniqueness, Research Participant D did not agree that Estonian approaches to security were unique, but instead that the ‘e-Estonia narrative’ was unique. This is both an approach to e-governance but also a distinct form of national branding, which outlines what Estonia is, and what it is not:

“Is there something unique to Estonia? Umm... a lack of people probably... a very sparsely populated area, the Soviet past... the threat from Russia.... but what else does the Estonian narrative have? It mainly has e-Estonia, and it’s a narrative they’re using very, very effectively. It’s what they have, and it’s what makes Estonia unique.”

(Research Participant D, 20.03.2018)

This suggests that often e-Estonia is sometimes more concerned with PR than security, but also that there is a close connection between the two. Estonia needs cyber security to be valued and that value is part of preserving the fragile future and independence of Estonia – by demonstrating Estonia’s value to the world.

6.9 Insecurities and Challenges

e-Estonia faces many future challenges, including; an increasing dependency on e-services; a dependency on connected devices; maintaining trust in public (and digital) institutions; and a poor diplomatic relationship with Russia which shows little sign of improvement. However, this negative relationship with Russia is simply a continuation of the Baltic States' combative approach to the Soviet Leadership in the final days of the Soviet Union (see Liik, 2020). It can be reasonably concluded that digital matters have a relatively small impact on these poor relations. Nevertheless, Estonia has used these poor relations to closely align itself with Europe and NATO in matters of cyber defence and has demonstrated its worth through its contributions to developing cyber norms, evidenced through both the Estonian presidency of the EU, and the Tallinn Manual contributed by the CCDCOE located in Tallinn (see 'small states as cyber norm entrepreneurs' by Adamson, 2019 for more discussion of how Estonia has established itself as a cyber power). e-Estonia is a product of present international relationships, the past, and the everyday, insecure anxieties of the present. Most participants acknowledged the inherent vulnerability of the cyber domain, and that it was 'impossible to be fully secure' (Participant J, 2018). They similarly acknowledged that they cannot change their neighbour (Participant A, 2019) and must find ways to suppress or contain Russian influence. Maintaining trust in the Estonian state, and by extension of that, Estonian digital solutions are seen as the most likely means to do so.

This research is unique in that it speaks to high-ranking digital professionals yet interacts with everyday life in Estonia. The interview participants are a link between the 'elite' and the 'everyday' in Estonia. Participants are largely aware of their privileged position but reference wider public opinion, their own mundane, or 'everyday' attitudes (which they frequently contrasted to their professional attitude to cyber security) as well as the thoughts of their personal friends and families. What glues them together is a shared belief in the Estonian state, as well as the belief that Russia represents a threat to the state via different digital means – notably disinformation, but also varying other digital approaches discussed in this chapter. One of the primary ways Russia is said to undermine its neighbours online is a combination of subterfuge and disinformation, via both diplomatic and non-diplomatic means (Manor, 2019). The goal of this, Manor identifies, is to undermine trust in institutions. Participants suggested that Estonia is more resilient than most to these attacks, thanks to the experiences of the Soviet and the immediate Post-Soviet era. This also reflects the observations of Lanozka (2019) who notes the Baltic states lived with such challenges previously, and digital means are simply an extension of that power and influence exerted via other means.

The paradox of e-Estonia is that it also makes Estonia uniquely vulnerable. This is evidenced by mixed attitudes to connected devices. This is informed by general anxiety and the recognised fragility of the Estonian state but also exacerbated by a negative perception of the Russian government and Russian foreign policy goals, as well as concerns with how secure digital devices and their supply chains sometimes are. It was also supplemented by some concern that a proliferation of connected devices and their intertwining with the e-state increases Estonia's vulnerability. As one participant remarked, if and when things stop working, everyone goes crazy (Participant J).

This chapter has also illustrated some of the insecurities that cyber security can generate, building on existing research exploring so-called ‘hybrid’ warfare (Mälksoo, 2018). Concerns relating to potential hybrid conflicts and ‘little green men’ (Participant N, 2018) seem to reference recent events in the wider Post-Soviet World, such as Georgia and particularly post-2014 Ukraine. Estonia has sought both closer political and cultural ties with Georgia and Ukraine in the aftermath of those conflicts (Makarychev & Yatsyk, 2016), and suggested that resilience can be built by learning the lessons of these conflicts. Research participants expressed both anxieties but also empathy with events in both of these Post-Soviet nations.

6.10 Conclusion

This chapter has sought to answer the question of whether cyber security concerns are changing wider geopolitical and security concerns, especially in relation to Russia. It has discussed how many of Estonia’s contemporary insecurities are shaped by Estonia’s past. It has also argued that issues of trust and along with Estonia’s Geopolitical relationships continue to shape the research participants’ relationship with cyber security and e-governance. e-Estonia is shaped by these geopolitics of the past and the present, and research participants were proud of its inbuilt security measures, which are a testament to Estonian ingenuity. e-Estonia is frequently used by participants, as well as governmental PR, as a barometer of progress compared when compared with the Soviet past. It is seen by research participants as a marker of Estonian civility and democracy cast against the backdrop of an increasingly autocratic Russian neighbour. For many in Estonia, the Soviet past remains traumatic and this is reflected in research participant’s everyday geopolitics as a source of geopolitical anxiety or fear (mirroring some of the everyday geopolitical fears identified by Pain & Smith [2008]). This chapter has highlighted that citizens’ trust has been formed through a complex mix of Post-Soviet era geopolitical identity politics and is continually evolving, reflecting contemporary relationships with Russia also. The Estonian state is trusted, in spite of the democratic preferences of participants, because it is perceived as an ‘Anti-Russia’. Nevertheless, the insecurities generated by the contemporary challenges relating to devices and disinformation remain serious challenges for the Estonian state and are deeply connected with the national relationship with Russia.

7. Estonia's Emerging e-Nordic Strategy: Opportunities

7.1 Introduction

Estonia has long been held as a leading example of e-governance, with over 95% of public services accessible online. This is enabled by the open source 'X-Road' platform, developed in Estonia in 2001. Existing research has commented on the successes and limitations of Estonia's e-governance. Yet Estonia's e-governance has arguably elevated the international standing of the nation which markets itself as e-Estonia. The X-Road supposedly provides the Estonian e-state with a transparent and accountable means of interaction between the citizen and the state and has many admirers.

This chapter explores e-Estonia as a form of Digital Diplomacy and discusses some new developments in Estonia's e-governance. This chapter seeks to answer the third research question: *How does Estonia use its status as a digital pioneer to extend its influence?* It explores how both Finland and Iceland have adopted the same platform and are formally collaborating with Estonia to develop international e-solutions for citizens and businesses. This chapter also examines the implications of integrated X-Road enabled e-governance across borders and poses the question of whether this approach represents an explicit foreign policy goal for Estonia, as a means to extend international influence.

"it's crucial for Estonia to extend its system beyond the country because we've invested so much into it"

(Research Participant A 01.02.2019)

This chapter represents an examination of contemporary Estonian e-governance as a foreign policy tool. Additionally, it explores some of the security implications of this approach, the wider utility of the e-Estonia model and heightened levels of digital cooperation in the e-Nordic region in the past few years. e-Nordic as a term, is derived from the words of Estonian President Kersti Kaljulaid:

"We need to have all the Nordic circle countries connected to a single digital identity or at least have the ability to recognise digitally our digital signatures. We will strive to cooperate in this sphere and we are developing from e-Estonia to e-Nordic"

(President.ee, 2019)

President Kaljulaid was speaking upon the event of Icelandic accession to the NIIS (The Institute of Nordic Interoperability Studies)²¹. This organisation began as a collaborative agreement between the Estonian and Finnish governments and is based in Tallinn. The focus of this institute is the development of X-road platform-based e-governance solutions across international borders. The goals of the organisation include increased cooperation in the realms of e-governance, e-service development, and cooperative security. Estonia and Finland are the founding members of the

²¹ Further information on the Nordic Institute of Interoperability Studies can be found on their website at: <https://www.niis.org/>

NIIS whilst Iceland and the Faroe Islands are expected to become full members shortly. Full membership is contingent upon the implementation of the X-Road platform, with a focus on developing interoperable, cross-border services. As President Kaljulaid does not explicitly name the countries of her e-Nordic vision, this chapter henceforth utilises the term to refer to the signatories of the NIIS, while reflecting on those who may be invited or interested in accession in the future.

The chapter provides an overview of utilising e-governance as a foreign policy tool, exploring what the e-Nordic brand of e-governance is, who is utilising it and why those nations have adopted this approach. It discusses cross-border e-governance as a soft power tool and explores the concept of soft power to understand Estonia's pursuit of this strategy. Additionally, the chapter includes reflection upon some of the human security aspects of e-governance as well as the utility of e-governance in working towards wider foreign policy goals, building upon existing research by Nyman-Metcalf & Repytskyi (2016) who explored Estonia's role in exporting e-governance to Ukraine and Moldova, noting Estonia seeks to be a 'role model' to others and an example of what can be achieved with a modest investment.

7.2 What is e-Nordic?

The vision of an e-Nordic region based upon a shared embrace of interoperable e-governance represents a growing reality between both Estonia and Finland. The addition of Iceland and the Faroe Islands as associate members (with a view to full membership for Iceland) is also a significant development. The chief goals of NIIS, and by consequence we might assume the driving idea behind creating an e-Nordic region include 'enabling secure connectivity, searches and data transfers' (NIIS, 2020). These are roughly reflective of the principles of 'confidentiality, integrity and availability' of data which is integral to most information security approaches. These principles, therefore, extend to good e-governance, as noted by Kerikmäe et al (2019).

The sovereignty of data has also come under increasing scrutiny. In particular, the importance of geographical locations for the storage and maintenance of data (for example, see Amoore, 2018). Just as good e-governance is roughly guided by the principles noted above, it is also subject to geographical and geopolitical forces. The idea of e-Nordic is thus driven by the principles of good security, good governance, and good practice. The e-Nordic idea of interoperable e-governance represents a tentative example of enhanced, interoperable cooperation in the field of e-governance but also closer economic and strategic ties within the region. While e-Nordic can be seen as simultaneously mindful of collective and human security concerns, it is impossible to ignore the geopolitical undertones – especially given how research has noted an increasingly assertive Russia in the cyber domain (Dahl & Järvenpää, 2013, Pigman, 2018, Kurowska, 2020). When this is combined with Estonia's outspoken stance on Baltic-Russian relations (Liik, 2020 & Trenin, 2020), and how Estonia has long hoped – in vain – for Finnish (and Swedish) accession to NATO (Coffey & Kochis, 2016) the e-Nordic vision might be understood as part of a wider, alternative strategy for Estonia to build closer security ties with its northern neighbours

The threat of Russia as a malicious cyber actor might also be noted to reflect Baltic fears of Russia in the sphere of conventional security (Liik, 2020 & Trenin, 2020). Ongoing events in Crimea and Eastern Ukraine have been perceived particularly within the Baltic States as an indication of a threatening Russia which is contemptuous of international security norms. Consequently, it is important to acknowledge the geographical and geopolitical environment that the e-Nordic idea is a product of. Namely, a tense geopolitical environment, defined by the competing national security goals of Baltic states and Russia, where the threat of 'hybrid' conflict looms large (for more discussion on the geopolitics and competing identities of the region see Aalto, 2013, Berg & Ehin, 2016). Famously, Estonia was the target of malicious cyber attacks in 2007 which were also supplemented by disorder on the streets (Hansen & Nissenbaum, 2009). The consequent fall-out of these 2007 attacks also served as inspiration for Estonia to initiate the data embassy initiative; a programme that situates critical data storage in a geopolitically friendly nation (Robinson & Martin, 2017).

Actions such as those of 2007 involving both cyber and 'real world' attacks have been argued to represent a form of 'hybrid' conflict, although not without some cynicism that arguably all conflict is 'hybrid' in the modern era (Mälksoo, 2018, Galeotti, 2016). Nevertheless, with the advent of 'hybrid' threats, it is crucial to recognise that citizens hold security concerns brought about by the increasing digitalisation of the state and that this increasingly impacts on everyday lives of citizens. Existing critical research is often scathing of a contemporary security environment that increasingly places the burden of security upon citizens (such as Vaughan Williams & Stevens, 2016), and the Estonian 'cyber war' of 2007 has been critiqued from a perspective of securitisation (Hansen & Nissenbaum, 2009). Yet, despite these concerns, as well as concerns regarding the potential elite-level of cyber security discourse as being inaccessible to average citizens (Cavelty, M.D. 2013), Estonia has continually embraced the deployment of digital technology in delivering public services. Indeed, some 99% of public services are available online (e-Estonia, 2019). Not only has the Estonian model been popular domestically (quantitative research has indicated a continual growth of online service usage, see Solvak et al, 2019) it has also been perceived as impressive enough by other states that they would like to replicate those services. It could be argued that this desire to replicate demonstrates Estonia's growing soft power in technology.

Recently there has been a growth in nations using technology to boost their soft power. As noted earlier in the thesis (see 2.8), soft power is a concept generally associated with Nye (1990) and sought to explain the non-military ways in which states can exercise power in the international system. This includes cultural and economic power, and how excellence in these areas can increase the international standing of states. Nye has expanded this research in recent years, developing the notion of 'cyber power' as a means for nations to expand their influence via digital means. This has further been adopted by Dunn-Cavelty (2018) who notes Europe's growing role as a regulatory cyber power. Additionally, Tsvetkova's (2020) research highlights how Russia increasingly utilises digital means to exert soft power over civilian populations, something which Pigman (2018) argues is a danger to international norms. Estonia does not seek to utilise cyber power by coercive means but instead seeks to expand its influence through expertise, innova-

tion, and collaboration. This chapter exclusively focuses on innovation in the development of cross-border, interoperable e-governance and analyses what is being adopted, where, and why.

7.3 What is the X-Road and How does it Work?

Estonia leads the world in e-governance, with over 99% of government services available online for Estonian citizens (e-Estonia: 2019). The Estonian government boasts that the only things you cannot do online are to get married, get divorced, or buy property. These restrictions are for legal reasons, to ensure no party is being coerced. Everything else, whether declaring taxes, renewing prescriptions, checking children's school grades, and much more, is all enabled by the e-government system. Every Estonian citizen has a citizen number, a secure digital identity, and (from age 16) has access to online government services. All services function via the population register which is connected to other systems and databases via the X-Road and allows for the exchange of up-to-date data. Thus, when a person applies for a study allowance or a social benefit, or files taxes all the relevant data is retrieved from the Population Register automatically. This means that there is no need to submit any documents or fill in forms etc. Each person can receive a service and access registries via the national portal www.eesti.ee with their eID or Mobile ID; citizens can also review and correct their data in the online Population Register (e-Estonia, 2019).

Critical studies have argued that in Estonia there was a lack of informed consent on the citizen's behalf regarding the initial implementation of identity cards and digital identities – and the wider e-Estonia ecosystem – which continues to develop apace to this day as additional digital services are added (Drechsler, 2018 & Bjorklund, 2016). Estonia's ID cards are not optional. They are automatically issued to citizens from age 15 and unique citizen numbers are also assigned at birth, and although their use is optional (it would be possible to simply discard a card or leave it in a dusty drawer), the above research has also noted that it is increasingly difficult to do so, as many public services are reliant on a digital identity, and in-person alternatives are increasingly rare (Drechsler, 2018 & Bjorklund, 2016). The state places a considerable emphasis on trust-building (mindful of human security concerns) when introducing e-services and has done so since the inception of e-Estonia. In other nations, this would be unthinkable. In the United Kingdom, for example, identity cards do not exist, and the public has generally strongly opposed their introduction, forcing the Blair and Brown Labour governments of the 00's to abandon plans for their introduction. In Germany, there is strong opposition to perceived governmental surveillance overreach, and the public is highly sceptical of perceived governmental interference in daily life, leading the German government to make the e-component of identity cards there optional. It has been noted that this limits the potential success of such cards, as both wide deployment and support are required to justify investment and the development of e-services (Poller et al, 2012). The reasoning behind this is chiefly concerning privacy concerns and accountability. Germany has both the technical expertise and the economic capability to introduce secure digital identities and the services these enable tomorrow if it was desired (Poller et al, 2012). The crucial difference is the differing human security environment in Germany, which, like the United Kingdom, has a sceptical attitude to perceived governmental overreach, and the feelings of insecurity this generates (Poller et al, 2012 & Kolsaker & Lee-Kelley, 2008). This was also highlighted by a participant who worked with German colleagues while pondering the replicability of the e-Estonia model elsewhere:

“The German one is slightly different. They certainly don't have the same e-government capacity. But again, they have a big resistance to this kind of thing. And I think that comes from the history as much as anything else from talking to German colleagues”

(Research Participant H, 03.04.2018)

The comments of the participant above illustrate the vital human security challenges faced by nations wishing to digitise services, and also illustrate the situated, and geographically varied nature of human cyber security, even in nominally similar countries on the same continent. Regarding the e-Nordic project, Finland has also adopted many of the e-services Estonia has already and has integrated these through the suomi.fi platform (which is based on X-Road technology). Now, through the X-road and in collaboration with the Nordic Institute of Interoperability Studies (NIIS), cross-border services are interoperable and accessible to citizens from both Estonia and Finland. Despite goals to target the wider Nordic sphere with this approach (President.ee: online), at the time of writing only Iceland and the Faroe Islands have signed association agreements. However, whilst X-Road based platform adaption is limited to Estonia, Finland, Iceland and the Faroe Islands, others have adapted the UXP platform. This is a privately developed and fully interoperable alternative to the X-Road (which is open source) and utilised by several including Greenland, Ukraine, and Azerbaijan (Hardy, 2020). This demonstrates some of the possibilities for Estonia to build soft power digitally.

The Estonian experience of comprehensive e-governance is one which must be understood within the specific social, cultural, and political environment in which it has thrived. The possibility of the replicability of Estonian e-governance beyond Estonia's borders has been subject to critique (see Chadwick 2003, for an earlier academic example, or Anthes, 2015 for a more contemporary take), and this has also recently spilled into popular media outlets including *Wired*, *The New Yorker* and the BBC (see Hufkin, 2017, Heller 2017, Sterling, 2017). These outlets have highlighted the efficiency and the economics of the Estonian model, and how it might represent the future of governance beyond Estonia's borders. This has been driven by the many high-profile campaigns driven by the Estonian government, such as e-residency, which has branded the nation to outsiders as cutting edge (Mäe, 2017, Kattel & Margel, 2019, & Kerikmäe et al, 2019).

The X-road is an integrated information system that enables the accountability of data for e-governance users, thus providing trackability, ownership of data, and accountability of government officials who access or potentially misuse personal data. The X-road is a centrally managed ledger, which tracks data, notifying users when their data has been viewed by public officials, and why. It operates via the secure digital identities of citizens, which are authenticated by the user, through their devices and identity cards. Estonia's ubiquitous digital governance systems are occasionally (mistakenly) labelled as 'blockchain' (such as Khan & Shahab, 2020) However, this is equivocally not the case, as highlighted both by (e-Estonia, 2018) and Research Participant U (14.12.2018). Nevertheless, while not

‘blockchain’ the X-Road has similarities, including distributed ledgers. It also utilises digital signatures and leaves a paper trail, providing accountability and minimising abuse (Goede, 2019).

It is this principle of accountability which has so enthused exponents of e-Estonia. However, at the core of the very principle of the X-road, is the issue of who manages the central database. Trust in public institutions in Estonia has been reasonably easy to come by for the Post-Soviet Estonian governments, who built upon a wave of patriotism in the aftermath of re-independence to make sweeping digitalisation core to their modernisation of the nation, which lacked much critical infrastructure, and what it did inherit from the Soviet Union was considered outdated and in need of urgent modernisation (Kattel & Mergel, 2019 & Wrangé & Bengtsson, 2019) . The legacy of Soviet occupation marred Estonia’s post-1918 nationhood, where sovereignty was interrupted by both the Soviet Union and Nazi Germany. A consequence of the traumas of this occupation has been the increased levels of trust in public institutions within the country (Priisalu & Ottis, 2017). This high level of trust in Estonian governmental institutions has allowed the introduction of wide-ranging digitalisation with little public opposition in the immediate Post-Soviet era, although maintaining this trust is recognised as a challenge going forward (Kattel & Mergel, 2019 & Research Participant N, 26.02.2019).

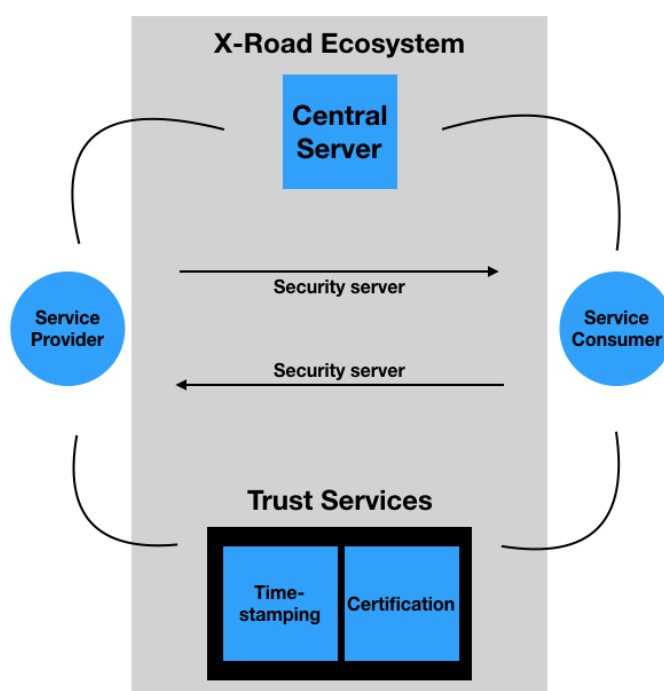


Figure 5: An overview of the X-Road Ecosystem. Author’s own image. Citizens trust

As illustrated in Figure 5, an X-Road instance consists of the basic components illustrated within the large, central square²². Those components include the central authority that maintains the central server, as well as associated trust services (including time stamping and certification services) and the security servers which permit communication

²² For a highly detailed breakdown of the individual aspects of the Estonian X-Road Ecosystem including individual public and private service providers, see Vassil (2015)

between service providers and service consumers²³. In the case of e-governance, the service consumer is most often the citizen. Service providers can be both public and private institutions. Communication through the X-Road is signed digitally to ensure data integrity. This is achieved through trust services, which provide certification and time-stamping as part of the public key infrastructure (PKI). A combination of procedures, software, and hardware alike combine to implement securely encrypted digital transactions. These authorities all require the approval of the Governing Authority. The X-Road itself is open source, however, nations or organisations wishing to use it must set up and maintain these authorities. This requires trust in public institutions to operate services, to regulate users, and not abuse their authority.

The process of X-road enabled authentication through a centrally managed ledger is crucial to the accountability and trust-building aspect of e-Estonia. It could be argued that this simultaneously gives the user ownership of their security, yet also places an additional security burden upon the individual. It both provides a degree of human security, whilst simultaneously further securitises seemingly mundane processes by making the individual responsible for a process of authentication and a significant part of the overall security process in order for the transaction to be secure. As further, seemingly everyday interactions are shifted online, those interactions become subject to cyber security concerns. Furthermore, engagement with e-Estonia requires a base level of knowledge to use this technology. The Estonian state sought to counter any skill deficit during Project Tiigrihüpe (Tiger Leap) in the 1990s, which featured a comprehensive technical education outreach, to give Estonians technical skills for the future. Similarly, in present-day Estonia, tech skills including basic coding are taught from an early age in schools, moulding citizen-subjects through formal education. Whilst both of these approaches are laudable, it is worth also considering there is still a minority of the population left behind. Increased digitisation generally leads to the running down of physical, in-person services, particularly in non-metropolitan areas (Aradau, 2010). This was noted by participant S:

“I think the way it will work here is that it would be a natural replacement. So the old people will die and we already have the skills. So just have to wait 20 years... it sounds cut throat, but it's how it is...that's kind of how it is at the moment. There's and what's happened with the Services thing is the digital there is a face-to-face Services have been scaled back. The amount of post offices we now have is I think Tallinn has three Tartu has one or two. And the customs office here and I've been to the customs office because I do have some I couldn't sort my paperwork out online and the queues are massive and they're mostly older people because they don't know how to use any of these services that they should be able to, but if you speak to people from the e-governance department. Oh, yeah, they think everything's hunky-dory.”

(Research Participant S, 01.03.2018)

Participant S also reasoned that the Estonian state had essentially accepted that some people would suffer from the digitalisation of the state and was reasonably comfortable with treating those people as collateral damage in the pur-

²³ The diagram represents a simplistic overview of the X-Road. For further information on X-Road Architecture, see the NIIS (2020: online) available at: <https://x-road.global/architecture>

suit of modernising Estonia. This also somewhat mirrors the findings of Björklund (2016) who suggests that there is a willingness to overlook the occasional failings of e-Estonia due to the economic positives it has provided and more so because it has become so intrinsically part of what it means to be Estonian.

Moreover, as noted by a research participant, the movement of nearly all services online creates a national reliance on the availability of online services:

*“The unique thing is that first, we do *everything* online.... as I’m sure you noticed from spending so much time here... Estonians are really closed people.... so whenever you can avoid talking to other people, you just find the alternative... and we go crazy if, for whatever reason, things stop working”*

(Research Participant J, 29.02.2019)

Indeed, as other participants mused, the X-Road enabled digital state is now integrally part of the nation, and being without it would be quite unthinkable:

“it’s totally changed life now, and people have a much easier life now... I don’t know how people would cope without it... you would have to... go to places!”

(Research Participant E, 06.04.2018)

These remarks also speak to some of the cultural traits of a nation that prides itself both on its technological capabilities as well as cultural introversion (a trait often noted in even online literature promoting Estonia - for example, Work in Estonia, 2020). What becomes increasingly clear is that technological capability is not the only consideration and that social and cultural matters are also relevant factors to the introduction and success of ubiquitous e-governance.

7.4 Who is Adopting X-Road and How the e-Nordic Vision Might Work

“It’s so important we have this ecosystem, we have the x-road, we have the secure identities, based on census information... so people trust it. Other places, like India, are starting to try and replicate this, but with some difficulty”

(Research Participant G, 09.04.2018)

The Estonian digital ecosystem (i.e. the sociotechnical assemblage of devices, systems, and users) outlined above by Research Participant G has not been an overnight success, but rather a gradual and quite deliberate policy success by the Estonian government (Kattel & Mergel, 2019). As the participant notes in line with Kattel & Mergel’s (2019) observations, the Estonian approach to digitalisation has been popular domestically and as this chapter highlights, there is a growing clamour to replicate this approach (in some part due to a considerable PR campaign on behalf of the Estonian state [Dreschler, 2018]). Statistically, the success of e-Estonia has been measured within existing quantita-

tive research illustrating a growing trend of service uptake among the population (see Solvak et al, 2019). As previously mentioned in the introduction of this chapter, this has generated considerable interest overseas for X-Road enabled governance. The most notable development is the move to integrate platforms between like-minded countries, spearheaded by Estonia in the NIIS. The NIIS, summarised, is focused on the enhancement of interoperability in the field of e-governance between signatories. Current full membership to the agreement is limited to Estonia and Finland, the Faroe Islands are an associate member, and Iceland is an associate and set to become a full member shortly. The institute has even bigger goals, however, with the potential to expand to the wider Nordic region a strategic goal (Participant U, 14.12.2018).

The additional goals of the institute are displayed on the organisations website:

"the aim of the association is to ensure the quality, sustainability, cross-border capability of core e-government infrastructure components; to save resources upon the development of digital society and cross-border cooperation"

(Memorandum of association of MTÜ Nordic Institute of Interoperability Studies, 2017)

Estonia has a long-running association with excellence in e-governance, and has been utilising the X-road for purpose of modernising online governance since 2001. The benefits for Estonia were driven, at the time, by larger economic factors, helping to streamline public service costs, which could then be invested in other areas such as infrastructure and defence (Kalja, 2002). Whether such comprehensive services were envisioned in 2001 is unclear and the Estonian development of services has often been carried out on an ad-hoc basis, thanks to both the unique freedoms bestowed by the Post-Soviet context, which effectively meant Estonia could build a new government from scratch (Solvak et al, 2018). More than this, the growth of e-Estonia has served a dual purpose of giving Estonia a unique, soft power tool that marked the nation as different from its Baltic neighbours, more outward-looking and progressive. Such an interpretation might be drawn from Nye's work on soft power, which he emphasises as being drawn from culture, values, and sometimes, measured against also what a people or nation is not (for more discussion on this, see Nye, 2008 on public diplomacy and soft power). Consequently, it is often a source of pride for many Estonians to identify themselves as Nordic rather than Baltic. It is also a way of emphasising their Finno-Ugric cultural connection to Finland and the Nordic sphere. The development and smooth branding of the e-state is a continuation of this public diplomacy and furthers this perception to outsiders. Conversely, the Soviet is used as a marker of incompetence or backwardness, as well as a cultural marker:

"I think being Digital means not being Soviet somehow... A lot of Estonians like to identify as Nordic now..."

(Research Participant L, 31.10.2017)

“I think this is part of the Estonian identity these days... it’s very much that they want to show themselves as being Nordic... for the other Nordic countries, it’s very much about the information system architecture... for Estonia it’s a key part of their foreign and security policy also have close links with these countries... for the others, yes its beneficial for everyone to cooperate too”

(Research Participant U, 14.12.2018)

The above quotes again support the wider assertion that Estonia desires to be recognised as Nordic, and utilises the digital sphere to further its public diplomacy goals. e-Estonia thus becomes a means to demonstrate the civility of contemporary Estonia, as opposed to the supposed backwardness of Post-Soviet space.

The functionality of e-Estonia is predominantly dependent upon X-Road technology which the system requires to securely identify users and grant them secure access to services. The X-Road functions from a centralised database; a secure portal accessible only when users authenticate themselves utilising a citizen’s ID card (which contains a chip, and citizens are provided with authentication keys to securely access services) as well as secure mobile identities, based on banking technology. Users must authenticate themselves, in doing so creating a trail so that if data were to be misused, it can be traced to the source. This grants a platform that citizens can trust to be secure, albeit with one extremely vital caveat – that the users trust the central database and those who maintain it, as well as trust the technology itself. In this respect, the X-Road (and other X-Road instances such as the domestic X-Tee and Finland’s Suomi.fi) are fundamentally different from conventional Blockchain technology (e-Estonia, 2018). The relationship between Estonia’s X-Tee and Finland’s Suomi.Fi is further illustrated in Figure 6 below.

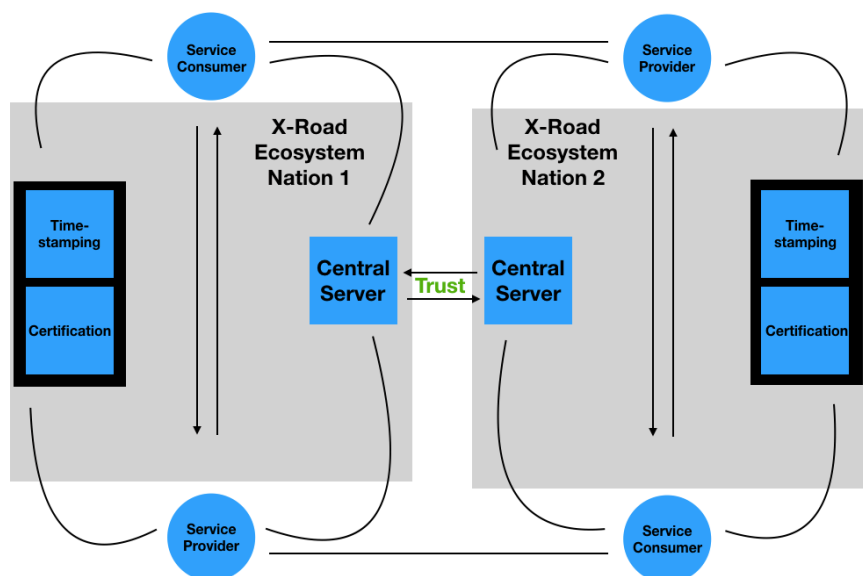


Figure 6: Integrated X-Road instance: Author’s own image. Service providers and consumers can interact across X-Road instances, allowing cross-border service provision.

Whilst we have already examined this functionality above, it is worth considering how this trust affects the potential integration of X-Road platforms internationally. One of the primary reasons to federate X-Road instances is to facilitate cross-border interactions between service consumers and service providers. While the X-Road instances are parallel to each other, the federation allows governing authorities to agree on cross-border access. However, it is important to note once again, the trust aspect which is central to such agreements. For cross-border functionality, there must be a trusting relationship between governing authorities in both nations, as access to services is based on trusting the security protocols of the parallel X-Road instance. In this example, the Estonians must trust the Finns, Icelanders and Faroese to maintain similar digital security standards and vice versa. Crucial to the mutual trust relationship is shared trust in the authentication process and secure digital identities:

“connecting systems is probably the hardest part. We have that now between Estonia and Finland. The rest, who knows. But security for the cards is so important, to keep trust.”

(Research Participant N, 26.02.2019)

One of the challenges in rolling out a similar product beyond Estonia is replicating that level of public trust in the would-be e-Nordic nations. In this regard, Estonia’s soft power is crucial as it builds confidence in Estonian technological capability. The trust placed within the Estonian government by the Estonian public at the time e-governance was rolled out was in an age of new-found self-governance and Post-Soviet optimism in the early 1990s. This led one research participant to note:

“Estonia as a young country... it had this trust credit... we didn't have the political legacy of creating distrust... we also didn't have the same technical legacy as other countries... if you have old systems it's much harder to change things... you can build something from zero that works...”

(Research Participant P, 11.04.2018)

So, for all of the technical assurances available, rolling out comprehensive e-services requires a buy-in of trust from citizens beyond the tech community. After all, this expansion of X-Road instances theoretically opens up potential attack vectors and more risks. However, this risk is also counter-balanced against the opportunity for Estonia to spread its expertise and influence in e-governance internationally, which is seen as a great source of prestige for a small nation (Kerikmäe et al, 2019 & Tammpuu & Masso, 2018). Getting non-Estonians to buy into the project is, however, less simple, and relies on some of the soft power and nation branding evidenced by Mäe (2017 & Papp-Váry, 2018) as well as trust-building.

This, as noted by the research participant above, can be shaped by the political landscape as well as existing e-governance services or general governmental norms and procedures. It can also be limited by demographics, the availability

of skilled workers, and economic restrictions. As a general assumption, it seems relatively safe to assert that most citizens, unless they are directly involved in the tech industry, or pursue technical expertise independently, do not understand encryption, the X-Road, PKI, or many other technicalities involved in developing secure digital services. Nevertheless, it falls upon the authorities to sell these digital solutions to the community; an approach that Estonia has wholeheartedly pursued. Harsher critics have suggested that Estonia sells a ‘fairy tale’ which is a ‘façade’ of good governance (Drechsler, 2018: 4) and that this creates in effect two tiers of citizens in Estonia: those who are good ‘e-citizens’ (who securely consume the wealth of digital services available to them) and bad ‘e-citizens’ who do not (Björklund, 2016). Others have suggested Estonia’s popularly promoted e-residency is a rather shallow form of nation branding, yet the vision of e-Estonia has undoubtedly been effective, winning admirers beyond Estonia (Mäe, 2017 & Tammpuu & Masso, 2018).

7.5 e-Estonia Beyond Estonian Borders

Whilst Estonia extols the benefits of its e-governance model (such as improved access to services, anonymity and economic opportunities) it seems pertinent to address why Estonia feels the need to spread its model beyond its domestic borders. Whilst the prior section highlights some of the processes and structures involved in making inter-operable e-governance function, we should also address which aspects of that e-governance are being utilised by foreign governments. Perhaps the most notable adopters of X-Road enabled governance have been Estonia’s northern neighbour Finland.

In the Finnish context, the X-road data exchange layer was introduced in November 2015, following a decision made in September 2013 to work in collaboration with Estonia. This followed an earlier announcement that year that Denmark, Finland, Norway, and Sweden would share their Open Government Partnership work and together promote open data (European Commission, 2016: 8). Finland’s collaboration with the Estonian government is broader in the sense that it involves an integration of the data exchange layer, meaning that Finnish and Estonian citizens can mutually access digital services in either nation (This can be seen in Fig 5, where service consumers and service providers can communicate with each other across borders). This allows for the development of cross-border services. Given that many Estonians live and work in Finland, and an albeit smaller number of Finns live and study in Estonia. e-Nordic would arguably provide a tangible human security benefit²⁴.

“The goal is not necessarily to replicate e-Estonia, but we are capable of achieving their level of digital services, and want to work collaboratively with them”

(Research Participant V, 17.12.2018)

²⁴ The lack of tangible benefits for citizens has been a common concern for critical researchers concerned with the increasing digitalisation of public services. For example, see Coles Kemp, Ashenden & O’Hara (2018)

The promotion of such citizen-oriented benefits has led enthusiastic foreign media outlets to encourage their nations to adopt this platform (see Thomson, 2019's argument that Scotland should adopt the X Road for such reasons). Indeed, as research participants also noted, in Estonia, Citizens benefiting from e-governance is crucial to the ongoing success of the project, while they are often less concerned by the security (or potential lack of) within that service.

"it is the services people care about. The state has provided a service which is secure, but security is not citizen's primary concern. If you talk to most people... the average person on the street... they perhaps don't think about the security so much"

(Research Participant B, 08.03.2018)

Undoubtedly, this is representative of the Estonian experience of e-governance, which is notable for its relative lack of controversies and resistance to its implementation, leading Kattel & Margel (2019) to label it a policy success. Yet it does not account for the necessity of gradual introduction, familiarisation, and trust-building for citizens to engage with e-services. Indeed this might explain the Finnish resistance to e-voting as a step too far, despite possessing all of the technological capacity to implement it. (Yle, 2017). Those who extol the X-road of course highlight this as an advantage, in that states can cater their approach to local concerns (Research Participant U, 14.12.2018).

As of yet, both Iceland and the Faroe Islands have yet to link their instances of the X-Road to Estonia and Finland, yet have committed to do so in the future (their associate membership with NIS is based upon progressing towards full interoperability in the future). Significant drivers for increased digitisation of governance and public services in such small states might be said to include demographics, mobility, economics, and efficiency. Such factors are identified by McBride (2019) in the Faroe Islands, as well as some unique factors pertaining to Faroese independence from Denmark that has informed e-service adaption rates and the popularity of e-governance there. Existing research focusing exclusively on Icelandic e-governance right now does not exist, although Saputro et al (2020) discuss the prerequisite conditions for X-Road adoption, which include (but are not limited to) appropriate legal frameworks, political leadership, technological expertise, adequate funds, and the principal of a secure digital identity. Iceland would comfortably meet such criteria, with its high GDP, as well as high levels of political and digital freedom. Furthermore, Iceland fits with the other culturally Nordic nations with whom Estonia perceives itself as associated with (see Thorhallsson, 2018a for discussion of Iceland's embrace of its 'Nordicness' as shelter).

It is important to note, however, that despite public aspirations of building e-Nordic, Estonia is not only providing e-government expertise in this area of the world. Indeed, several nations in both the Post-Soviet world and Africa have adopted either the X-Road itself or UXP (a similar platform based on X-road technology, which is inter-operable with X-Road instances, provided by privately-owned Estonian company Cybernetica, who have close links with the Estonian state). This international adoption of similar models of e-governance has been enabled either through private enterprise, public diplomacy, and the Estonian think-tank and consultancy 'e-governance Academy' (for more, see

Hardy, 2020, which argues this forms a considered strategy of Estonian soft power). It is somewhat notable that the Post-Soviet and African nations are excluded from much public discourse about future, close collaboration. Perhaps the most controversial user of the X-Road might be Azerbaijan. Described by Freedom House (2020: online) as ‘not free’ with ‘rampant corruption’ and ‘little freedom of expression’ for citizens, Azerbaijan is more comparable with some of the least free Post-Soviet states (Turkmenistan is officially ranked as the worst, and ‘less free’ than North Korea) than Estonia and the Nordic neighbours it publicly courts, raising some significant moral questions. The Estonian government ‘assisted in the development of an information system similar to the X-Road in Azerbaijan’ (EGA, 2014) and Cybernetica assisted with the development of Mobile ID services (Cybernetica, 2014). This is nowhere near as widely referenced as e-Nordic for good reason. Building close ties with some of the more oppressive Post-Soviet nations does not closely align with the public image of e-Estonia as progressive and western (which the Estonian government prefers to promote).

There is little discussion of similar goals of platform integration, for example, with Ukraine. This is despite Ukrainians being Estonia’s second most numerous migrant group who comprise around 1.7% of Estonia’s total resident population. There has also been increased mobility between the two nations in recent years as many Ukrainians have sought employment in Estonia (Work in Estonia, 2021). It might consequently be argued that the goals of interoperable e-governance are highly selective. Finland, as well as Iceland and the Faroe Islands, are affluent and Nordic, and closely fit with e-Estonia’s chosen public image. This cooperation is not purely platform-based but also involves the sharing of experience and good practice, which can also hold security benefits further explored below.

7.6 Why Develop Integrated, Cross-border e-Governance?

This section analyses some of the reasons *why* Estonia is determined to develop and expand cross-border e-governance. This section argues that these include: *Security; Mobility and citizen-centric services; Money-saving and economics; and Politics and Foreign Policy*. These aspects are all explored individually below. The following analysis was drawn from participants who were asked ‘Is there something unique to Estonia or Estonian mindsets that makes technological innovation possible?’ and ‘What is the future for e-Estonia? Is it [The Estonian Model of e-governance] likely to spread across the Nordic region? Participants responded with musings ranging on security, economics, and foreign policy, discussing why it is vital e-Estonia spreads beyond Estonian borders.

Security

One of the potential benefits of cross-border, inter-operable e-governance is the possibility of enhanced cyber security cooperation and the establishment of shared norms and procedures. Norm and subsequent international law building have been identified as a means to improve security online (see Mačák, 2017). Of course, one of the contradictions of e-governance is that, for all the security which can be built into the process, it creates vulnerabilities which could be exploited by malicious state or non-state actors. It simultaneously secures data (for example, digital data stored properly on a distributed ledger is far more secure than paper documents which could be accidentally de-

stroyed or misplaced through human error) but also creates additional attack vectors for would-be cyber attackers and criminals to access that data (Yang et al, 2019). Ubiquitous connectivity and ubiquitous e-governance pose significant security challenges, which involve a complex series of assembled relationships between public and private sector actors (see Collier, 2018 for more on such challenges).

The advantages of centralised security and e-governance, which the X-Road enables, include a uniform and consistent way to manage risk, the ability to adopt a common security policy, the ability to securely encrypt access to services where necessary, and the ability to maintain and update the system in an ongoing, and streamlined manner (for discussion on the benefits of secure e-governance and e-voting, see Zissis & Lekas, 2011; Pappel et al, 2013; Solvak et al, 2018).

A recurring pattern among the research participants was an emphasis on the ‘smallness’ of Estonia, and the unique vulnerabilities faced by small countries. As such, many research participants emphasised the need for increased collaboration and regulation on an international level, and for other nations to adopt collective stances on security challenges. For many participants, Russia represented a security threat to the development of e-Estonia and any potential e-Nordic collaboration. It was stressed that Estonia and other countries should adopt collective stances and policies against private companies, and even individuals, which they felt posed a security risk to the collective security of Estonia and their neighbours and allies:

“It takes guts and its political wisdom and courage to spell out that it’s the policy in Estonia that government officials shouldn’t use Yandex taxis, for example, or we take a position about Huawei productions, or we take a position that we should not use Kaspersky Anti-Virus tools... so it seems maybe common sense you shouldn’t use those if you consider Russia your primary security threat... but it’s not down in the paper anywhere. So the security supply line, it’s a question of strategic investments, but cyber security companies... private sectors.... what restrictions do you make in terms of accepting investment from outside. So... Estonia is a small place you know... Guardtime, Cybernetica, Cybexer... we have a few main companies... but what are the measures for these companies, other than say common sense, for them to not accept Deripaska Russian investments? Or not to hire Deripaska as a member of their board?²⁵... no Estonian company that wants to be taken seriously would ever do it,”

(Research Participant A, 01.02.2019)

Such comments highlight an association of ubiquitous e-governance with matters of cyber security and the wider security and geopolitical concerns that Estonia and its neighbour’s face. The more popular geopolitics of those relations cast Russia as a menacing and malicious adversary. This chimes with other existing research which has noted

²⁵ Oleg Deripaska is a noted Russian oligarch with links to the Kremlin, who is subject to US sanctions as of 2018, along with a number of other Russian oligarchs

non-conventional soft security threats as a growing security concern, particularly for small nations (see Grigas, 2012 for more, or Galeotti, 2016 & Mälksoo, 2018 for discussion of supposed ‘hybrid’ security challenges).

Mobility and citizen-centric services

Another benefit of the development of cross-border interoperable e-governance is the mobility aspect for citizens. As noted earlier, there is significant, cross-border movement between Estonian and Finnish citizens. The motivations for the development of cross-border services are said to include the ease of access to services and amenities across borders. As illustrated earlier in figure 6, the cross-border federation of X-Road between Finland and Estonia now allows for service consumers in each nation to access service providers in the other (for further details on the functionality and challenges of this federation, see Freudenthal & Willensen, 2017).

Through cross-border X-Road federation, the e-Nordic vision of the NIIS has a unique opportunity to demonstrate value to citizens through the provision of people-focused services. Research participants were eager to emphasise that the integrated system, should provide a common approach whilst also catering to localised concerns, rather than being a copied and pasted version of e-Estonia:

“The X-Road provides a data exchange layer which enables exchange between the two countries... this can be the same, but then the way it is presented to the user can be sensitive to local concerns... the x-road itself is just the layer connecting the databases... they can then use the solutions locally that they want”

(Research Participant U, 14.12.2018)

“It’s about mentality and trust... I think it’s crucial for Estonia to extend its system beyond the country because we have invested so much in it... we are conscious of what is happening at an EU level, with the development of services... we don’t want a situation where our model becomes obsolete, so it’s crucial for us to develop a critical mass... so it’s demonstrable to Brussels, if it comes to a European level, that ours can work across borders”

(Research Participant A, 01.02.2019)

A key challenge to rolling out the system across the wider region in the pursuit of e-Nordic lies in the geographical variability of security concerns. The shared values of these countries, as well as their close socio-cultural ties, make this easier, but not without sensitivities. As the system grows, undoubtedly there will be concerns as to who controls and maintains the X-Road exchange layer. However, the project hopes to offset concerns with citizen-centric benefits of interoperability. Furthermore, as NIIS (who are charged with the responsibility of implementing interoperability) is an international NGO, this supplements trust. Many participants also highlighted how providing tangible results was crucial to trust-building. By making services easily accessible (and removing bureaucracy, which nearly all citizens dislike) citizens quickly adjust to new norms:

“People don’t want to go back to the old way of doing it.”

(Research Participant N, 23.03.2019)

However, as the same participant consequently noted later in their interview, this trust and security relationship may diverge when other states become involved in the process. Thus, whilst trust in Estonia is high, this dynamic can alter when it involves trusting other states to uphold the same practices and procedures, and also that inter-connectivity may change the trust dynamic of citizens, who may implicitly trust their government, but perhaps not others utilising the same platform:

“Yeah, so apparently that’s been an issue because the systems for these things are different a lot over Europe, so if other countries do their own e-citizenship systems, it’s probably not so easy to make them work together, so connecting systems is probably the hardest part. We have that now between Estonia and Finland. The rest, who knows.”

(Research Participant N, 23.03.2019)

Fundamentally, issues of trust and security are vital in the potential implementation of cross-border, citizen-centric e-governance initiatives. Finally, regarding the human-centricity of e-governance, it was not universally accepted that Estonia was the best in this regard, with a Finnish participant noting:

“Finland just scored the first place in human centricity in e-services, so in some areas we are already forerunner and not so much in position where we need to replicate e-governance models. However, we of course do regularly benchmarking and cooperation to learn from the best practices where applicable, as was the case with X-Road concept a few years back.”

(Research Participant V, 10.12.2018)

So whilst Estonia vocally takes the lead and has been essential to establishing X-Road as a platform for e-governance, the way that services are presented and made accessible to users still varies locally (and indeed be improved upon). Finally, it seems crucial to note the 2019 movement of national business registers and tax boards in Estonia and Finland towards cooperation that would allow the agencies to exchange data more accurately and efficiently (NIIS, 2019). Whilst the ease of paying taxes is one of the promoted benefits of e-Estonia, there are also financial benefits to both governments in terms of tracking taxes to counter potential cross-border tax avoidance.

Money-saving and economics

Aside from the ability to easily track cross-border taxes, one of the central arguments for ubiquitous e-governance on a domestic level is the money-saving aspect. e-Estonia (2020) estimates that Estonia saves roughly 2 percent of the national GDP from its use of digital signatures alone. They further estimate that voting online costs 1/20th of the cost as opposed to voting in person, based on the cost of vote counting, vote processing, and voter identification (based on

the study of Krimmer et al, 2018). For smaller nations such as Estonia and Iceland, the opportunity to make such savings is significant, as both operate with limited budgets due to their size. However, critics have noted that some savings are exaggerated by the Estonian authorities and that costs have simply been redistributed elsewhere. Drechsler (2018) notes that there are significant costs to digitisation, which absorb some of the savings made by the shrinking paper-based bureaucracy. This is further illustrated by McBride (2019) whose analysis of the Faroe Islands e-governance strategy suggested that digitisation would not generate significant economic benefits (although the Faroe Islands is significantly smaller than the other nations involved in the NIIS). However, there was hope that digitisation could support the diversification of the economy. Estonia, Finland, and Iceland all have established tech sectors, which is also conducive to having a skilled population prepared to engage with e-government and the further development of potential cross-border services.

Foreign Policy

Estonian Foreign Policy might be characterised by both enthusiastic NATO membership, support for EU institutions as well as more informal, personal ties to the Nordic sphere. Since the restoration of independence, Estonia has continually emphasised its ties to the West and the North. A heightened sense of identity has played a significant role in shaping Estonian Foreign Policy (see Berg & Ehin, 2016). It seems quite logical to suggest that this cross-border e-governance policy is further reflective and a continuation of that Foreign Policy, given whom the vision includes, and whom it does not (as noted in 7.2). It also further cements Estonia as being a unique ‘e-Nation’. As Research Participant D notes “You don’t find any other country that has it like that”.

There is limited existing evidence that small nations have successfully inflated their influence and international standing through specialised expertise in digital technology (whilst small state literature specifically addressing such questions is limited, Burton, 2013 argues for New Zealand as a successful example of this). Nevertheless, specialisation in interoperable e-governance may be a desirable foreign policy goal for Estonia and also for the small nations of the wider Nordic region. While the data embassy (Robinson & Martin, 2017 & Kimmo et al, 2018) and e-Residency schemes (Tanel & Särav, 2015) have received attention for their role in enhancing Estonian international prestige as well as ensuring ‘digital continuity’ of the state, the most promising cross-border development for Estonian foreign policy may well be cross-border e-governance services and X-Road platform integration.

7.7 Challenges

A consistent theme identified by research participants was the idea that the Estonian brand of e-governance fundamentally requires trust to function, grow, and be attractive to private developers. Functional security collaboration also requires trust. Domestically, in the case of e-Estonia, that trust is a collaborative social contract formed between the government and the populace over a significant amount of time. The government, in the Estonian case, has sought to keep its end of the bargain through the development of citizen-centric services. Most research participants hailed the Estonian government’s role in building trust and were pleased by the functionality and accessibility of services, the security of e-Estonia in general, and optimistic that this approach could work beyond Estonian borders.

“I think that the interconnectivity and the services that are shared by different countries... that’s what we will see in the future... But I will say this, that I think the electronic ID and all of these measures... they were the influencers, or the basis to use the electronic environment, so cyber security measures actually made it possible to use a networked environment. So now we are seeing what different governments, what different businesses together can create... I don’t know where it’s going! But the possibilities are limitless. But, they are limited by general culture in different countries, how much they want to cooperate with others etc etc... But the possibility is there... we’re probably going to see all sorts of innovations.”

(Research Participant I, 23.09.2018)

Given the Estonian experience and the input of research participants, it seems reasonable to conclude that the general culture of countries is vital for collaborative e-governance. The X-road, and wider e-Nordic interoperability goals represent a strategic, foreign policy objective for Estonia. Furthermore, in political terms, this enhanced collaboration fits with the wider foreign policy goals typical of smaller states, which often seek closer ties with other small or larger states due to their vulnerability within the international system (Thorhallsson, 2012 & Bailes et al, 2016). From a security perspective, this chapter also highlights that whilst there are benefits to close collaboration and ubiquitous e-governance, there is paradoxically an increased risk through the creation of additional potential attack vectors.

7.8 Conclusion

This chapter has sought to address how Estonia uses its status as a digital power to extend its influence. As this chapter has illustrated, this is undertaken in a number of ways including public diplomacy (which references the human-centric benefits of cross-border e-governance), financial incentives, and extending Estonia’s reputation of expertise in digital matters. The financial case for building Finnish and Estonian cross-border services is relatively clear cut in terms of financial incentives. The financial case is less clear in the case of Iceland and the Faroe Islands. As of yet, whilst both now operate their own X-road instances, these remain unconnected to Estonia and Finland. It seems reasonable to conclude that these instances serve as a form of public diplomacy and reputation enhancement more than for financial gain. This chapter has also illuminated how Estonia’s cross-border governance works and identified the key actors involved in its development. Future research could perhaps explore this international collaboration as it develops further. This also applies to the development of future cross-border use cases between Estonia and Finland, as additional services develop over time.

8. Conclusion

8.1 Introduction

This thesis has investigated the challenges, insecurities, and opportunities of e-Estonia. Framed through three research questions, and supported by around 25 hours worth of extensive interviews and immeasurable ethnographic observation based on two years living in Estonia, the thesis can draw a number of conclusions, as this chapter illustrates. e-Estonia is the culmination of over 30 years of digitalisation efforts by the Estonian government. It is well-established and generally respected domestically. Nevertheless, this thesis has highlighted some of the major challenges and insecurities that e-Estonia faces. However, conversely, the ubiquity, popularity, and growing reputation of e-Estonia presents a unique opportunity for Estonia to expand its influence and secure its longevity through technical expertise sharing, concerted diplomatic attempts to build cross-border interoperability, and encouraging others to adopt the e-Estonia model. This is limited right now, and there are a number of security concerns that future expansion ought to be mindful of. Similarly, this research has sought to highlight the mundane security threats that litter everyday life and interactions with e-Estonia. It has also highlighted that while digital professionals hold privileged positions in Estonian society, they also face everyday challenges and are mindful of the experiences of ordinary, non-technically minded citizens when undertaking their work. This chapter further expands upon this in more detail, outlining the unique contributions this thesis offers. It reflects upon findings of cyber insecurities in the everyday, the challenges of ubiquitous connectivity and trust, and the opportunities of cross-border e-governance. Finally, the chapter reflects critically upon the methodologies employed within the thesis and identifies areas for future research.

8.2 Unique Contributions & Developments from Existing Research

This thesis has argued that Estonia is a digital pioneer, but also a unique Post-Soviet anomaly created by highly specific local conditions after the break up of the Soviet Union. Estonia has pursued rapid digitalisation and nurtured and developed its e-governance and cyber security institutions, and infrastructure over time. In 2018, e-Estonia celebrated being top of the national cyber security index (NCSI) (*e-Estonia, 2018a*). It is important to note, however, that the NCSI is funded by the Estonian government through the e-governance academy and is based in Tallinn. This thesis has argued that while e-Estonia is strongly linked to the modern Estonian identity, that bond is not inseparable, nor universal. Despite the promotion of e-Estonia (something also discussed critically by Drechsler, 2018 & Kerikmäe et al, 2017), the reality is somewhat less clear. Rather than being a unanimous benefit to all, there are considerable grey areas relating to citizens' everyday anxieties. There are also doubts over how a proliferation of smart devices and ubiquitous connectivity alters security relationships, and question marks over how geopolitics shapes everyday security decision making.

e-Estonia is a truly sociotechnical project. It owes much of its success to the digital professionals who have carefully shaped it over nearly 30 years, and as this thesis has demonstrated, have often had the best of intentions regarding the security of citizens. Conversely, its ongoing prosperity is threatened by distinctly non-technical contemporary Eston-

ian politics. It is also a geopolitical and diplomatic tool, capable of building closer ties with like-minded nations, but also a tool for excluding ‘undesirable’ others. While there are numerous everyday security considerations of citizens within the e-Estonia project, there are also blind spots and those who are excluded and left behind.

Estonia has consistently provided wide-ranging online services for citizens, as noted by the research of Solvak et al (2018) who have noted the ad hoc implementation of e-governance services over time, and the subsequent service adaptation rates have increased through increased familiarity with those services. This research has demonstrated that e-Estonia has been a success story. However, rather than illustrating this success with quantitative data such as service adaptation rates or e-voting use (see Gibson et al, 2016) this thesis demonstrates the varied, sociotechnical interactions which encompass everyday interactions with and the political utility of e-Estonia. The thesis has sought to highlight the diverse nature of e-Estonia, looking beyond statistics, and instead closely interrogating *why* e-Estonia is so widely accepted by Estonians, *what* the utility of e-Estonia is beyond e-governance, and *how* e-Estonia addresses some of the contemporary insecurities of its citizens.

This research has additionally suggested that the human-centric nature of digitalisation promoted by the Estonian government is somewhat overstated. As noted both by research participants, and highlighted within existing research, citizens were not consulted in the implementation of such ubiquitous digitalisation and e-governance (see Kattel & Margel, 2019). The growth of e-Estonia was heavily dependent upon a ‘trust credit’ placed within the newly independent Estonian government in the immediate Post-Soviet era (Research Participant P, 11.04.2018). This ‘trust credit’ was utilised to develop a programme of digitalisation that was primarily concerned with cost-saving and economic growth. Whilst there have been many human-focused innovations, as noted by both existing research and the participants of this research, they form part of a wider national strategy, and strategising was undertaken at a top-down, national level designed to ‘leapfrog the west’ through fast, deregulated innovation (Burlamaqui & Kattel, 2016) rather than through citizen engagement, which was assumed rather than sought.

While Estonia’s X-Road enabled governance has been designed with citizens in mind (as illustrated in chapter 7) it has also involved citizens placing significant trust in state institutions which would not be permissible in other states. This might be evidenced in the Finnish government’s refusal to entertain online voting, despite otherwise adopting the features of the X-Road for its soumi.fi platform. This builds upon the work of Drechsler (2018) who argued that despite local antagonists and overly positive media reporting, there are limits to what can be extrapolated from Estonia internationally and that the e-Estonia narrative is a well-rounded exercise of PR rather than widely desirable. Whilst the research does find sympathy with some of Drechsler’s assertions, particularly relating to the perceived ‘slick marketing’ of e-Estonia, it nevertheless suggests that common collaboration and international expansion of the e-Estonia model *could* work in select alternate locations, albeit with more considered, human security-focused conditions. This builds upon Mäniste & Masso’s (2018) observations on Estonian institutional trust and offers suggestions for other environments that a similar (but not identical) model could function.

Furthermore, this research has noted the everydayness of connected devices, and their importance within Estonia – suggesting they represent a complex but crucial sociotechnical relationship with their users and are a meeting place for citizens, the state, and their devices. Whilst anxieties or paranoia towards connected devices have been discussed previously, such research has usually focused on data security (such as Medaglia & Serbenati [2010] and Sicari et al [2015]). This research connects those fears with everyday objects and illustrates the link between such objects, everyday security, and everyday geopolitics, suggesting such concerns are interwoven, like Pain & Smiths' 'helix' of everyday geopolitical concerns and everyday life (2009). Whilst concerns relating to data privacy and security were also important in Estonia, this took on an extra dimension when connected devices were used to access governmental services, providing an immediate link to geopolitical anxieties. Living with ubiquitous connected devices in Estonia also suggested an acceptance of risk in the name of convenience. Existing research on risk such as Bernard-Wills & Ashenden's (2012) study has focused on the discursive elements of cyber security and risk, whilst Hall et al (2015) adopted a more sociotechnical approach, engaging with human perceptions of cyber security risks in daily life. This thesis furthers this valuable research.

The project also concludes that e-Estonia has enhanced its international standing considerably through its specialised focus on cyber security and e-governance. Whilst ostensibly a state-centric notion, this research also contends that the idea of 'smallness' is also part of the Estonian identity, and demonstrates how geopolitical narratives find their way into everyday security concerns. Estonia's success in spite of its smallness was a badge of honour for research participants but also was a perceived source of unique vulnerability. This expands upon notable contributions to small state security, such as those of Crandall & Allen (2015) Burton (2013), and Thorhallsson (2012 & 2018). Panke & Gurol (2018) and Adamson (2019) have also noted the ability of small states to be agenda setters, and this research suggests both the possibilities and the limitations of e-Estonia's reach.

Further to the Estonia specific contributions of this thesis, the analytical chapters contribute conceptually to our understanding of the diverse, sociotechnical aspects of contemporary cyber security and digitalisation. These are elaborated within a particular, geopolitically charged case study and this study also conveys the importance of geopolitics to cyber security concerns. The research also concludes that further focus on the sociotechnical aspects of cyber security should involve the political, social, and cultural constructs that inherently shape the dynamics of citizens' interactions online. This case study is a particularly timely intervention, given the proliferation of connected devices, the increased cyber security challenges posed by ubiquitous digitalisation, and the human challenges of ubiquitous e-governance. Whilst, as addressed throughout this thesis, Estonia is a small case study, the thesis has wider conceptual value.

This case study is also distinctly interdisciplinary, and involved significant development of knowledge from the author's perspective, becoming part of an Information Security department, whilst also working with Political Geography and International Relations, the project engages with and speaks to multiple audiences. It is a reminder of the enduring power of geopolitics; the political nature of contemporary security challenges; the security dynamics of e-governance; and the relationships between these sometimes seemingly distinct subjects.

8.3 Cyber (in)Security and the Everyday

This thesis contributes to the tentative yet growing field of sociotechnical security research. Stevens (2020) has recently argued that everyday cyber approaches are vital in understanding contemporary security challenges such as AI. Stevens cautions against further automation and the removal of agency from humans in the ‘cyber security assemblage’ (2020: 168). This thesis broadly expands upon Stevens’ exploratory remarks on AI, noting the breadth of sociotechnical challenges e-Estonia poses. These wide-ranging sociotechnical challenges have been tentatively explored by Oravec’s (2017) investigation of the everyday security challenges posed by pervasive household IoT devices. Oravec similarly urges a degree of caution, concluding that developers and governmental agencies must do more to cater to citizens’ concerns, especially given how rapidly intertwined IoT devices are within daily life. The thesis also expands tentatively upon this research, noting the anxieties and insecurities generated by connected devices (chapter 6) whilst also observing some of the sociotechnical security built into e-Estonia, thus providing an illuminative case study. Moreover, the thesis furthers the arguments of Salminen et al (2020) who focus on a rights-based interpretation of everyday cyber security, highlighting the importance of accommodating human security in cyber security approaches, mindful of local communities and the effects of digitalisation. Salminen et al focus on the high north of Finland and provide an important case study with wider implications. This thesis, as with the above literature, suggests that sociotechnical approaches are vital to our understanding of increasingly diverse security challenges, including issues of trust and privacy, insecurity, and ubiquitous e-governance.

If we assume ‘everyday’ as being the mundane and embedded actions that litter daily life (as suggested by Lefebvre, 1991), then there is arguably nowhere better to explore the ‘everydayness’ of digitalisation than in a nation where internet use and digital services (public and private) are so overwhelmingly common as in Estonia. This thesis has sought to continually highlight the utility of everyday security and the sociotechnical as critical concepts to better understand the impacts of ubiquitous digitalisation within the Estonian context. Stevens & Vaughan-Williams (2016) argue that everyday security is a vital approach to understanding contemporary security challenges, but do not extend their research to the study of cyber security and digitalisation. Malatji et al (2019: 233) suggest that there should be equal importance placed on both the social, technical and environmental dimensions of information and cybersecurity, however, do not extend these claims to a particular case study. Chapter 5 of this thesis answered the research question ‘what, in the Estonian context, is the relationship between the citizen, state and everyday cyber security?’. It concluded that the Estonian relationship between citizen and state is uniquely forged by various historical, social, and political factors. It is also moulded by the ubiquitous digitalisation of e-Estonia. This furthers the observations of Cardash et al (2013) who note the novel nature of the Küberkaitseliit (Estonian Defence League Cyber Unit) as potentially adaptable to other nations and is further developed in Chapter 6. Chapter 5 also concludes that the power of digital professionals in e-Estonia is disproportionate to wider Estonian society, noting some of the contemporary political and social problems of Estonia that e-Estonia is ill-equipped to address, furthering the research of Drechsler

(2018) and Kerikmäe et al (2019) who argue that e-Estonia frequently overpromises, and the benefits are not felt by many ordinary Estonian citizens.

The thesis additionally addresses e-Estonia as a concept, and argues that e-Estonia is a term that refers to Estonia's e-governance systems, as well as a social and cultural phenomenon, which forms an intrinsic part of the modern Estonian identity. The thesis demonstrates that to secure e-Estonia, Estonia needs to be mindful of the myriad human and non-technical aspects which inform contemporary cyber security. This is especially pertinent given the diversification of cyber threats with the rapid expansion of the cyber into everyday life. It has also illustrated some of the ontological insecurities that cyber security can generate, building on concerns surrounding the growing threat of so-called 'hybrid' security challenges, expanding upon existing research conducted by the likes of Mäliksoo (2018) and Galeotti (2016), about the idea of information warfare as a tactic. This is often employed by Russia (Estonia's perceived primary security threat, as identified both within formal documentation and political statements, as well as this thesis by research participants).

This research has also highlighted the societal risk of cyber insecurity in Estonia, given the importance of trust to the functionality of e-Estonia highlighted within this thesis. The poor diplomatic relations with Russia (which show little sign of improving in the near future) continue to generate fearful everyday geopolitics (Pain & Smith, 2008). This anxiety of an assertive Russia, eager to meddle in the affairs of its neighbours was a cause for concern for many participants, demonstrating the importance of everyday geopolitics to research participants' cyber threat perception. To counter concerns of Russian aggression, Estonia has closely aligned itself with Europe and NATO. It has sought to demonstrate its worth to the west through its contributions to developing cyber norms, evidenced through both the Estonian presidency of the EU, and the Tallinn Manual contributed by the NATO CCDCOE located in Tallinn. For the participants of this research, there was also concern with events across the wider Post-Soviet world. Conflicts in Georgia or Ukraine were frequently mentioned by participants, suggesting the Post-Soviet label is still relevant, despite the protests of some who are unhappy to still be referred to as a Post-Soviet state 30 years after the collapse of the union (Erizanu, 2021).

One potential resolution to the challenges of securing the e-state is through the establishment of international norms and structures to prevent the spread of disinformation and educate citizens. It is somewhat clear that this must be done through international cooperation. As noted in the literary review stages of this thesis, data flows are not limited to national borders, and cyber threats permeate the borders of the physical world. Existing research has noted how the prestige of e-Estonia has given Estonia an elevated role in the shaping of these norms which exist thus far (Crandall, 2016 & Adamson, 2019). Ultimately, cyber threats will continue to be transnational, and both the EU and NATO cannot hope to resolve the cyber security and insecurities of their citizens alone. At some stage, it will involve collaboration and consensus building with others. The relationship with Russia will continue to define Estonian, European, and NATO cyber security pursuits for the foreseeable future. Given the current political climate in the 'post-Crimea' world, Russian relations with the west, NATO included, are at a considerable low point. Indeed, even though it often

does not seem possible, the formal relations between Russia and the West can somehow always get worse. The prospect of any outreach or positive engagement with Russia in regards to such matters is thus incredibly low. Estonia and its neighbours must consequently multilaterally build norms and an increased focus on regulation, transparency, and accountability. Increased research on the transnational flows of data and building cyber resilience is vital.

One of the lessons of e-Estonia that this thesis has highlighted is that cyber security is an ongoing process, and is fundamentally about building a trusting relationship with citizens. The average citizen will not fundamentally understand technology such as the X-road. However, it can be made more accessible through engagement and education, as the experience of e-Estonia has demonstrated. The project has also highlighted how crucial it is that citizens trust e-governance systems to operate transparently. e-Estonia helped to forge trust through regulation and transparency. This was abetted through the utilisation of everyday geopolitical tropes, patriotism, and the narration of independent Estonia as small but stalwart in the face of Russian aggression. Russian influence has been frequently characterised as threatening Estonia's independence and extends to the cyber realm (see Giles, 2016 or Pernik, 2017). This characterisation has filtered into the everyday geopolitical consciousness of Estonian citizens. It furthers the narrative of a small nation facing an existential threat, while e-Estonia conversely offers a solution for Estonia's national resilience. The existence of programmes such as the data embassy, a programme dedicated to the survival of the e-state in the event of Estonia's territorial integrity being threatened (see Robinson & Martin, 2017 for more detail on this) and e-residency, a supposed means to grow Estonia's population virtually (Tamppuu & Masso, 2018) further highlight the use of e-Estonia as a means of national resilience building.

Research participants highlighted a range of insecurities throughout this project. Some of which are fuelled by geopolitically-related security concerns, as noted in Chapters 5 and 6. However, crucially they did not feel that they particularly shaped their relations with the Estonian state. Indeed, they trusted the state and their associated services, i.e. e-Estonia implicitly. The overall narrative about smart devices, therefore, reflected feelings of insecurity, however, this did not extend to mistrust of e-Estonia itself. This highlights the distinct sociotechnical nature of e-governance and everyday cyber security concerns that e-Estonia encapsulates.

Regarding relationships with smart devices, these are nuanced, and influenced by multiple, and often conflicting factors, as this thesis has highlighted, particularly within Chapter 6. The thesis has highlighted that objects are a vital, and under-recognised aspect of the wider cyber security assemblage, as highlighted by participants' concerns with how these objects interact with e-Estonia. This expands upon existing research, such as Collier (2018) highlighting the need for a greater focus on smart devices. It has also argued for the importance of security infrastructure, and the potential unintended insecurities everyday devices can generate (Aradau, 2010). Furthermore, the thesis has noted that human relationships with smart devices can be altered by mundane interactions.

8.4 e-Estonia and the Challenges of Securing a Small State

This thesis highlighted the increasing importance of cyber security to conventional security while challenging notions that cyber security and security should be disparate subjects. It has engaged with small state security literature, which has also tended to focus on conventional security concerns. This thesis furthers research by Burton (2013) and Crandall & Allen (2015) on the cyber security capabilities of small states. The thesis illustrates some of the unique circumstances which led to the development of e-Estonia and how these are a product of Estonia's size. It also highlights the challenges it faces regarding cyber security and citizens' cyber insecurities.

The research highlights how Estonia has achieved a degree of soft power beyond the typical capabilities of such a small state through excellence in the digital domain. It draws attention to the different ways in which Estonia has achieved this, including alliance building (Bailes et al, 2016), acting as a norms-entrepreneur (Adamson, 2019), as well as establishing novel digital innovations to expand influence, such as e-residency, the data embassy, and cross-border e-governance (even though some participants felt some of these schemes were a gimmick).

8.5 Trust

This thesis significantly illuminates the role of trust in Estonia's sociotechnical security landscape. It notes the importance of establishing trust with the public when introducing such wide-ranging technological innovation. Moreover, it notes the specific context of Estonia in establishing trust. Notably, the cultural and historical factors which have shaped contemporary political attitudes. The trust placed in the Estonian state is the product of several unique factors which are not immediately replicable elsewhere. This furthers the work of Henshel et al (2015) who argue that trust is crucial for trust-building with the public and users, encouraging a renewed focus on this particular human-centric aspect of cyber security. The human centrality of e-Estonia is questioned within this thesis, noting the sometimes top-down way in which e-services have been introduced and a lack of citizen engagement.

Issues of trust have implications far beyond Estonia and have wide-reaching implications for the study of cyber security. Buchanan (2016) suggests there is no silver bullet for issues of trust, noting the complexity of establishing trust posed by the challenges of the modern world. This, he argues, is particularly pertinent to studying the role of cyber security in international relations, noting that digital devices and connectivity are a powerful tool for weakening trust rather than instilling it. This study illuminates some of the approaches of the Estonian state in establishing trust, as well as some of the notable challenges posed by increasing digitalisation and digital devices' potential to undermine trust in e-Estonia.

Research by Goede (2019) and Lee-Guier & Lee (2019) has also suggested that trust-building is central to the development and democratisation of effective e-governance. This thesis contributes to that body of knowledge. While not a thesis explicitly focused on e-governance, it is a vital part of the e-Estonia project. The qualitative approach employed by this thesis also provides a slightly different approach than the often quantitative approaches favoured by e-

governance researchers. It joins, for example, the work of McBride (2019) in exploring the motivations and human challenges faced by digitalisation, while also exploring some of the political and economic motivations which are often more central than the issue of trust in decision making. Yet, as this research highlights, issues of trust were core to establishing the e-Estonia vision domestically, although this was informed by a variety of attitudes to technology and governance which will vary in each case study.

8.6 Sociotechnical Relations and Ubiquitous e-governance

This study, by virtue of the participants sourced and the research design, adds unique added value to the study of sociotechnical relations and everyday interactions with e-governance. This research speaks to high-ranking digital professionals, yet interacts with everyday life in Estonia. The interview participants are a link between the world of e-Estonia's technical experts and everyday life in Estonia. Participants are largely aware of their privileged position but they reference wider public opinion, and the thoughts of their personal friends and families. What glues those two seemingly disparate groups together is a shared belief in the Estonian state, as well as the belief that Russia represents a threat to the state via digital means. The research participants add unique insight into e-Estonia, given they are effectively its architects. Whilst, as noted in the thesis, e-Estonia was largely imposed as a top-down process, this research has also highlighted the interplay between high-ranking digital professionals and their everyday concerns. Whilst there are undoubted differences among groups in Estonia (which are increasingly evident politically, given the rise of the populist right and their anti-elite discourse), there is also a degree of convergence on the matters of digitalisation, thanks primarily to the economic benefits it has provided. e-Estonia as a project and an idea appears to be safe relatively (for now) despite some fears for the future of the project posed by rising far-right sentiment (*Politico*, 2020).

The thesis has also contributed significantly to the field of e-governance, highlighting the insecurities of citizens, and also the limitations of what can be achieved. In terms of the Estonian experience, the author found criticism from participants hard to find. This was somewhat surprising initially, but as the research progressed, and the author spent more time embedded within Estonia, the functionality, convenience, and fundamental trust relationships which all work as a sociotechnical assemblage become beneficial to the convenience of e-services being heavily embedded in daily life. Despite hope for more critical insights from research participants, it became apparent in the research conducted, that overwhelmingly, Estonians approved of e-Estonia, echoing the trust in institutions noted by Männiste and Masso (2018). Indeed, unprompted on several occasions, participants aired their disbelief at the antiquated approaches in the United Kingdom, and that more of the world was not interested in replicating e-Estonia as a model, noting the popularity of services, as noted by research such as Solvak et al (2018) and Gibson et al (2016). However, participants did offer considerable insights as to why Estonia was different in this regard, noting that such services might not be appreciated in other countries, or seen as intrusive, justifying the need for research to better understand the Estonian relationship with technology and online services. Furthermore, the research highlighted that Estonians did not believe that cyber security was something that could be achieved unilaterally, but that it was indeed a collabo-

rative process. Particularly, this was emphasised in the field of e-governance and security, as evidenced in Chapters 6 and 7.

The thesis identifies the importance of the X-road software, which, as discussed in Chapter 7, is the data exchange layer with which the e-state functions. This has been expanded to include the functionality and also the services and human security aspects of the e-state. The thesis has highlighted how exporting the Estonian e-governance model, together with goals of wider Nordic interoperability has come to represent a strategic, foreign policy objective and a unique opportunity for Estonia to expand their influence and value. It has then argued that this represents some wider human and everyday security benefits, empowering citizens with ownership and management of their data, as well as providing cross-border services if implemented on an international scale. This is the case currently in Estonia and Finland, and cross-border services are under development in Iceland and the Faroe Islands, as identified in Chapter 7. The thesis has further noted that e-governance services should be selected based on local priorities and that local social, cultural, and political sensitivities are of the utmost importance to cater to the everyday security needs of citizens.

The thesis has furthermore demonstrated the varied nature of integrating e-governance platforms internationally. This can enhance the everyday cyber security of citizens, and utilising Estonian collaboration and international cooperation with Finland, Iceland, and the Faroe Islands as an example, the thesis has shown how interoperable and integrated platforms can have real, everyday security benefits and securely accessible online. The mutual recognition of digital signatures between these nations is also a tangible human security benefit, and Estonia continues to lead in pushing for further international recognition at a European level. Cyber security has provided a niche for Estonia to greatly expand its international influence, secure domestic consensus, and generate comparative economic advantage. It has also provided an opportunity to demonstrate a commitment to rights and human-centric security agendas, as opposed to the more traditional, realist forms of security often pursued by larger powers. It has, however, also been somewhat cynically deployed on occasion as a source of soft power (Hardy, 2020).

8.7 Methodological Reflections

The research methods utilised by this thesis might be described as conventional for qualitative analysis. The original data contribution consists of interviews with high-ranking digital professionals, numbering a total of around 30 hours. These have been transcribed fully and appear in the annex of this thesis and anonymised per ethical guidelines. They were conducted with various digital professionals from both the public and private sectors in Estonia. The sourcing of these participants is reflective of the Estonian government's approach to e-Estonia, which involves heavy collaboration between the public and the private sector, therefore a mixture of participants from both made the most sense to achieve a broad overview of Estonia's digital professionals. The project was an organic process and was gradually adjusted throughout the lengthy fieldwork process, as the research developed. The following reflections by the author consider how this study might have been conducted differently, or how the chosen methods might change the findings of the project.

- Upon reflection, a more comprehensive field diary, and utilising a more explicit ethnographic approach would have been useful. It might have been beneficial in terms of documenting the many informal discussions which informed the author's knowledge of cyber security and e-governance events and during time spent as a visiting fellow at Tartu University. The length of time spent in Estonia – nearly two years – was unforeseen in the initial research design, but facilitated by an extended spell due to new funding being obtained.
- Focus groups, planned in the original methodology, proved impossible to source and were the source of many wasted hours in trying to achieve. The practicality of getting individuals in the public and private sectors together during the working day proved problematic and unfeasible. This required flexibility and adaptability whilst gathering data.
- There are limitations to our understanding of the 'everyday' that can be extrapolated from interviews with high-ranking digital professionals. Any conclusions drawn as to the applicability to ordinary Estonians are somewhat caveated by this approach. Nevertheless, these insights are important and offer crucial insights into the sociotechnical design and utility of e-Estonia. On reflection, the research could perhaps have reached out to Estonian Riigikogu members and MEPs with expertise in the technical field to expand the dataset, as well as to the armed forces and the Baltic Defence College for further consultation.

This thesis might also be viewed as a positive argument for increased qualitative research in the field of e-governance and cyber security. It can serve to further the case for increased engagement with practitioners, policymakers and professionals, exploring their security concerns with systems, and impact on the wider public.

8.8 Implications

The implications of this research hopefully illustrate the growing case for a greater focus on the everyday security anxieties of citizens, as well as an increased focus on the utility, and limitations of e-governance and digitalisation depending on geographic location. This thesis concludes that Estonian e-governance is highly successful and functional, but this is contingent upon multiple unique factors which are not easily replicable.

From an academic perspective, the thesis furthers research in everyday securities, exploring a previously unaddressed cyber angle to this research. It has also provided an overview of the sociotechnical factors which have helped Estonia rapidly digitalise and were crucial to the creation of e-Estonia. This research has been mindful of arguments that security is most achievable not through raw power alone but is built through a common community (Booth, 2005: 38). e-Estonia is built upon community foundations, although its imposition was notably top-down, as this research has illuminated. Future research should recognise the value of social and cultural factors in understanding sociotechnical interactions.

8.9 Summary

In sum, the key contributions and achievements of this thesis include:

- A detailed sociotechnical analysis of e-Estonia
- A focused case study on the importance of socio-cultural and historical factors in developing e-governance and security solutions
- An illustration of the soft power potential of e-Estonia (based on cyber expertise and e-governance) and how small nations might find additional diplomatic and geopolitical power through specialisation in niche areas
- A unique case study featuring the security concerns surrounding connected devices, and the data securities and insecurities they generate when combined with ubiquitous connectivity and e-governance
- A demonstration of the clear link between geopolitical narratives surrounding threat perception and cyber security anxieties and the
- importance of the ‘everyday’ and non-technical aspects of cyber security to e-Estonia
- A study of the danger that Estonia’s populist right poses to the future of e-Estonia

Whilst this thesis has some limitations, as highlighted in this chapter, it demonstrates an original contribution spanning interdisciplinary research fields including security studies, geopolitics, e-governance, and cyber security. This reflects the diversity and the sociotechnical nature of e-Estonia. The findings of the research could have potential utility to policymakers, security developers, and practitioners, as well as academic researchers.

8.10 Future research agendas

Future research in this area might further explore aspects of small state security related to interoperable solutions, the development of institutions, and the establishment of digital norms. Further research to interrogate Estonia’s international e-governance relationships is crucial, and the NIIS initiative should be further investigated as it expands to further nations and services. Further research may alternatively choose to focus on collaboration in Post-Soviet space. Azerbaijan, for example, operates a similar system of e-governance, utilising Estonian technology. The geopolitics behind these developments would make for an interesting research project. It would seem, at face value, that Estonia is less eager to emphasise and promote links with Azerbaijan (a regressive, non-democratic regime with a poor human rights record) but is happy to provide technical expertise and profit from a diplomatic relationship with that regime. For some of the positive, philanthropic goals of e-Estonia, profit is vital. This has been highlighted by existing research as a driving force of technological innovation by scholars of digital and surveillance capitalism (such as

Amoore, 2008). Azerbaijan has now similarly begun to offer e-residency (DTH Azerbaijan, 2019). This is similar to Estonia and utilises X-Road based technology supplied by a private Estonian company. This has received less international attention, however, and crucially does not allow access to the EU single market for business purposes. A comparative study, nevertheless, would be of interest.

There is also not yet sufficient interrogation of how such ubiquitous e-governance and digitalisation might be used (or abused) by a less democratic regime such as Azerbaijan. As other nations continue to roll out e-governance initiatives which imitate the e-Estonia model, additional research might focus on the security mechanisms employed by other governments, and should highlight the deficiencies of inappropriate security procedures (see Hardy, 2020a for discussion of Russian i-voting provision). There is also significant interest in developing e-solutions in Ukraine. The e-governance academy, headquartered in Estonia, has a branch in Kyiv and is developing cooperation and encouraging collaboration between the countries. One of the stated goals of the Zelenskiy government in Ukraine has been furthering e-governance and cyber security cooperation, with Estonia as a model (Kyiv Post, 2019 & Talant, 2019). Further research could follow the development of such cooperation, or indeed interrogate collaboration among other democratic Post-Soviet states also.

Additional future research might also address the issue of digital diplomacy and disinformation emanating from Russia toward Estonia and the Baltic region. Tentative research has already been undertaken in this field, exploring the nature of the Russian MFA's use of humour as a diplomatic tool (Manor, 2020) yet analysis specifically focusing on Russian digital diplomacy towards Estonia and the Baltic States has yet to be undertaken. As disinformation was identified as a key security concern by many research participants, a greater understanding of how Russia targets the Baltic region may be beneficial. Finally, future research may focus further on everyday relationships with connected devices, expanding the focus to explore new IoT devices which are increasingly commonplace in daily life. This could build upon the research of Coles-Kemp & Hanson (2017) as well as the findings of this thesis, exploring the connections between everyday interactions with smart devices and their link to national security.

Annex

Interview Questions

Researchers note: These questions are utilised through the interviews as a guide to discuss key topics of discussion. Participants were informed of the content of the interviews ahead of time, and the author also introduced his research area, as well as chatted with participants regarding their occupations ahead of the interview. All interviews were semi-structured, to allow for discussion to flow, and reasons for this research design are highlighted in the methodological chapter of this thesis. As can be evidenced in the transcriptions, some interviews were more tightly structured than others, based on the personalities of participants, and the order of questions was sometimes naturally altered by the flow of conversation.

Questions

- What does cyber security mean to you?
- What measures do you take to ensure your own cyber security? (procedures / cyber ‘hygiene’ / everyday practice / VPN?)
- Do you, for instance, utilise a camera cover for your smart devices? If so, why / If not, why not?
- Do you take any security precautions with your smart cards? (for example; an RFID blocker)
- Do you utilise contactless payments with bank cards or your mobile phone?
- What are the key threats to cyber security in Estonia? (top 3 in importance, if possible)
- What are the key threats to your personal cyber security? (top 3 in importance, if possible)
- Can you describe the Estonian approach to cyber security? Do you believe there is anything unique (after all, in many areas of security discourse, Estonians are considered experts in the field)
- Do you believe that e-governance, and the use of digital identities, makes Estonian citizens feel more secure?
- If not, in your personal experience, what are the common security concerns of Estonians?
- Do you think these are commonly linked to ideas of national security?

- Do you think there is something unique to Estonia, or Estonian mindsets that make them more willing to accept technological innovation?
- Do you feel Estonians are more security aware than other European nations? (such as the UK, for example)
- Do citizens have a role and responsibility in ensuring their cyber security?
- What is the future for e-Estonia? Is it desirable to see this across the wider region? Nordic? European?

Figure 9 (below) demonstrates the clusters of popular codes and their relationship with one another. These clusters informed the analytical direction of the chapters.

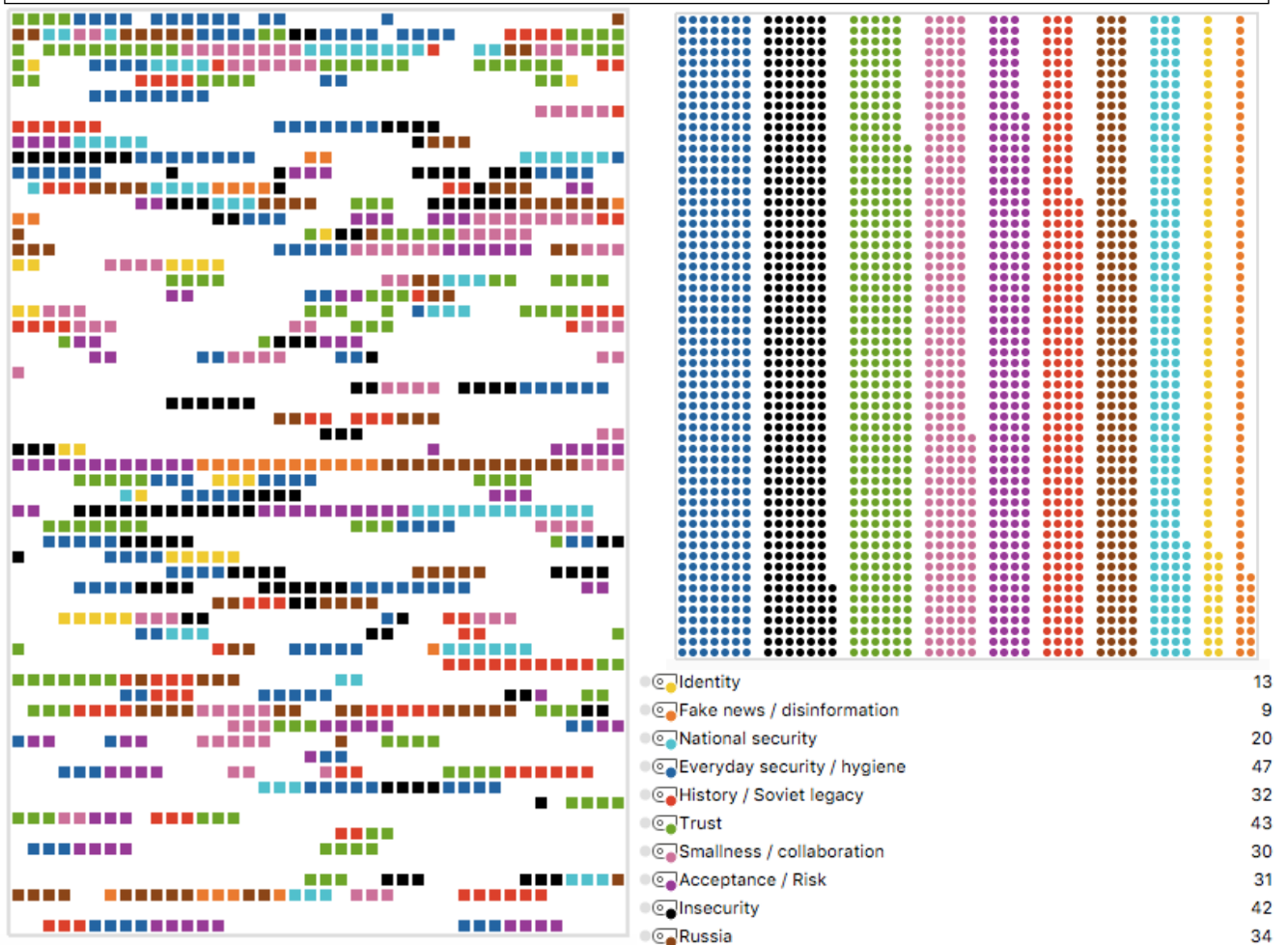


Figure 10 (above left) & Figure 11 (above right) Coding - in interview order (10) and ordered by frequency (11)

Interview Transcripts

Participant A - 01.02.2019

AH: What does cyber security mean to you?

A: Well... I like to use the traditional CIA approach when talking about cyber security... so confidentiality integrity and availability, so for cyber security and incidents relate to those which have a direct impact on the confidentiality, integrity and availability of information or systems. One or more out of these three parameters are being influenced... what do i mean more specifically... confidentiality refers to the system is being protected against unauthorised access by third parties. Integrity refers to how well data is protected against unauthorised changes or destruction. and availability measures whether is system is up and running as expected

AH: Thank you, and can i ask what measures you take to ensure your own cyber security?

A: Well, first of all, i've undergone the cyber hygiene test that [REDACTED] has developed... so this is a bit of a product pitch, but [REDACTED] has done this work for the state information agency of Estonia, I like that. It's good, it maps the persons own individual risks when using cyberspace, and it measures things like attitude and gives a holistic approach to things, so it starts with a personal attitude and extends to your hygiene in exposure in things like social media, as well as corporate culture, things like shortcuts.... more specifically, as a standard, as a while i used a cover for a camera... a screen protection tool... (A product not specifically discussed within the research, but prevents onlookers peering over shoulders at screens)... two factor authentication, uhhh VPN access to the internet when available.... sometimes you have to measure.... i mean, encrypting your emails as well, you have to decide between quickly sending your information quickly and also protecting it... it's the same dilemma in the physical world. It goes back to my days working for the Presidents security advisor, stuff is classified, when you produce a memo you want to have a proper classification... but then sometimes *laughs* if it's top secret you can't even write it, so the question is like, you can't talk about it even, and let anybody know, and say you don't have the time to go to the top secret rooms to use appropriate secure computers... there's compromises to be done.

AH: Just to pick you up on the hygiene test, it'd be great to know more, I'm not aware of it

A: Yes, I can send you a link. It's something outlined also in the annual cyber security assessment which the national information authority produces every year. In their last edition, they do mention this. So it's an online hygiene test, developed working with RIA, if you've come across that in some of your other interviews?

AH: Yes

A: So they're largely in charge of infrastructure and information systems. So basically it's a test that you can do online that maps your risk behaviour in cyber space, starting from perceptions and discipline, your knowledge of removable media... it covers a lot of basic things as well, not picking up random usb's and sticking them in your computer *laughs* it doesn't preach though... the philosophy isn't pass or fail, but it allows us to map the precise risk management, with attention devoted to specific weaknesses. So it's, it's not like... it's a holistic map. So when you usually take a test and you say, get 80 or 90 out of 100 you feel good... well, this text addresses that ten percent vulnerability.... and it's not recommended to all public officials in Estonia, that includes at the institutional level, but also like doctors, policemen, you know, we've shared 50'000 licences to Estonian state officials... uhh and yeah, it's also available in a dozen different languages and we sell it elsewhere.

AH: Cool, and this has been developed in collaboration with the state?

A: Yes

AH: Thank you for the information! So, i usually ask about the camera cover, but you've already told me that you do use one, but do you use... or sorry, do you take any other security precautions?

A: A screen cover, yes... well, i try to avoid usb's generally... regular security checks, updates... yes, basic hygiene I guess

AH: An RFID blocker?

A: No, i don't.... sorry, what are those again?

AH: So they're usually sleeves which block a signal from smart cards usually. They're most commonly used for bank cards with contactless payments I guess

A: Ah, i see... but no, i don't use these. I guess i just don't think it's really on my threat radar

AH: No worries, so what do you think the key threats to cyber security are in Estonia?

A: First... i think it's the capacity to have a place that's responsible for driving the strategic thinking... it's vague, but who is to ensure that you have enough money spent on the cyber security holistically... because we are so dependent on only innovation. It's not just the brand, it's like real time security, how seriously we take it, but this is a field where you have to keep on running to stand still.... i spent nearly twenty years in the public sector before joining [REDACTED]... the question is... who is... driving the forward leaning thinking in this field. In the state, who is responsible, but doesn't get lost in technical detail... but also is fluent enough in the technology to understand what are the threats.... and carries political leverage and weight in budget discussions... i mean, it's not just about money, it's about talent, but you can't just expect people just to work for free. So this kind of structural / strategic concern is number one, for me. Number two, the security of the supply line. That's universal, but also for Estonia. We had the issue with the ID cards of course recently, about a year ago... there's papers out there discussing this of course... I'm sure you spoke to people about this at RIA too? So way down in the supply line, even if we discover a bug or security concern... do they consider the government of Estonia an important enough client to inform... i mean, maybe we were not considered important enough in the food chain... but the whole country is dependent on this! But more generally... the more we build things.... big things, NATO headquarters big, for example, you outsource things, and it's very difficult to keep an eye on the whole supply chain.

AH: Do you think the relationship between public and private is problematic in this regard?

A: es, that's part of it... but yes... you... or whoever orders, is important and they build relationships with the biggest actors on the market... but the question is when you zoom down... like the small parts get outsourced... and then who is behind some of these partial works... and which country... which government... how do you guarantee security on each phase of work when its something complicated as constructing a headquarters building, or whatever. The ID card that is mandatory for your whole population, that's important

AH: So would you be concerned if some parts of this technology that you've cited in this example is coming from different places? So i know of course the recent Huawei controversy is huge news right now

A: Exactly. And then part of that s... how do you.... it takes guts to spell it out. It's guts and its political wisdom and courage to spell out that, yes, it's the policy in Estonia... that government officials shouldn't use Yandex taxis for example, or we take a position about Huawei productions, or we take a position that we should not use Kasperky Anti Virus tools... so it seems maybe common sense you shouldn't use those if you consider Russia your primary security threat... but, yeah, it's not down in the paper anywhere. So the security supply line, it's a question of strategic investments, but cyber security companies... private sectors.... what restrictions do you make in terms of accepting investment from outside. So... Estonia is a small place you know... Guardtime, Cybernetica, Cybexer... we have a few main companies... but what are the measures for these companies, other than say common sense, for them to not accept Deripaska (a noted Russian oligarch with links to the Kremlin) Russian investments? Or not to hire Deripaska as a member of their board?

AH: So you think there's an important trust relationship with Estonian private firms as well?

A: So yeah... I'm playing devils advocate, no Estonian company that wants to be taken seriously would ever do it, but we... i don't know. Russia investing. So it's the case in Finland. So say Russia wants to buy some ports in North Eastern Estonia, where they invest in an area... say near Tallinn, or they buy an island, and then they start their nuclear training there... *laughs* i mean, this is going away from cyber, but these things happened in Finland, where islands were sold off

AH: So... getting away from national level, what do you think the key threats to your own personal cyber security are? Are they actually related to the national security concerns?

A: Yeah sorry, I'm just thinking i only gave you two for the last answer... So yeah, the third would be like training, or lack of training. Or training the human being in cyber. So it's both the basic cyber hygiene and also education... so how do we ensure cyber in our education from an early age, so as soon as kids get hold of smart phones, which is Estonia seems to be about age 7, and they go to school and parents give kids phones because they have to be reachable, and very often these are smart phones. Also, IT personnel and making sure that they know what they are doing, and these are the people they trust... and how we measure their performance... and then at the top level. Management, how do we ensure they're taking it seriously.

AH: Ha thanks,

A: and to answer the other question, on an individual level... i think i share some of it. I hope I'm not being targetted individually... but what are my key threats... trolling or social media identity theft. Is something that concerns me. Ummm... it could do harm on a personal level a lot, and our image is very much linked to our online image. But yeah, the integrity and confidentiality thing, your phones or emails being hacked is something.... information security i guess. A lot of our lives are on social media, and I suppose if someone wants to build a file, we sometimes make it very easy

AH: So, do you think then that these concerns that you talked about, do they relate to ideas of national cyber security, or do you think that they are two very distinct areas, your personal cyber security and national cyber security?

A: No, I think naturally it comes together... well, it comes together in the fact that RIA tries to keep, at least for public officials, a level of cyber hygiene, that there are... umm... practices and suggestions and availability of your social media in places... well, when i used to work in the public sector.... in the ministry of defence and so on, you have limited access to your social media, and you have to think twice.... and there are some good conduct recommendations. The same.... very much for the use of phones, where you take your phone, how you conduct your calls, preferably through facetime, but not since last week when they discovered the bug... how much information you're sharing over various different SMS's, or using more of the safer apps like signal... and so on

AH: Could you possibly describe the Estonian approach to cyber security? Do you think there is something unique about how things are done here? Of course a lot of security discourse has suggested Estonians are world leaders and experts in this area

A: Yeah... umm.... well, Estonias approach to cyber security, I think comes from critical thinking and self reflection in Estonia, vis-a-vis cyber security, and started on a large scale after the 2007 attacks. Those were... that was the time when top decision makers as well as everyday people really understood that cyber attacks can have as much of an impact as physical attacks. We had people looting in Tallinn because of the political tensions created by the removal of the second world war monument, from the city centre to a military cemetery, and online attacks took out a lot of online services.... so everyone realised how vulnerable we are. That was a wake up call. After that, a year later, Estonia plunged into the first national cyber strategy as part of the national security strategy, so ever since then Estonia really understood how cyber security is an integral part of cyber security, and that's plunged in the thinking... so it means it's not a one time action, the state information department was set up, and they're the point of contact for problems. They're where the search is location, and they're the one responding to critical infrastructure requirements... they set requirements and check if the industry needs them. So the Estonian approach is comprehensive. And finally, the RIA is one that keeps the community together, learned from 2007... that includes public and private officials. So there's a revolving door almost, and naturally you need the private sector. The information sharing goes both ways. Mostly private to the state, but in order for this to work... what's in it for the industry, so in return the state creates some outreach events and offers training... free training... so there's something in it for everybody. Trust has to be build before

a crisis hits, and trust is built through common, informal event. Conferences, information sharing, things like that. Informal activities together.

AH: Thinking about Estonia and the e-state... do you think that all of this actually makes Estonians more secure, also in relation to the events you talked about in 2007 for example

A: *laughs* Yes, there's a funny paradox there... you would think that it would make Estonians feel much less secure, but the result is on the contrary... there is also a very conscious choice of the government back in 2007 to share the fact that we were under attack. We did so in public, and with an international audience, and we have to realise that it didn't come in of itself, it was a conscious choice, there was a discussion in the government crisis division and not all were happy about sharing this information because after all it was embarrassing being under this attack... but sharing it with the public led to the public understanding what was going on, and understanding why services were not available at the time of crisis and attack in 2007, and then also when you understand something, you trust it more.... and people... when it all ended well in 2007 - after all, it was a simplistic DDOS attack - peoples trust increased. Actually, the fact that the government... and all together, many private sector volunteers stayed to help the systems... that resulted in a trust boom... an increase of trust... and its been a trend all throughout... the time is taken to explain to journalists and outside observers, at e-Elections for example, how the integrity and security of data is maintained. Journalists... the ID crisis last year it was the same, the prime minister didn't hide away, he actually said yes, this is bad, we're working on it. So i guess... umm... it's thus, citizens feel more secure. Well, more I'm not sure 'more', but regular progress is being made and positive studies on the i-voting for example... after all, these services are convenient, and they are really comfy... the question is... well. the key is that it's taken seriously. So far, we believe it is. There's no reason to stay complacent however.

AH: Do you think there's something unique to Estonia in this regard? That people are willing to be involved in this? In other contexts this would be deeply embarrassing for a government, is there something unique here that allows for this openness?

A: Ummm, well part of it is that we live on the edge, and recognising that nobody is at fault for the geopolitical location of Estonia... we have the neighbour that we have, and we don't turn a blind eye to the fact that our eastern neighbour, Russia, is malicious sometimes. That is shared... so security is always very important for Estonia, and people largely share that understanding. It's different in other European countries. It's also pride, national pride. I think that Estonia became this digital forefront ... became a source of pride, and it dates back from the nineties, you know, why people want to do it... and it all links to the trust, but people enjoy Estonian being the place where digital innovation is adopted, because it was the thing that took us... well, when we became independent in the nineties we were lagging behind from Western Europe, but we very much wanted to be part, and at the forefront like... a civilised western country, and the digital gave us an equal competition ground... that was where we were equal with others in the nineties, because no one had e-governance much. So, I'm drifting away from the answer somewhat, but that's why Estonia is special.

AH: Well you've actually led into my next question very much as well, which was if you felt Estonias were more 'security aware' than other nations, and indeed you may well have answered it also with your Geopolitical comments

A: Yeah, and it's wider than cyber... i definitely think, as i said we are definitely more aware... it's like northern Europes Israel, we are feel that freedom is not guaranteed, and we have to fight for our freedom. It's not an open war, but it's a constant battle, especially for people working in the security and defence sector. Hybrid is the trendy word I guess. But we definitely are more security aware than most, and the threat perception is quite clear.

AH: Do you think then that ordinary citizens have a role and responsibility in ensuring their own cyber security, and more widely of the nation?

A: Absolutely, and that comes from cyber hygiene and thats the foundation. If it's a house, you build from the foundation, and cyber hygiene is the foundation. Education as well. Yes, we all have to make sure... we make sure you wash your hands in flu season, or following the traffic light rules... but then also, whats special about Estonia the volunteer national defence organisation, i guess you've come across in your interviews... how it all started... and the 2007 attacks demonstrated how we needed a cyber division, and people from the private sector volunteering at times of crisis in helping the state... and helping make the state secure. It's a way for IT geeks... uhhh patriotic IT geeks... uhhh citizens.... to devote their time in ensuring cyber security even more *laughs*

AH: I guess, my final question, is what does the future look like for e-Estonia? Do you think the Estonian model will spread further?

A: Absolutely yes.... first in Northern Europe, i mean, it doesn't have to be Geographical... but it's about mentality and trust, and umm... well, i remember when i was the presidents policy advisor, for when the president Ilves met with the then new Finnish president Sauli Ninnistö, and he was thinking, what could he push to start afresh, to push a new, positive relationship with the new Finnish president, and of course it's always useful to suggest something concrete, so he decided that he really wanted to push the X-Road being interoperable between Estonia and Finland in this regard... and I think it's crucial for Estonia to extend its system beyond the country because we've invested so much into it... and if the EU, and well naturally, everyone is developing their digital online services, and if the EU takes a different path, we run a risk that our investments are not compatible with the model the EU adopts, so its crucial for us to gain critical mass with our X-Road way of thinking, so this is something.... this is a model for Brussels to care about when developing future strategies.

Participant B - 08.03.18

AH: *Introduction and explanation of the project*

B: (Introducing herself) So just so you know, I also am from a political science background and I got my bachelor's in political science. And then I got my Master's here in Estonia at the e-governance Academy. Excuse me. e-government services and Technologies Masters at to do and which is a joint project with the e-governance academy. And so my my interest initially was there internet voting system because back home in the u.s. I worked for I was a political operative. I worked for a progressive candidates in one of the most conservative states in the country. Which one am I like to ask which one? Yeah, so I live in Oklahoma. And so anyway, I got tired of losing and so I decided that you know the internet voting.

Would get more people voting which might help have better outcomes, so I came here to study their system. But when I'm when I was listening to you talk about your project to me the first thing that pops out his trust. So what you're talking about is how you get you know, how and why is it that the Estonian is trust the system so, you know because it's funny because I just emailed a girl who from Cambridge who was interested in knowing more about how to run an e-government and how to get people to use that e-government and that's like the million-dollar question. And so there are a couple of facets and let me start by quoting one of my favorite teachers who actually works and is on the board of the e-governance academy and he said, so if you take the view if you look, The views about government and he broke them down to three there may be more but he broke them down into three categories. So the first category is you have the Anglo view, which is your country my country. This is this is where we view government as definitely not a friend, but more like an enemy the government is bad. The government is out to get you they just do bad things and they miss manage our money, right? This is basically what government this is the view of government for most of the Anglo countries. So then you have this sort of Parental view of government. You have a motherland Fatherland, they're there to set boundaries and limitations for for the constituents for their own good, right? So this is the sort of Parental View and then you have the Nordic View and in the Nordic few government is your friend there there help they're there to help facilitate.... The things that you need so life is better. So let me just say post Soviet times Estonia falls into this last category that sort of Nordic view. That's that is the first thing that helps with trust. So first they just inherently trust this new government.... but it is the services people care about. The state has provided a service which is secure, but security is not citizen's primary concern. If you talk to most people... the average person on the street... they perhaps don't think about the security so much

AH: Yeah..

B: Okay. So then the next thing I would say is they offer services that are accessible and that work and then they gave them the government gave these stunning people cookies in order to to get them to use use the services be it. If you pay your taxes online you signing in with the ID card, you'll get your refund in five days by law or you can use your bus ticket. If you if you link your ID card with your bus ticket, you can use your ID card now as your bus ticket and so everybody and they got a discount. So everybody wanted to do those things. Another another thing is they taught them as they went along and

They enacted they had classes that they did there was a program called tiger leap. Yeah, which you may have heard about right this help teach kids then they had look at World which was a program that was done through with banks and ngos in order to educate older people about how to use technology and it started with the bank's it started with this is how you use your debit card. This is how you use online banking and these sorts of things and then they set up computer stations in public places for people to use and this is early on we're talking back in the 90s to try to educate the populace. So you have these things and then

I would say as far as trust. They don't have the they they didn't have the Legacy system that your country my country have right? So when when when new technology is wanting to be deployed then they can be more agile in adoption at the legal level because you have to look at you have to look at the technology on various levels and from a technological standpoint anything that we do in Estonia we can do in the US or the UK, right? However, they had less Legacy systems to fight one and two they have they have the political will to do something different here. We actually have no political will in your country my country to make any sudden movements.

AH: Yeah, we have no ID cards, although we attempted it in the UK. It was around 2006 2007, and dropped due to popular opposition. I've had to check the exact date to the Blair government attempted to introduce them and it was abandoned when they realised. They just wouldn't have a majority to get it through parliament

B: And then you'd the standard debate came out about how it would be severe land and the government overreach. This is the same sort of libertarian angle brand of thinking that you would be talking exactly but they also say it's also posed to them like? Here we're going to implement this with no thought behind the rollout, right? So the rollout of service e-service. This is also important, you know you for instance when the ID card faux pas happened. Yeah last November, right? It was talked about on the TV there were placards up at the bus stations. There were articles in the newspaper. They were talking about it on social media the you know, you have the information Authority putting out tweets and LinkedIn news about about the ID card. So roll out and how you Market rollout is hugely important, and we talked a lot and in some of my classes about the marketing aspect from the public sector in adoption of E-Services, you know, they don't want to spend money on it. However, if you don't tell people why

They're not going to pay attention. It's the same with cyber security. If you tell people okay, you can't take documents from your you know from work to and put them on your home computer. You know, it's just a no-go and you don't tell them why they may not get it and they may do it anyway, because you didn't explain why so it's the same thing with with e-governance in that respect. If we don't tell people why this is needed why it's a value to them then they may not they may immediately push back. So Oklahoma is one of a handful of states that still hasn't complied with a piece of legislation called the real ID act which was which was done in like 2005. I think it was a post 9/11 piece of legislation it said that all drivers licenses had to comply with a certain threshold of security meaning a watermark a chip, you know a hologram something that was less likely to be forged and you have a handful of states that said no we're not going to do it. So here, you know 13 years later. They haven't done it and now they've they've been told that if you don't do this, you're not going to be able to fly domestically with your driver's license. You're going to have to get a passport.

So now their hair is on fire Oklahoma being one of them and it's going to take them two years to now Implement a new drivers license scheme. So you're going to have a year Gap where people in the u.s. Cannot people in Oklahoma cannot fly with their drivers license and I of course laughs hysterically because I was like live see act dumb get punished. You were told ya. Yeah. It's not like this was new but they actually pass legislation in the state of Oklahoma that said we are not going to comply because of x y z reasons. Yeah. So anyway, but no one told them explain to them why you know look in the long run. This will be beneficial because of da-da-da-da now, I've every time I go home I try to get in touch with legislators and I say look, hey since we have to since we have to implement the ID scheme, let's do a chipped ID. Let's build up services for that and and it will lead to you know, digital identity laws and things like that that will position Oklahoma ahead. That being said this is also the state that as of today is the worst and teacher pay and the teachers are about to walk out of classrooms, you know, but marvellous and I'm trying to get them to you know, do e-governance.

But anyway, I think that so so one of the main things that I challenge you is, you know to think about it as a trust issue and and one of my friends wrote her thesis on the trust issue and she asked all of her Estonian friends, you know, why do you trust the system and basically was just that they do. They're not there to harm us. So then how do you change the narrative?

AH: I mean, based on similar questions I'm asking... the overwhelming response I seem to get is well one they trust them but to also because there's a Service attached to it. They see a value in it right?

B: So, whenever i try to talk about it back home, I try to start out with the features and benefits. So I say what if you could pay your taxes in less than two minutes, what if you could sit on your couch and vote in your pyjamas or what if you never had to go to the DMV ever again? Yeah, and and this this is the wow. Is that even possible? Of course it is of course these things are possible but that in I found because I mean, you know, I've been talking about these things for several years now and and I find that if I start with that approach versus what do you think about a chip tidy now, if I ask people in the military they've had it for a really long time they understand it but if you ask the common person they don't get it now.... Voting online is a little touchy especially now people like people if you say what do you think about online voting they'll immediately say no, but if you say would it be nice if you didn't have to go to the polling place on a Tuesday because it's in it on a Tuesday in the US and they're like, yeah man, that would be great. And I think of what that would do in areas where you know, they notoriously have fewer polling stations and longer lines. Yeah, that would

be really great. Yeah, all those things are possible, but the....But then you go up one layer and you go to the politicians and nobody wants to be first. They all want to be eight. So if you say but you could be first to be, you know to be a Trailblazer in this in this Arena.

Too much risk, right, like the Estonian data flaw one last year. And I know that they were having that they all talk about how transparently they dealt with this but it would be a major Scandal in the US. It didn't really like it was but it did what do you think the Equifax hack was it in essence was the same damn thing because I was I got caught up in the Equifax hack. They you know, so somewhere on the dark web is my Social Security number my date of birth my address every house I've ever owned my mother's maiden name. You know, how many kids I have whatever. Yeah, you know. So basically it's the same thing now that leads to another conversation, which is In the u.s.... Particularly, I think in the UK. It's a little bit more distributed? Well we have one, we have our social security number right in the US and every thing is attached to that. So if I go to the if I go to the you know, the doctor's office, they use my social if I go to my commitment renew, my driver's license. They have my social the insurance company has my social my job has my social the state of Oklahoma has my social the course the federal government has my social the bank has it who I've I had literally have to give this to everybody in order to identify myself yet. I am supposed to keep it sacred and secure within an inch of my life.

Yet no one else does and again it's like you said before it's about ...Shifting the burden of that from the government to the consumer right now. They're not at fault. Now the bank what is the bank to the bank get takes out insurance in order if something gets, you know, if the data gets stolen then they get it they get a payback from the insurance company because they ensure the data but I still get the headache over it right? Yeah, whereas in Estonia for comparison. They have devalued the ID card number. So my personal ID code here in Estonia is not worth anything. If you have my code number, you can't do anything with it. Yeah, but if you would you could only do something if you had my card in my PIN codes. They have devalued that number to the point to where what does it matter? Right? So this is this is sort of the this is sort of the opposite side of the coin either either you created an ID number that you know is more valuable than anything or you create something. That's that's a value less without the token. Yeah. So and in this regard Estonia has done it the right way. This might be also another way to try to sell it to governments and government officials, right? Because basically we created a huge monster with the social security number. It wasn't actually supposed to it wasn't initially meant for all that right? It wasn't meant to be the identifier of all identifiers, but that's what it is.

AH: I did I had no idea you had such wide-ranging utility... see right in the UK. We don't really we have National Insurance number but it's just for tax purposes you provide it to a new employer but I mean it has no real utility beyond that then if you go to the doctors, you take some form of personal identification with you whether it's your passport or your driving license the first time you go and that's Right, that's about it. And it's all distributed in different ways.

B: Yeah, you know for the for the UK if you look at the voting Arena really and I've heard this and I may be incorrect that if you take a utility bill with your name and your address that prove you live and the in the place that you live you can vote with that that can that can that's enough to identify yourself?

AH: Yeah. So this is also not necessarily the most secure secure in anywhere because I mean all it would take would be you'd moved house your ballot gets sent out via post a few weeks in advance. So your ballot could be something out and then accidentally one of your bills girls and someone else is living there. Well, then can then go to a pool institution and the you yeah, the person you're not required to produce photographic identification because this is part of the ID card to be we won't have.... And your driver's license does have a photo, but you're not required to produce that.

I heard that as well and Ireland and I was like really like if the police stop you you don't have to give them your ID. Nope, they run your car tags, but what if you're driving someone else's car? That's not their problem. I was like, yeah that freaked me out a little bit. Sorry. I have to say yeah, but what about that's considered like an insurance issue so they can there's a centralised database. So if there to stop you they pull you over and then they run because the centralised database they give them a call and check that you're insured on that vehicle in one way or another the only way it would ever really turn out to be an issue as if someone's pulled over cars either stolen or that person. Yeah, they discovered that and for insurance purposes can't be driving it or doesn't have a license but you're not actually required to provide as long as you have a license, you know, you don't have to produce it. Yeah. Yeah. So I mean, that's the first thing you do in the u.s. If someone stops you.

You know license and registration, you know, you have to show that but that also tells you the the how far behind we are in in connecting databases and and digitising, you know, you shouldn't it shouldn't be that hard actually, so I should actually be able to handle my driver's license say it has a chip in it. They're able to run run my ID, which should them like here and here going to study it would connect them to they would be able to query those certain those five questions. They're allowed to ask, you know, do you have insurance are you is this your vehicle registered? Is it is it up to inspection? Do you have any criminal record or any past and fractions and something else? So anyway these five queries go out and they get that information they can make a determination. So I wish I wish we had nice things. Yeah, we've got a lot of nice things either if it's on.... So, I mean one of the other things when we talk about selling the idea ID cards as well though.

AH: Yeah, i mean, to be honest, even in the UK, we have problems with selling the benefits of an ID card even for security reasons...

B: Well, the thing is the passport all you only ever have to have it when you fly or bold leave the country I traffic but what if you were like like an Estonian people they can travel with travel with their ID card. Hey, yeah. I know I've seen it because it's got a big bottle. It's got the same chip in that a passport doesn't it? So it has the same legal credentials. But so what if what if they were to just somehow and that's what they did in the study at the beginning they offered if you were if you were going in to renew it. Now, the ID card is mandatory, right? Yeah, but if you win and you you apply for your passport and this was initially and you got the ID card at that point you got the ID card for \$5 5 Euros, so they so the government was covering. Part of the cost initially to again to get up take on it. Yeah. So if you if you offered it. Hey with the with the passport. Oh Yuri, issuing your passport. We can also offer you this digital identity which can be used in got it out of the countries as in the same with the same functionality for five pounds more. Would you like this option Hmm. This might be a way for people to try to you know, get used to this idea but really without incentives.

And you may have heard this from some of the people that talk about the ID card, you know, when they first launched it the people that actually had it used it as an ice scraper. It was the best ice scraper and and then then they offered then they offered it as a bus ticket they offered it to pay your taxes and they passed the law and then internet voting came along in 2005 ID card was introduced.... in 2001 2002 something.... So because X Road was 2001, the ID card came shortly after that. So yeah, the service is actually weren't there initially but as they started to sit incentivising it and they told everybody was mandatory, but it wasn't you're not penalised for not having it.

AH: Right and the whole way of that I've heard this described as well, so actually while you have to have it, you don't actually have to use it. You can put it in a drawer and let it gather dust if that's what you really want to do with it.

B: Right it makes you know, if you have mobile ID, then you seriously I just updated the certificates on my ID card after the change last week because I literally never use my ID card and it's that it was that situation where I needed to I needed a sign a document by mobile ID is not down because I just can't change phone carriers and my new Mac does not have a slot for the old USB. It only has USB C. So she's going to the really new ones. So my ID card reader didn't fit, and so I had to send the document to my my boss who had his ID card reader then when he put my ID card and it wasn't working because the certificates were out of date. He looked at me and he said really do you realise the company that you work for? Do you realise that we fix this and I said, yes, so anyway, so that's how it is. So I now have a functioning ID card but still no way to use it with my work computer. So but anyway, yeah, I mean you could literally just use mobile ID and well, you can't use you can you can log into St. Dot ee with smart ID because you go in through the bank so you could almost do just about everything with smart ideas. Well, and this is another thing as we're sitting here talking about an ID card....Actually, I would not suggest an ID card for your country or my country at all. I would say let's go to the next level. Why the hell are we talking about a plastic card when I have this that lives with me all the time. And this is my token to log in securely if I want to use it through sim-based with mobile ID if I want to use Smart ID. Are you familiar with smart ID?

AH: Yeah. I'm familiar.

B: So if you want to use Smart ID and in there are lots of companies that are doing that. So make this a token. This is now the way you log into things and and you might be able to sell that to people. Hmm But do you then have to make it optional rather than compulsory? Yes, but when you make it optional, but you give them pain, so if you don't have it, you're not you're not at maybe they can't access Services.

AH: Well, this is the one of the things that I've heard (from Estonians) that it's just problematic in Finland where they've tried to introduce some of the similar Services because it's rather than being mandatory. It's optional right there just haven't had the level of uptake that they really need and because the uptake hasn't been as high therefore the services haven't developed from is that yeah.

B: Yeah. Yeah. So I mean I think in in and it's wrong for you to just have an online service. You have to have a parallel parallel service. I mean even in Estonia you still have offices you don't have as many and if somebody needs to file something via paper, then they have to work a little harder for it, but you know.

I mean this this would be you know some options. Okay. Sure, you can still fill out whatever on paper you can still do this. You can still do that or you can you know, one thing that the Transportation Administration did here in Estonian is that if you were to when you sell a car or buy a car, you have to change the registration, right? So it's the transfer has to be made if you do the transfer online you get a like 5% discount or 10% discount for doing so right versus going to the office where they have overhead. So you're going to have to pay more and so yeah, you have parallel Services same with with voting you can still vote on paper. You can still vote by mail. You can still vote for people who have really, you know, serious disabilities. They'll send someone from the polling station to your home here because they really want to infringe eyes people which is fantastic. Yeah.

AH: Um, but anyway, so yeah, I mean if Estonia can skip paper checks.

B: Well, I still get given one by my I've never written the check ever. They still give us them. I've never written one. Yeah, every step. I still have a handful of people of companies back home in the u.s. That I have to send a check to really I mean that that basically non-existent in the UK. I vaguely remember them when I was you know, I'm gonna go back like it nine years. I vaguely remember them but only guy ever personally wrote one because I would have always had a chip and pin. So yeah, it's always been completely redundant but

But I love the fact that Estonian never did it. They just went straight to wire transfers. Why not? Yeah, I've always wondered that they are always very eager to implement these things and there doesn't seem to be the same stigma of failure here. Now if a public service goes wrong in the UK, you're gonna get crucified for it. Whereas if it goes wrong here. I can't quite if that's a cultural thing. I don't know whether it comes back to the Nordic thing in terms of the government, which is another interesting too because I'm not sure do we Class 2 onions as Nordic?

Well, I'm not saying that they are Nordic I'm saying that they use that view. Oh, yeah, I mean so I certainly agree with you because it doesn't mirror a lot of the Nordic countries, but then actually if you look at them politically they're not really no politically they're still really conservative right but but in regards to technology and again that may go back to to history, you know Estonia was one of the one of the leading Tech hubs for the Soviet Union. Yeah. So you had all the you had all the computer scientist here you had this was where you know this sort of Technology Innovation was going on during Soviet times. So you had a lot of like-minded people. Yeah. I'm not selling things I've heard is that they have the people that you didn't have the body. But yeah, there's another money and they didn't have the you know the actual

Hard work but I think that you know, as far as no, I mean, you know, socially they're much more conservative than the nordics but when it comes to technology in the uptake of technology and the and the utilisation of technology, I think I think generally the majority are you know at that level even and I say that knowing very well that I'm a I have to go at the end of May to speak in Norway for the second time because they want to hear about Estonian Innovation because they feel like they're behind Estonia in Norway. Yeah Sweden feels like they're behind you know, British. never mind this stone age stuff that you know! Whatever it is in the UK was in the news, the way they vote in Parliament?

AH: Yeah, I mean our MP's have to line up and it takes hours upon hours of time for them to vote. It's like a ceremonial thing. They have to line up one by one and go through whether going to cast their vote whenever they have a vote in Parliament. They won't even use a digital system to do that even.

B: It really is. so this is and this goes back to political will... Alex you will make my heart happy if you please discuss the political will because this is once I finally say this in a group of people from the UK or the US and it's sort of chal-

lenges them a little bit. Do you have the political will to take a step? Fast forward and create a system for the future Generations. Not the damn baby boomers.....Oh, I know but hey, I did meet Boris Johnson when he came to Estonia.

AH: How was that?

B: Actually? No, I I kind of stood off the side and took pictures my boss and and and the head of marketing or actually shaking his hand and I was taking pictures I said no. Thanks you guys keeping fast on that one, but he was I mean he was okay speaking wise can comparatively to Trump. I mean he's at least educated whether or not he uses it is another matter... didn't he go to Oxford?

AH: Yeah and Eton... I'm not a fan

B: Yeah, me either

AH: Yeah. Anyway, let's talk about cyber security. Well it really what so what I'm going to skip a few questions as we've naturally covered quite a lot of what I ask anyway here... but one of the other things I ask here is in terms of society security awareness thinking about like, you know, everyday cyber hygiene.... so you have noticed when I answered the call that my screen was black because I've got one of those camera covers. Do you use one of those as well as well?

B: Yeah, I use the more temporary version The Band-aid that's you know, you'll keep it old-school. So yeah, when when I found out that President Ilves covered his video his webcam I covered my webcam as well. Now. This is my work computer. So I do not I did not put anything permanent, but I do have like I have the filter the screen filter so somebody's sitting beside me. They can't look and see what's on my screen from the side if they're sitting behind me they can but I purposefully don't use my work laptop or log into work when I'm in a public place where people can sit behind me. So because I work where I work this has raised my level of personal cyber awareness, so but prior to that prior to working there. Yes. I had I had covered my webcam. I use vpns. I wasn't on social media for a while but I am on social media now. I'm some for some reason I need it for work and I needed it some for school. But yeah, I mean I try to I try to do those things that.... that I'm supposed to do right?

AH: So do you mainly do that because of work?

B: Yeah. Especially the screen filter. I didn't have one on my personal. I don't still have one on my personal laptop. I don't know that I would go to that extreme, but actually after after one year of studying more about cyber security and and how vulnerable we are how we are the weakest link sort of so to speak. I did try to step up my game. Yeah looks the same. So I was actually given I've got one of the the semi-permanent so you can't see it because we're doing this of Escape its like a sliding thing and it yes it Clips on It looks a bit more smart than a Band-Aid. But yeah, I was gonna say if that's really fancy. I got one. We were at Mobile World Congress last week and I some it was a giveaway from some company they were giving away. So I got a couple of them and I was taking them back to my kids.

AH: So you pass on cyber security knowledge as well?

B: They've been a little more advanced than I am about those sorts of things. Let me qualify that my kids are twenty six an

AH: That's generous of you... I'm 30, but yeah,

B: So they they were doing pretty well in general but I think no I don't know that I've actually taught them anything. They used to give me crap for covering my webcam and I'm like, "hey look the President of Estonia does it, he knows, so I'm doing it". But yeah there they do understand as most of the Millennials do I think.

AH: So you think that millennials are generally more cyber security aware... So the other device i have is a micblocker, which you plug into your microphone slot as well. So your headphones slop and it mimics there being a microphone inserted. *shows example* So it makes it think that there's a set of headphones with a microphone in the stopping any sound go ahead. Is that something you use?

B: Now. It's interesting that so many people have these camera covers yet. So I take it you don't have one of those devices either now, I don't and I you know, I've I've also heard that the Governance Academy gave away what they called their cyber security kit and it was a Band-Aid and a piece of chewing gum. So you could put a piece of chewing gum over your over your microphone to try to muffle the sound. I mean, yeah, it would work if I cover it with my finger you can't hear me. So I think that that's probably not too far from I mean if you really in a pinch, but no, I don't have one of those I don't I haven't gone that far. But I also don't deal with a lot of really sensitive information or sensitive data, right? You know, if somebody were to hack into my my computer, they would mostly hear me watching YouTube videos and and Netflix binge watching. So yeah, I mean to be honest, there's no value in the hacking into my computer either but with I personally feel about other than maybe they want to steal my thesis but I didn't like it's not exciting to be totally honest, but I would be more bothered about my voice being recorded constantly than someone having a visual of my face looking at a screen which is but I've got bad news for you because we're on Skype right now which runs through the United States which then runs through the NSA and I'm also American so I'm sorry you were probably being recorded....Hey guys! Yeah, I mean I always joke, I'm probably on a list but no, I you know, I live I live in a foreign country and I do send emails through the United States to get routed through United States and I use social media to get surrounded the united through the United States. So probably the NSA has you know, they do collect all that data what they're going to do with the terabytes and terabytes of data is good question. Yeah, especially a lot of it will be frankly did it are conversations that exactly exactly so but anyway another question on actually so do you use anything? So for example to use WhatsApp do use encrypted messenger services on your form? Yes. So I use WhatsApp. I use Viber which is double end encrypted now. Yeah, instead of sending messages when at all possible. Yeah, I mean well that actually is a less of a function of cyber security more function of cost. It's so expensive to send text messages back and forth to the US. So I use other other options the fact that there is end-to-end encryption on those on those things that that that makes me feel a little bit better. Hmm. Yeah originally when I go what's up, I got it because it was at the time I think when it still cost money to send pictures. I mean, I think it maybe does now but it's included most contract even you know, internally, but now I still use that instead of any other messaging service, even though I haven't any form which is of course encrypted, but after all I still prefer to use WhatsApp because of that.

Yeah. Yeah. I'm with you and again that was something I learned here that you know if you want to take a device and and give it a little more and protect your messaging then you need to use you need to use a some some message service that it has encryption. So so I thought is something you use as well. So, I mean one of the other questions I sort of had. We've touched upon it a little anywhere in terms of security precautions with your smart card. So obviously I would discuss the double end encryption there and the process so I'm thinking specifically now bank cards now. I don't know if you bank with an American bank or was an Estonian bank and what sort of Technologies involved as I know that in the state's you still you do have chip-and-pin by large. Do you not? Yes still there's some so there's a couple things I have an Estonian bank account and I was able to get that in 2014 now it's much much harder for u.s. Citizens to get bank accounts in Europe and in UK due to the IRS no one wants to deal with our tax Authority but beyond that I still have an American bank account as well. And in order to login to my remote banking, it's just username and password. There's actually not even two-factor authentication on that. However, if they notice I'm from a different IP, then they will require a second like a cut special code that they'll email me or text message me and then I have to put that code in but that's only if they don't recognise the IP that I'm that I'm currently using. Yes. My bank card does now have a chip in it. Most of the point-of-sale resellers in the United States now have gone to a chip reader, but some still don't so you have the technology.

AH: The next thing I was going to ask regarding bank cards. And so if you do have an Estonian when you might have it, do you have contactless payments?

B: No, I did not enable that where you can just touch it and go. Yeah, I didn't do that one in and you know, maybe it's because I'm just still a little weary of this technology. I don't know. Um, but no, I don't have that enabled. I just I still have to put my pin in physically when I go places, so I opted out of having that. And I don't know why I mean I see that I see the benefit of just being able to do it. I see my friends do it but this is this is not a step that I guess I still feel like I need a little control. And again, I'm also older so that may be part of it.

AH: I'm quite interested in these little devices that you can get that sort of makes sense of security. Have you ever seen those RFID blocker wallets or sleeves for cards?

B: Yes, I have a purse and you have one I own a purse now I own this purse. Well, actually I want to I bought one and then I my mother-in-law gave me one for Christmas this year and however, I don't carry it. So I have one but I don't

use it. So that was fashioned over function at that point. So I think if I were to go to if there was a country that I was little more suspicious about I might actually take it but coming back and forth to Estonia. I'm not so worried as much yeah. Maybe if I were in maybe if I went to Russia, then I might be a little more inclined to take that. I mean, I've just I've been told like seriously lock everything down. If you go to some of these countries

AH: I'm actually going to Saint Petersburg this weekend...

B: So but I think I think more importantly it's your cell phone. So be careful about logging into any free Wi-Fi use used for G. If you can it dips below 4G don't use it just turn that off and I was told to turn off to deactivate my USM for sure. Hmm, so Because it was there I guess holes in that if that could that could enable my phone to do things that I don't want to do. So anyway, so so you would come to your SLI just turn your phone off or dead so I consciously turned my I turned that sim off I turn data roaming off and and just sort of did with out for a little while until I until I got back into an area where there was 4G far enough. I may be a you know, making me think about it. Whereas I I wouldn't have previously done that's that's really interesting that you would consciously think about where you're going to use that dependent on how you perceive the threat in that area.

AH: Well, i doubt i'll use my phone too much anyway...! But good to know

B: That's good. Enjoy your weekend! We have such a heavy conversation... Do you have to transcribe all of this?

AH: Ha yes...

B: I apologise! Well, no, it's absolutely fine. It's gone a little off the questions, but most of it is relevant, so that's fine. These are meant to be semi-structured anyway, it's okay!

B: Sorry, I'll keep focused focused! But you've brought up an interesting point about phone security... that I haven't actually thought of there in terms of phone security soon. It's legit. It just went a little bit. All right after you know, I'm trying to keep an eye on what I haven't asked you to do because we've wandered a little bit... but you mentioned before there's probably some IoT there. I mean not everybody is secure is as is as secure as they should be in regards to devices. So I'm sure they're still dealing with open ports around printers and you know connected items thermostats, you know, smart home things. I think this is where we're all still learning and lagging. Yeah, keeping up with those sorts of things personally, you know for

Anyway, so I think I think you know from a public perspective from if you look at the public sector, I think the public sector is trying to stay ahead cryptographically to protect citizens data as best. They can I think at the personal level, you know, people are still responsible and they click on links that they're not supposed to and I think we're all we could all be subject to fishing. Yeah and spearfishing. You know, we see something that looks legitimate it comes from somebody legitimate and we got oh, yeah. Sure did it now do I wouldn't personally give my bank details and I don't I don't know that it's Tony ins would either but you know, I think that percentage is quite low in Estonia comparative-ly, but I don't know those numbers right off hand, but I would like to

They did they probably fall for some of those a little less than we do in the US but they're also a smaller population. So I don't know. Yeah, who knows but so I still think that the the perceived threats even here in Estonia would probably be the same things that you would that I think plague everyone at the moment which are you know, things like spearfishing campaigns crypto of malware that you know that you just don't see hmm. No, that's interesting because not you my follow-up question was going to be key threats to your own personal cyber security. And obviously we've talked about a couple of those things naturally anywhere so that they have an interrelation for you then. Yeah. I can't say that. I can't say that.

break in the interview - CL has to take a quick phone call

AH: We talked about what makes Estonia unique and the link with National Security. I mean actually, this is the final question. I mean we have talked for a while anyway, but the final one I always tied up with is do you think that citizens do have a role or a responsibility in ensuring cyber security whether that's their own cyber security but also a wider idea of National Security.

B: Well, I think... I think everyone does yes in this day and age... I think citizens do have a responsibility to be mindful of what they're saying and what they are doing online as we have moved into this weird era of fake news and of disinformation campaigns, we are getting more desensitised to these things, and I but we but we have to go but we need to stay on guard. So and I think that's at the personal level and but also I think that our leaders need to be they need to try to be more educated. You know, we're Beyond we're beyond the conversation where you know, the internet is a you know, a connective, you know tubes the inner tubes are all connected, you know, we should we should have moved beyond that but we still have leaders that still don't understand the basic concepts.

AH: Yeah, the Home Secretary in the UK last year discussing cyber security made a comments about needing the necessary hashtags....

Yeah, I know so this so you would hope that as we look at the Millennials who are more more cyber Savvy, I would say you would hope that that that would go up but when we still have leaders that are of the generation that you know, that didn't grow up as digital natives. They are, you know, they are a part of that sort of, you know generation where they didn't grow up with those things and that has been a problem. So because they're still creating the laws..... I was excited when Obama got elected because Obama did hire a bunch of Millennials. He put together cyber security strategy. He hired a CIO and he hired a technology advisor in the White House and in his administration and these were positive steps towards getting ahead of some of these things but sadly when administration's change, it's the same in the UK then some of that knowledge leaves. So every time they take their eye off that ball something happens and sadly until it starts costing people money. They're not going to pay attention. So you if you look at so from a governmental standpoint, they need to they need to look at cyber security as a threat to all security from a business. Perspective The Business Leaders and Industry needs to start, you know taking responsibility. You look at GDP are this may be one way where they have to take responsibility for personal data at least at the minimum. And then from the citizen standpoint and Civil Society. You people just in general need to be more Mindful and and careful.

Participant C - 14.2.18

AH: *explains premise of project* What does cyber security mean to you?

C: *laughs*

AH: Appreciate it's an open question, but that's intentional really, as it is interesting where people take their answers

C: Do you mean on a personal level?

AH: Well actually, that was going to be a follow up question, so perhaps you could suggest your general thoughts and then what it means on a personal level... if you feel there is a differentiation?

C: I think it could be generally categorised as 'cyber hygiene'... so you know, following best practice. Things like knowing to use private browsing features to ensure you don't leave your password lying around... replacing default pins also, for instance also.... taking care of the small vulnerabilities that i am able to manage. If someone likes to sync devices... making sure you don't leave your devices insecure with passwords, locking your computer as you walk away from your work station... things that are easy to follow, and also quite efficient. They prevent lots of very simple attacks. So more complicated attacks on the other hand... against me, lets say, by large companies... state actors... google has access to my email anyway for example, so i don't need to hide it. If i need to do that, i'll use encryption... for this i use either the encryption function of the ID card, or some EGP encryption, or stuff like that, if i would need that. The problem with this, is the risk assessment for this type of threat is non-trivial. So.... people in Estonia for example, we have these sort of awareness campaigns, so there's state information agencies that try to target the population, to make them aware of how to treat your personal data with care... what to, or not to do on public networks... so if a member of the public or a business comes to us and asks what to do, the state has provided encryption facilities within the ID card. You can use my ID card to send private messages. Perhaps you are aware last year we had some issues with these cards?

AH: Yes

C: Yes, it was down to an optimisation measure, taken by the hardware of the ID card. It was pointed out by some Czech researchers. One of the unfortunate side effects is the encrypted files, which were attached to the vulnerable cards, are also now vulnerable still. So this was an oversight. The unknown vulnerability in these cards was not a part of our everyday risk assessment.

AH: So does this does play into the trust aspect, and how much you can trust the software or the technology you are provided with?

C: Yes, and what assumptions you can make. We also see that these trust relations are not static also. The government trusted the manufacturers of the hardware back then, then the citizen trusted the government, but then again it turns out this trust chain doesn't really give the security it would like.

AH: So, on that note, what measures do you take personally to ensure your own cyber security?

C: Yeah, i listed a couple of them already... but yeah, again, one of the measures, if this ID card or mobile ID... so it allows you to get rid of things like bus cards... it provides you with a notification mechanism... the thing is, it's less trivial for a service provider to set up. So Estonian service providers have done this, but the rest of the world... is behind.

C: Other measures... so things like private browsing, following company policy with things like laptops, as this is best practice... again, this doesn't prevent all the personal attacks, it doesn't prevent attackers accessing you remotely.... but it does prevent basic threats like someone stealing your laptop and trying to access it

AH: Do you take any security measures with your smart devices, beyond the basic things let setting complex passwords and so on?

C: Um, yes. For instance, I do not use remote access software to access my company network from the smart phone. it's possible, we can install a VPN client to do it... but i feel phones are more prone to theft, for example, and i won't risk the company network being compromised for this convenience. Also, for instance, for private communications, i and my colleagues use 'signal' if we need to have a private conversation. We're not using standard phone messaging, we choose a safer, encrypted messenger instead.

AH: Do you, for instance, use a camera cover on your computer and smart devices?

C: No, I haven't.

AH: Would you ever consider using one, or do you not believe it is a risk?

C: Not particularly... for example, if i am concerned about something sensitive, it is on my screen, rather than on my person... i recognise that this can be a concern for some people. Perhaps elite-level, state actors, but for me personally, i don't consider it an issue

AH: How about a mic blocker?

C: I don't believe they work, there would be a workaround for this, as it happens on a software level. But yes, what can be heard is more sensitive than just seeing someones face. Again at a state-level, i see why this is more of an issue.

AH: Do you take any precautions with your smart cards at all? So with your ID card, your bank cards... do you for instance, use an RFID blocker?

C: So, i don't have a blocker. But i do have concerns about the security of some RFID technology. So if i can't turn the RFID off... i have disabled payments from the banks side. So i choose not to use contactless.

AH: Why did you choose to do this?

C: A lack of trust. The reason was, well.... part of what i am doing at [REDACTED] is writing regular recommendations for the government concerning cryptographic applications. So these are available online... one of the topics we looked at were NFC protocols. There are various kinds of them, one could be accessed quite easily... for example, public transportation cards. There are thousands of them out there, they could be attacked with ease as the protocols are not so secure. Ok, so if someone attacks these, they could get a free ride on transport here, but not much beyond that. But nevertheless, i know the older generation of oyster cards were the same.... so we looked at these cards, and these protocols are very similar, and are easily clonable, and also easily blocked. So a simple enough device, you could overwrite these cards with random garbage... these sorts of things.

AH: And you noticed some similarities in the technology used with these travel cards and contactless bank cards?

C: So we started looking into these, in a report for the government... and i could not find the protocols involved. So i actually went to the bank, and they referred me to a white paper that didn't contain anything interesting... so i went back to the bank, and spoke to the girl behind the counter, asking about the cryptographic details *laughs* she looked blankly at me, called somewhere.... they said they'd get back to me. I received an email, i asked what i wanted, and i never got a reply. So there was a presentation about some of the details of apple and android pay at a recent conference... that still did not touch the payment cards. So i still don't use this.

Brief discussion of contactless payments using Apple pay, and how it functions - JW agrees this is more secure as it uses a separate cryptographic process, even though the payment is taken from the same card, however it is not available in Estonia at this time

C: The reason i generally don't want to use this is lack of transparency. It's not clear to me as a cryptographer... so what exactly are they using there?

AH: So to bring things back to the wider Estonian context, if i can, what do you consider the key threats to Estonian cyber security are?

C: As a society... a country?

AH: Yes

C: Well... obviously, a large scale cyber attack is a threat. We've gone through that, as you know, around ten years ago. There was a cyber war. This is one of the reasons the state-level responses began, as well as all these awareness campaigns and things like that. It didn't kill us, it made us stronger. So that's a good thing, but it still remains the key threat in the future.

AH: Do you think this relates to your e-governance systems then, and Estonia is more of a target because of this?

C: No, no. Not necessarily. If someone decides to do something, i don't think we are that special, but if they would like to attack us... the Russians... or the Chinese or whatever. They'd probably still go for a denial of service attack, for disruption reasons. You can't really prevent this fully anyway. Of course if they start firing at you, then that's very different, but in terms of cyber threats, denial of service will be key, and you can't do much about it. We've also seen different types of threats too, occurring more and more, are open manipulation attacks using social media, paid content in Russian-speaking media for instance... this has become pretty big recently. So the Russians are very good at using propaganda. Some people call them political campaigns, others call them brainwashing...

AH: *laughs* and you would call it brainwashing?

C: I think there's a fine line between this and informing people. These things become more important next year when we have another election, when politicians make a bigger deal of it. There is also different channels involved now, so social media adds another dimension to this. Is this what you would call cyber war... or an attack... there are many definitions. These things have the potential to influence the population, which in turn has an influence on our international relations with other states. So it is a threat. Also, you also have this threat of global surveillance. Whether from countries, or from companies such as Google, Facebook, Amazon... they profile you... want to know many things about you... they're selling your data to god knows who, and they're ok to do so, because you've given them permission to do so

AH: Although it is an issue a lot of people don't fully read these permissions, or are not aware of them?

C: Yes, absolutely. You probably didn't read it.

AH: Would you say that is a personal cyber security concern?

C: This is tricky. So there is a personal security aspect, because you sign this and you agree to it... but also, these things are written in long winded, legal mumbo jumbo, which prevents most people from actually reading them... people never read it because they care about the service. They want their Gmail account... they need to use facebook... so they don't really have a choice, because a lot of these things are virtually essential now... and if you don't agree to the terms, you don't get the service. So this is an ongoing legal debate in all of Europe right now. So if a very large service provider, whose service isn't really optional... if i don't feel easy with the terms and conditions... how do we do something about it? I think an alliance of states, like the EU for example, should do something about this.

AH: So you feel stronger regulation will be key?

C: Yes, so we will be getting GDPR in a couple of months... which is a move in the right direction

C: But yes, you were talking about if this was a personal or a private issue? Well one can be elevated to the other sometimes, I think. So there is a possibility that data collection can start off on a quite small level, but then gradually over time, so much has been gathered it then represents a threat to citizens. So there is a definite link between personal cyber security and national cyber security, it just may not be immediately obvious

AH: Could you possibly describe the approach of Estonia to cyber security? Do you think there is something unique about it?

C: Well.... one unique thing was the aforementioned cyber war of ten years ago... it has been happening time and time again since then. So it happened to Georgia shortly afterwards too. There are some unique services of course... the e-voting... we are still the only ones doing that. There are probably some other things... the e-residency...

AH: You're not convinced by the e-residency?

C: Not entirely

AH: It seems a little gimmicky to me

C: Yes, it's political as much as practical. It does provide access to some services of course, the x-road I'm sure you've heard of...

AH: Yes, which was developed by cybernetica, right?

C: Yes, and still is

AH: So do you think the use of digital identities makes Estonian citizens, generally, feel more secure? I know this is a large question to speak for everyone...

C: So i think actually, for the vast majority of Estonians, it is the services people care about. The state has provided a service which is secure, but security is not citizens primary concern. If you talk to most people... the average person on the street... they perhaps don't think about the security so much

AH: Can i ask, regarding your work, do you consult clients regarding security concerns? If so, what sort of issues do you come across?

C: One of the things I often come across... well i work as a consultant for the state also, so they are of course a major customer. So we are interested in the cryptographic security of applications, for digital services, in this regard. I have also done consultancy work for private companies. We have close collaboration with Swedbank... we have also done work developing internet voting solutions and securing them, every once in a while, small companies approach us to look at security protocol around a product they have designed... or with specific devices, and how they could be more secure

C: Typically we have an end customer who is having a product designed for them, and they want the process monitoring. The idea that this end device needs some kind of protection, whether it is through encryption or whatever.

AH: Is this re-assuring that companies are doing this, as one of the primary concerns particularly around the IoT is that they don't check these things?

C: Yes *laughs* it is perhaps the companies that don't do this that we should be worried about. I am very much concerned that overwhelmingly this is the case... and I'm afraid that the companies that do reach us are the tip of the iceberg. That some places don't even know some devices represent a cyber security threat, many of them are building the solution without actually stopping to think about the threat... and likewise, customers aren't aware these devices can be providing an open access source to threats...

AH: Do you think the concerns of citizens here relate to concerns of national security, or do you think they are disconnected?

C: I think you can ask this in any country... and you'll hear i care about my privacy... and my own security... where as the state has its own concerns, and it should stay out of mine

AH: So i noticed you mentioned a perceived Russian threat earlier in the interview, do you think the aftermath of 2007 changed things?

C: Yeah, so i don't think it's a key everyday concern really. You know sure, people think about it, but it's not a top priority. I mean, if the Russians wanted to roll over the border tomorrow, there isn't really anything we could do to stop them, so there's a kind of fatalism... we just have to accept this... I mean i can't speak for every Estonian of course, and i might not be the perfect person to ask, but to me there's a clear separation, but of course I'm much more involved with national security issues than the average citizen would be, so my answer will be biased...

AH: Yes, obviously this is different to what I would get if i were to stop people in the street

C: Yes, so if you were to do that, i think you would also receive a set of answers biased by what they have heard reported in the media... so for instance, the ID card received a lot of attention, so people will remember this. Similarly, internet voting... this receives a lot of attention a few months before every election... so you get a contrast of opinions... it can't ever be secure.... other people trust the government provide it.... very few will tell you the technology behind it, and how they know it is secure because of the encryption and the decryption process involved... i mean, you're talking 0.01% of the population will be particularly familiar with this. So it comes down to trust. So there was a study conducted by social scientists at Tartu a few years ago now, which found that even though people did not fully trust internet voting, they still used it.

AH: Yes, it was a guy called Krisjan Vassil, right? We've met before

C: Yes exactly. It's an interesting insight into attitudes.

AH: Yeah absolutely, and the trust is key, rather than the technology itself.

C: Yes

AH: So the final question i always ask, baring in mind she of the explanation of the goals of my project and also in line with cyber security policy goals, do you think the citizen has a role and a responsibility in ensuring cyber security? Not only their own, but also at a state-level.

C: Absolutely.... well... far more, they should take care of their personal security.... national.... there are probably things a citizen can't do for national security.... but there are definitely things they can do, and they should do what they can. So once or twice a year, for example.... this now goes back to the Russian neighbourhood. We are in the sphere of influence... or shall we say interest of Russian secret services. So once a year or so there is some kind of incident... so it's definitely the case that the Russians are trying to fish around here. So.... one thing that definitely should happen, is citizens should support incidents, and i hope they do. But again, these are openly targeting people, causing a national scale problem. To citizens, these might look like phishing emails... or weird services that contact them and ask for seemingly harmless information... but there are sorts of information which help you draw conclusions about people. So these are the sort of things... I'm not quite sure how you handle, or classify them. If someone asks for your password... or to become a Russian spy... sure these should raise the alarm... but it can be much more simple questions... like when you last visited St Petersburg? So looking for your contacts... so I'm not really sure how to handle this, and it's a point of contemplation for security services of all countries.

Participant D - 20.3.2018

AH: *Introduces project in brief*

Anyway, so I'll stop talking now and ask you a few questions if that's all right. So, I mean the first one super open, but what does cyber security mean to you?

D: cyber security is having control of access to my files and to my services on an individual level and so and on a national level, of course to be able to ensure an orderly working of the data exchange networks available in the country.

AH: Perfect. And so do you take any specific measures to ensure your own cyber security?

D: I run a firewall on my on my laptop computer, and here. I mean, of course, we're in the private Network... some more or less. I trust also the institutional cyber security awareness, right so I don't have any major of my own infrastructure.... also because I'm not allowed right... but at home, I have my own private firewall and BPM, excess and these elements. I try not to use the open free Wi-Fi. So I am of course I use a Mac which makes me less prone to it, but I still have the same security measures as I have my mobile PC.

AH: So for example, you're slightly wary of using public Wi-Fi networks? Would you enable a VPN if you were to connect to a public Wi-Fi?

D: Not for regular browsing, but I mean for as soon as they do anything secured critical like banking or any other digital signatures that I use a VPN on top of that and I have like a paid subscription VPN, and I have my own VPN server.... and of course the university I vpns... I have a selection of tools and protocols available. Maybe it's a little different with my phone

AH: on the subject of subjective security with your devices... Do you use a camera cover for instance?

D: *shakes head*

AH: Why do you choose not to?

D: I just don't feel it's important or I mean, yes, of course, it's a it's one of those things you could do with you know, it's some place you got to stop.

AH: Yeah. I mean, I must admit to be honest... I was given mine at a conference.

D: Of course,. It was the one that was in tartu... (pointing at branded cover) Yeah. These area good idea to networking right but I think it's yeah, it's kind of like an identity thing

AH: Do you use a mic blocker?

D: No, again. It's not a concern for me

AH: Do you take any precautions with your smart cards? For example, so to use an RFID blocker or is it something you would consider using?

D: No, I mean I have one for my my critical points and that was a conscious decision because you didn't you felt that there was a potential security weakness. Well, it's because of security.... I don't know. What's the limit right now for my credit card for the contactless on there... But yeah, I mean for those cases right? So basically just the occasional not to make it too easy for people.

AH: Yeah, absolutely. So do you use contactless payments at all?

D: I mean, Estonia's way behind with contactless payments.... and when I lived in Poland which was 2010 to 2014, they were common. Estonia is still not quite there, surprisingly. So I was using that there, here it is infrequent, and

then it doesn't work ... and they don't maintain it and whatever, so I don't I hardly ever do ,but you don't have an issue like a security issue with using it.

For example, let's change the abyss using credit cards ten years ago. I need also use the back then. So I mean in the end the same security problems exist, right immediate transfer your credit card number unencrypted and whatnot unencrypted... it's very easily accessible. And so I monitor my transaction. There is a transaction problem. Then I just cancel it and switch the number. Yeah.

AH: You've not considered disabling it?

D: Yeah again, I mean I do I take a certain level of risk when it comes to I mean... I don't... I don't... it stops for me where it impacts my convenience, right? So that's and of course that's for most people but I'm at least aware.... and I know where need to check... and so I have been I had once an issue with a credit card that apparently was copied. Hmm But then I had a positive experience how that was resolved. So I don't really feel it to be a real threat to me.

AH: Mmm. So, I mean for example, if the limit was extended to be much higher on those contactless payments, would it concern you that reacts at the moment? I believe it's in 20 Euro.

D: Basically, it comes down to the banks... any claims that come out of that but basically based on their risk model, they just accept anything that you basically appeal against that your that your reimbursement, right? So based on that experience. I don't really care and probably should have put it that I mean you should be more aware... but I mean if I take my own risk mitigation... then yeah... for the convenience that has that trade-off. So I think I'm in control. I mean again experience tells me that we all act quite irrationally when it comes to a convenient. Yeah. Absolutely. If you make something easier people will go for it. Sure if I could ask a couple of things about Estonia more generally if that's okay.

AH: What do you think the key threats to cyber security in Estonia are? obviously I've been focusing very much on a personal level there. But nationally do you think those concerns are very different to key threats to your personal cyber security?

D: I would see the the way that cyber threats in Estonia and handled shows very clearly at margins of the country. So it is a small country. It has limited number of access points coming into the country and going out of the country. So there is at least the possibility to control, right? So Estonia has at least the option to switch off the international part of the internet, obviously, then it would only be National Services and that's what happened in 2007 because of their close context because of the limited size of the country the easy administrative level or hierarchies that are involved. So there is a particular situation that makes Estonia not comparable to anything. So that said, I would say Estonia is taking managing the security issues quite well. All right, it has close collaboration. It is able to assess established quite effective response mechanisms to to any threats that are coming out there on the Cyber level. They don't distinguish between a military threat versus attacks from criminals or whatever. So they just tried to treat all of them equally, and once they have identified what kind of attack has happened they tackle the response, and they have the units that necessary to do so, So that's the particular situation of Estonia. The second thing is of course that this is being used to position a country overall internationally using the NATO competence Centre and to also Transfer knowledge, but in the end the problem is that the situation that we have in Estonia is too simplistic to be easily transferred, right? Yeah.... of course because it's a very specific it's do you think of them being a small country is integral. Well, it's a very flatly administered country. So basically the hierarchical structures in Estonia are very, very, very low... and I mean we have we have the local level and at the national level and that's it, right. There are no regions. There are no big cultural clashes other than the Russian-speaking divide, and that has been overcome in the administration more or less. And and so that's that's just too easy. Right? I mean if you had Belgium already the has this Duality between French and between and Flemish, and there is much more complication there and then the different levels that regions, and you know or Germany, I mean where there is everything is totally decentralised as a way of of protecting you against any too powerful leader, right

AH: right

D: all of that context so you cannot take that in one way or the other... So Estonia has been a country that was established at a time when the internet networks were on the rise. It made the lucky choice not to go into institutional and into commercial Solutions, but rather select open low-fee applications that allow them to keep their maintenance constant and IT cost relatively low, and mainly deal with that on a... on a human resource level and to build that competence inside the country... and through that they have maintained or it was more a Darwinian approach that basically... it happened that Estonia had the best effective answers to the Information Society challenges compared to any other country. So I wouldn't say it's the particular achievement, it just evolved naturally...

That level of it sophistication.... both in the public and private... But rather an element that it happened the.... the exact right contextual environment to be able to develop such a society man. And of course also making the right choice in that mainly has to do with the fact of this be affirmative causation, right? So basically they do something they really only got positive feedback through media.... and that became very important to position the country on the map. And so it was it was a really a very formative pattern that emerged we do something we get positive recognition.... We keep doing more, and we're getting more positive recognition... and that goes in so far that they just put out statements like maybe we introduce an electronic coin and then everybody copies around the world. It's like branding it the next block blockchain Nation or Bitcoin Nation, whatever, and it basically goes to that level.... Many projects are legitimised by just the pr effort it brings to the country. And that's one of the downsides of this... but taking all of that in there Estonia is a special case. Hmm. Yeah and most egregious... very slickly marketed as well. So if you visit Tallinn and I'm sure you visited the showroom (e-Estonia)?

AH: Yeah

D: Yeah, so you'll know that the dissenters are very marginalised, and the entire brand of the country is center-right basically ... So because of the limited size of people that are working in that field you already know which narrative comes from where yeah, right.... So you really know. Okay, so they have been to the showroom before. Okay. That means that I've got that spin. Okay, then the enough that okay, then they meet the people in the in the ministry of economics and communication. Okay, so that means they have this picture now as well. Okay. So let's let's bridge this now with their UK perspective with the perspective here and then see where we take some it. It's very very transparent. Let's put it that way.

AH: Hmm. It's interesting. You should make a point of transparency then. So do you believe that this the whole system of e-governance particularly Easy Digital identities. Do you think this makes a Estonian citizens feel more secure and make them more prepared to trust their government?

D: I think the Estonians do have less reason to distrust their administration... in part because they have the feeling that this is now their country... and if not to us, whom else shall we trust? So if we don't trust ourselves... well, we've got big of this big brother, Russia, right? and he's not always been the best brother... So we build our own country, and we trust the technology... we just build it so if someone abuses that technology, we can catch the guy who did the bad stuff!

AH: So I do note for example, there's been a couple of reasonably high profile case where people have been punished for breaking the data protection laws here.

D: Yeah, but because it's been dealt with quite publicly that's actually enhanced public trust rather than undermined it. Yeah, but I mean, it's also possible to I mean the reason why they can deal it so publicly as because they're they're in control of the narrative, right? Hmm. So I mean take the case of the of the ID card failure.... Basically what they the the situation emerge basic on a Friday. They briefed the Prime Minister.... on the side, the Prime Minister called in all the newspaper editors in Chief on Sunday afternoon... and told them guys there is the issue. We have a problem, give us 24 hours to solve this or to a to develop an approach and you don't report about that... but basically on Tuesday afternoon at two o'clock, I will have a press conference you all will get the story and then you can write about it. It wouldn't have happened in the UK. No?

AH: No, every journalist would want to break the news of the problem first

D: Right. So basically this this National threat scenario, if you're going to release and information early on you're going to be the person that betrays their country works here very very well. And so we have a solution where every-

body contributes to the only narrative where even if people are critical.... They might still see the greater good in it. So you can control the narrative one way or the other... even though it afterwards goes a bit more. Yeah. Let's say but more conflict it right after the point. But until that point until there is a solution until their countries save everybody pulls on the same street.... So that's one of the big differences. That's why they can deal with it very publicly, because they know in the end they're in control of the narrative while in other situations in other countries, there is quite a different discourse taking place in that case.

AH: Yeah, of course. I mean, I think if that were to happen in the UK, it would have probably been a Mad Dash out of the room

D: Yeah, but here, there's like a social responsibility that you see across the board, right? So I mean nobody wants to really destroy that infrastructure and that probably is a good thing.

AH: Do you think it's a good form of patriotism?

D: Hmm, it's just unusual. And whether that would vary within the Russian - speaking community who might feel and still I mean everybody feels quite comfortable and stuff. I don't know any data that points to that.... but I would assume that this goes more or less across the board. I mean... I just from speaking to people the general consensus is the most Russians are pretty happy with the status quo the Russian - speaking community anyway, because they're pragmatic

AH: So, in your research, then you can certainly voting what common security concerns do you come across? I mean, did you consult everyday citizens or specific actors? And what concerns in Estonia?

D: There are security concerns... of course Trojan horses ...music anything that will manipulate the communication between the voter and Central service in particular the secure platform problem/// really that I mean that has been this is one of the things that I tried to tackle since 2013 when i wrote a book introduction on individual verifiability. Mmm. I don't know if you're aware of that but yes, I am awareness from the previous discussion discussion with Krisjan (Vassil) as well.

AH: Yeah, so we had this discussion one of the things that he said regarding trust and this whole process was that if you theoretically cause this is possible to do but actually in practice if you wanted to rig an election, it would be far simpler just stuff the paper ballots in secret rather than tamper with the digital system, because you can track that this has happened and he claimed that you could easily just nullify the election if this was detected

D: Yeah.... You mean just insert fake balance in the centre ... Yeah... I mean basic the problem is that you have thanks to a very strong identification mechanism meaning the ID card you you have a decentralised way and that off of maintaining credentials in the process. So you don't have really a centralised component for identity and identifying the voter because of the nature of the ID card and you need that signature to show that there was a voter involved in the election, right? So because of that you have relatively prone to about stuffing when it comes to that what you could do is basically you could replace the books that somebody has cast but adding additional ballots... It's very hard to do write the checks and balances will catch them. Yeah what you were where you you might have a solution to that is really replacing ballots. Work anymore, right? So that comes in with the university verifiable verifiability that was introduced with this election so that you can ensure the Integrity of the overall Ballot Box, right? So that's basically I'm going to would say more or less you have a lot of checks and balances in the number of of points where you have weaknesses are mainly down to the interim in the institutional hacker or basically the friendly or the internal the internal..... How do we call that now the internal hacking basically right inside Insider attack? That's probably the most likely one. Yeah, and you know, I'm not that basically then comes down to this Tony Society. I mean what would happen if somebody would really hack that for money. I mean, they will be completely. I mean, they would have to leave the country. I mean they couldn't do and find any other job. So you have this social say in how to say this punishment also in there so hanging above your head so... All I would say it's all the risk is fairly low.... because of the thing that they keep updating their algorithms to keep updating to the latest development. So they take the threats quite seriously, right? Yeah, and they are in control. That's the other thing. Right? So you would not actually say there is really much of a fear of someone from the inside. I mean, there is always there's always the one person knows too much. It's with any internet voting system. I've looked at you always find this one person that knows too much that you have trust that that person is well behaving right, but for that you have to social context in which it takes place if that will be a random person that just flown in for money, then probably I know you know that that person is a price tag if that person has a history of

bringing things to life of developing the systems the likelihood that that person goes Rogue is very small ...it's possible. But yeah,... So let's say all in all the risk is mitigated in Estonia, but risk is there it's always there. There is no hundred percent secure system, but more or less Estonia is doing what is needed to keep their internet voting secure.

AH: Yeah, that's interesting. So I'm do you think there's actually I mean, we've sort of touched upon this or if it was actually something unique to Estonia that makes them more willing to accept these systems?

D: Is there something unique to Estonia? Umm... a lack of people probably... a very sparsely populated area, the Soviet past... the threat from Russia.... but what else does the Estonian narrative have? It mainly has e-Estonia, and it's a narrative they're using very, very effectively. It's what they have, and it's what makes Estonia unique.

I mean, that's what they're trying to build. Right? Yeah, but but and then maybe the threat from Russia, but yeah, but what other elements does the Estonian it mainly has the e-Estonia narrative and that's one day using very very effectively. And so that's what makes Estonia need that you have a country that is actually branded as an 'e-Nation'. You don't find any other country that has it like that. Maybe maybe similarly you will find it with Singapore, but that also has other things to its narrative... more the cleanliness and do you properly administrated City... Yeah South Korea where you also a lot of top down and very advanced IT infrastructure... but also they have the manufacturing industry that is present in right? I mean really it is very strong IT industry and in car manufacturing too.

So Estonia really needs this narrative that what makes it so unique... theres nothing else.... and how that was developed right and that was developed just through the open source free information, right? Yeah tiger leap initiative by our Rector here... and and then the Cyber incident of course,

AH: right the Cyber attack in 2007 right?

D: Yeah. I mean that just forms this identity of the country and it's positive. Yeah, absolutely. So, I mean it almost makes you think it still needs buy into this because it sells them to the world as much as anything else. What's the most important thing for this song in that? They're that they're covered in international press. I mean not the not the only thing but base it first it's the depend on the celery's page, right? But in the end it there is an increase... there is a huge level of attention that Estonians give to their appearance in the world night. That's the most important to present. The former president is attending the world economic Forum where else would that be worthwhile of report.... right here in Estonia. It is a big thing. It's Toomas Ilves.

He's an interesting character. If something appears in a German newspaper criticising Estonia, or saying that Estonians don't even know how to do cyber security ,and then everybody goes like how dare they, do they even know us? I mean really this is a wrong statement. It was a commentary a leading German newspaper in the front of the documentary, but to that the whole country goes ... goes really like, "how dare those Germans again". They want to tell us how to do things right?

AH: I guess it goes both ways. In the British press as well. When all these errors came out because well, I mean when you sell yourself as something and then it turns out to be a little bit flawed.

D: That's the but the point is that that that's fine in the British press to do that. But I mean, why do these Estonians care that the British press is reporting negatively about them? I mean, it's totally fine and you can make one note that by the way is also noticed the wrong. I mean what else do they expect... but they made it topic for concern for Estonia. How can we correct that you can you can just fix it and accept it. I mean it is just life. Right? I mean errors happened... they are important, and what is important is that you address them, and you move forward. But this is the Narrative

AH: I mean do you think a lot of this mindset is linked to the idea of their National Security as well? I mean, obviously the experience of 2007 as well

D: Yeah. but it's very slick. Yeah, but it's also because it's possible to have a consistent narrative very quickly in Estonia because you know what, you know, the 56 people that you need to address and there is no this there is no opposing opinion that is being raised... Right and if it is then it's taken care of so I would you agree with the statement and this comes up in the National Security strategy.

AH: So do you believe individual citizens have a role and responsibility in ensuring their own, and national cyber security?

D: Yeah the individual citizen has a role in ensuring National Security and cyber security because it was two different levels there. I mean, I think generally the citizen is taking on huge responsibilities laid upon him or her to take part in public life or basically that everybody is expected to pay their their time to contribute to keeping up the Estonian State.... and that's something that for example the youth is getting now bit more critical of... I know I paid my dues now. I'm ready to leave after you've done your first job somewhere and then I want to make money now, right? So in this kind of setting and you see that more and more coming about I mean if you if you need to be our students and you do you will you will hear that right? So I'm fed up. "I don't want to I don't have any duty to the State anymore".... Right?

It's also it's part of the deal that everybody's expected contributors. I mean you have this cyber Defence league, right? Yeah, where else would that work? Right? I mean you might have an informal network of computer or network administrators that that work together.... and they volunteer to do it. How long does that continue to work?

Participants E & F - 06.04.2018

* Explanation of the background of all participants *

Thank you for agreeing to this interview, and being so generous with your time. Can i begin by asking you both; what does cyber security mean to you?

E: For me, It's understanding what can happen... what to do... what kind of threats do i have... and how I deal with them

So very much a process for you then? Do you agree?

F: Yeah, more or less... but i think for me the main topic would be data, and protecting data if we talk about cyber security... yeah, i don't know what else to add... we have lots of data we use and share.... so everything we do with it., and it's something we need to keep private and secure

So for you then, the focus is far more your own data and privacy then? As often, if you read for example, a government strategy, we are looking at the protection of critical infrastructure and the state...

F: Yeah and of course we've got to remember this data is kept on some kind of physical hardware as well, and this hardware must be kept secure as well...

So yeah, like the data embassy programme is inspired by this right?

E: Yeah

So can I ask both of you, what measures you take to ensure your own cyber security? In terms of measures... what it is that concerns you, products you use etc.

E: For me, the first thing I do is keep my identity secure. I have all my passwords with suitable complexity... and the devices are all kept in safe places... only I can access them... so the priority for me is my own identity, and to protect it from misuse by others.... second, I have a good understanding of where my data is... so i understand when i need back ups, multiple if necessary... and how to have continuity if something happens to one device... so i have things in at least three places... and i know where my back ups are, and that they're secure. This is part of my everyday life... that i put things n the right place

Do you use things like cloud?

Yeah... so I also use Flickr, which is Yahoo's service... especially for my personal pictures.... i have physical back ups at home too. So yeah, it's part server and the cloud, partly the company resources i use, and then hardware

So you keep a non networked copy of everything?

E: Yeah, although I'm not too sceptical of cloud devices... i generally trust them. I also have my laptop, my phone all speaking to each other, so it works together... so i can access things.... honestly though I think this is better than having just USB sticks lying around

Are you the same?

F: Yeah, i mean you mentioned encryption? Yeah i encrypt when possible, I locked my devices with safe passwords, so when I'm not around no one can access them... So yeah, part of the job is also knowing vulnerabilities and being aware of the threats around you. Cyber hygiene is important.

The other thing i've been wondering... I have a camera cover on my laptop. Is this something either of you use? Some people have sticking plasters... same idea though

E: No, i don't

F: It's something that you wouldn't you?

E: For me , no. I'm not really into that sort of thing. It doesn't bother me. I don't think anyone would be watching me.

F: I sort of think if someone wants to tape you... he will get his chance you know. Even if you cover your laptop or something... however, if you don't have something, it's definitely easier

So I'm guessing you don't take have a mic blocker either then? I mean, i have one, but i forget to use it most of the time, if I'm totally honest

F: Yeah, i mean i'd be more bothered by someone listening than just seeing my face

Yeah, I'm not sure people would get much from just seeing me staring at the screen... *laughs*

E: I mean, I think this might also be getting a little bit paranoid... but then it's different in different places. We have had these ID cards for 15 years now in Estonia... but in the UK, people don't really like this idea, and don't understand this

Yeah, so i have no ID card at all, we have passports and driving licences

E: Yes, it requires this trust... and I'm not so worried about what could happen. We have many services and I'm happy about that... we receive these benefits for having the card, and honestly, the card isn't a big deal... and we can see if someone misuses it... I'm more worried about... if i can't use my services... not if someone is misusing it

Can i ask *why* you trust this, and why you trust the government with this system?

E: Because it works and it rarely goes wrong

Well, i mean there was a flaw with the cards last year though? Did that not concern you?

E: Well, yes, but the way it was handled solved any concerns we had

So i've heard a lot of people emphasise the transparency and how that made a huge difference for them? Do you think this helps with the trust?

I think actually, because they were very quick to fix it as well, and they were honest, it actually helps with the trust, not make it worse

So you advised Lennart Meri when introducing these cards, could you tell me if there was any resistance to introducing these identity cards at that time?

E: So the only resistance... was that we don't have any services! So it was a useless card at first, people asked what is this for.... it took 2 or 3 years of solid services and people trusted more and more... and now we have so many. We are totally reliant on these cards. I think.... it's totally changed life now, and people have a much easier life now... i don't know how people would cope *looks at Siim* *laughs*

F: Yes, you would have to... go to places!

Yeah, I can relate to this... I've just changed the tenancy on my flat in London... well, I haven't, because they can't do it at all while I'm away. I have to go in their office and sign the paper... which is sort of difficult when I'm not back for a couple of weeks

E: This would be crazy in Estonia

AH: There's the other thing I guess so for you then so one of my other questions is always what do you think the key threats are the loss of services I'm going to guess is your main one?

E: Yes, but do you think there are any other key threats to the Cyber environment and Estonia it might happen that somebody actually crack system and misuse of authority. Are you gonna be easy to sell my house? No. But the first kind of vulnerability or loss of service impacts for my everyday life but not so much as the personal data.

AH: So I know you at the end at the beginning of the interview. The first thing you mentioned is that it's all about protecting data. Now when we say did or are we talking about personal here or are we talking about you know National level?

F: I was talking about personal and yeah, obviously National level is it might be even more important at the moment. I think that you know, because Estonia as a small country and not a lot of people living here, this might be an advantage at the moment or in some point where there might be worse or something like that. This should become a disadvantage that we always say Russia tries to hack us.... Then I would think that it wouldn't be too hard for them. I'm not sure. Yeah, I mean that sort of DDOS style of time. I hope that we are working on it that we would become better and better in these regards to prevent these kinds of attacks, but I think in pretty much every month or so there is some kind of new attempt. Yes, some kind of denial of service attack has been carried out on some Estonian information system. So this is so very big threat outside, but you don't really consider your personal data as a key. You trust the system. You trust the government with yes, I think well, I think that in in car mental Information Systems, the data is better protected and in the other likely third party information systems, at least in the governmental Information Systems, you have some kind of Places are counties in other like Cloud environments. You have some kind of General privacy policy and big which basically says that you okay in Europe to have some kind of rights to your data. But basically it says that most of the time you just give your rights to them or rise to the data to them new legislations aren't coming so which will try to somehow make this better or more understandable but the services are Protected. It's not directly government assets... as you may know that is a specification centre, which is actually giving your time stamps... And yeah, it's really still it's coming from third-party service not government service...

E: I really want to trust this sector also so it's a combination. So I mean at one of the key issues or concerns of generally come up with being what's the motivation of private sector companies. They're obviously the motivated by profit rather than by you know, people's concern them in the obviously come in because you know, if you want to maintain your customers you want a mint in trust... That's why Apple, for example have a fairly good reputation because people trust them as a company,

AH: That's a really interesting point that and I have noticed particularly here that you are very eager to work with private sector companies as well. Whereas there is possibly a slight skepticism of the mixing of public and private interests in the UK.

E: What's important is the security Frameworks that we have. If we have specific legislation to ensure that stuff our governmental commission systems and private sectors in which citizens data are well protected at audited. We established that everybody needs to apply to certain data security rules management rules. I'm combining that solid framework for 15 years. No incidents.

F: Hmm these things go together. I think it's mostly basics trust and this is costly idea of the GDP are being introduced on a europe-wide level as well that it will enhance this trust somehow ...

AH: It's very common for the UK ones that we have these contactless payments not as common here but increasingly more. So what are your feelings about these?

F: You don't have cash. Mostly they have card only now. I don't have cash in my pockets except in an emergency... - yeah, not so often or much. So yeah it's broadly trusted.

E: Yes. I trust it, you know, there is some kind of settings that you can modify to make it more secure some kind of limits and so on and I looked over the settings and yeah, it was it. However, I know that if someone would come and

put reader here and he or she could get some money from me... but there are these limits and feel comfortable with this.

...So it's like a you make it a sort of a cost-benefit analysis almost then so because they can't steal a lot of money, even if they were going to steal some you saw them you're fine with it because of the convenience that provides

AH: So I'm just thinking about the camera blocker as well... Do you have a would you ever use something like an RFID blocker so you can get sleeves for these cards like this:

E: I mean... i think the appeal is limited again often to people like crypto guys or people who are very involved because they don't trust the security in this....but rather than we also have these kinds of public transport cards that use this...I would have to take it out into and that's too inconvenient for that. You would choose a convenience. I will use this has to somehow work out and say somehow better use this functionality. Yeah as again someone like to try to steal something for me. It is not wouldn't be so much that I would care about this extra risk.

F: Yeah, same for me

AH: Do you use a VPN at all? So what do use a VPN?

E: Yeah we use VPN to get access to our internet company Network.

AH: But not on a personal level if you would I don't know?

F: I would say I am not using it.

E: Public Wi-Fi.... Yeah, so if I would use open like networks more than I would consider using vpn. Oh, yeah, lots of trust. So if I'm if I'm out of the office, obviously all of the work data would have to use VPN. So yes is the most have to say with our University Service as well. If I want to access. I don't know details from I'm more concerned about the data of the company rather than my my own is that because of the company in the room door but sanction.... I think this is a very good like way to control but to educate your workers or employees to keep your work stuff secure. Mmh through that some kind of confidentiality agreements and some kind of penalties.

AH: Do you think that only works in a work setting though?

E: You wouldn't use that with insert the public sphere. So one of the key interest is now the this grip push to make cyber so, you know citizens cyber security act isn't everybody's responsible in some way or another out of the talk the other day and one of the guys speaking said, you know, you're only as strong as your own social network because if you're speaking to someone who is you know, reckless with their personal data and you're sharing in some way yours then you're only as strong as they are.

AH: So do you think that that could be applied to the public as well? And you think the public should be security actors or do you think that's really the role of the government?

E: I think this is you have to be knowledgeable about things and understand what's possible when something happens... and I lost my card.... but some costs benefit more... so it's for me as I think for many Estonians. It is pretty convenient. My life is smooth and nice using Digital Services and much value more than my privacy or possible threats will what would happen.

Secondly, I think Estonians are more trustworthy because our digital neighborhood is quite a safe place. Mmm when you are living in New York Bronx, so if you feel threatened physically threatened every day. Hmm, if you live in give know maybe UK or London you feel physically threatened every day more than in this area. We have this kind of a trustworthy neighborhood around here, but in digital sense. Maybe that's it's why we are not so concerned about any security issues despite. We are aware of them, but we are not so much worried about can ask is that as I different places...

F: In Estonia, some Estonians are living in Russian (editor - Soviet) built regions of blockhouses... with many Russians, and there is a lot of kind of community culture still inside of that.

E: But going back to our systems You have to have good balance between services and data use the update has acquitted protected to use them for its and the balance.

AH: That's interesting... as a political scientist I tend to try and you know, apply political theories to cyber security contexts and one of the classic security balances this idea of balancing Liberty and security. So you're the idea that you sacrifice certain freedoms for the government to keep you safe. Do you agree with that?

E: I think in Estonia that people are more happy to you know, sacrifice what we don't need to call them freedoms... but you know in terms of your personal data... and you're more likely to give that up because the services are beneficial to you. Because I was this one's at the last architecture of Information Systems. I don't think that our government has poured or means to action but home everything about me in different Information Systems around governmental offices and Ministries and so on so that means kind of crippled and they would like to misuse my data. So that's why I have so much kind of I don't feel that I have the most Freedom or have developed some powers of this ministry by freedom for my rights. So it's kind of maybe my feeling is that sell is for medical services? I'm benefiting from some and it's kind of say they are not getting so much back from me. Mmm. So they say she can't miss use my data say actually don't do anything unreasonable.... about some see you very much trust the system because that this was this this only functions if you actually believe and you trust in the system, right because if I were to sit there while I don't trust the you know, the technology that you say I don't trust that that it's actually notifying me when personally has access my dear daughter has told me about so you really have to trust that somewhere in your system. And you do that's why yes. Yeah, and it's very hard to reduce Health Services in the UK or Germany or people just have this don't trust fully or very important in this student. People are actually happy about reporting taxes to moments and this is service. Very strange when you think people were happy to report access because it's so convenient.

AH: Do you think there's almost a national pride attached to this as well? It is part of being Estonian?

F: I think so. Yeah. Yeah being a small country we have this also national pride. So when we have this efficiency from governmental side, which is our tax system has been this is also a kind of a benefit for me as part of his nation that we have. Our government is doing a good job and is not losing money having paperwork or whatever other progressively rules to do my taxes.... it's not wasting my tax money.

AH: Do you believe that Estonians are actually more security aware than other European nations?

E: You know, I wouldn't say that. We also have this kind of no worries because trust me. Did you ever have any issues with so so you mention your mother and you know, I'm perhaps all the people the older Generations as well with pushing these out because one of the instances I've heard when I've spoken to other people about this is the found, you know, elderly people and they keep the cords and you know the same wallet with the card. So if anybody were to find it, you know that that would be there.

AH: Do you think that there's a bit of a generational Gap here or do you think the accessibility is actually quite good?

E: We tend to discover that elderly people are becoming more aware of data security. Yeah, but not because we are not specifically worried... but I think it's generally so it's not so much has happened. Also, why mother knows well that identity should be protected at all situations. But yeah, but it might be different in the next 10 years. People didn't understand the idea is that the threat is growing and proliferating because we have so many more connected devices with some your smartphones and smart cards that you have talked about

did you think that the use of the digital identities and the holy governance system actually makes a Estonians feel more secure because you all seem very relaxed about it as a system and its functionality and there's very little sort of you know, they are when I explain the system because when I have to do this in the UK, I have to explain how the Estonian system works because now obviously not everyone is familiar with it the and Pete the the reactions range from you know, wow, that's really convenient or that would be great to this is terrible. I can't believe that they trust this. So do you think that the it actually the whole system that we referred to it? I guess I don't in an ongoing with this makes you feel secure because of the system itself. Do you?

AH: Does that make you feel more secure?

E: Just maybe a relevant point maybe not but you have to understand also that maturity has been rising over the years. So then we started to do we have totally different kind of understanding what's security and people didn't trust tree or you know, think about us because we're not using it. Yeah. So now we have this maturity you can buy use this ID card to buy bus tickets or cinema tickets this kind of access for of services when you introduced to Foreigner, they don't understand that they have been kind of a busy... And yeah, it's the services have been introduced gradually and yeah when you show this end result to somebody it sounds crazy, but we have to understand that we have used some services and send... and broaden our services kind of environment and now we are using are using it mostly for every sense and it's it's hard to grasp it when you are not rising in this system. Yeah, of course because it was a gradual thing people. I think I didn't have a car. So we have this younger generation who's been inside us is kind of a trustworthy basically and grow up with it. Yeah you too. I don't know maybe trusted blindly or not. You know, if everyone uses it, it's some kind of....Do you feel that it is a safe? (To SJ).

F: Yeah!

AH: so I mean obviously you guys are Consultants. So what are the common security concerns that you guys come across ?

Those are seeking for actual security and the government of rules some have to spell it's between actual life and also security framework sweet obliged to do that and see how to do it. Well that's also pi the compliance thing, right? Yes so business continuity.... They are so dependent on Digital Services nowadays. They look how to make some companies in Services could be liable working. So they are bits of the reliable. So that builds public trust within them. Yeah, not so much about using data. So it's having Services is more priorities and having data.... So it's I just I wanted in terms of this big push the ideas of the the human is the you know, the key security threat here and I just want to do you ever come across this where you have to be used in an educational so naughty feel actually Estonians are pretty good you know! The Cyber hygiene here is very good

But this... It's not our Focus to be more like helping with these kind of company frameworks...but It's always the weakest link... people are the weakest link is he has information from person to heck you're in some kind of information system!... We are going different trainings for how people deal with threats

AH: Sorry I'm getting aware of the time here, so i'll wrap up here, but thank you so much both of you. That has covered all of my questions anyway

E: Thanks for taking an interest... but yes, these things are actually working it's the only has been a society has is working for 15 years and itself had been so much misuses and kind of other countries can learn about this experience apply is worries and from culture nation that but still it's very important to understand that actually it works. Yeah, and maybe it might not work for bigger Nations or other cultures, but but still it can't work this year, very important thing.

Participant G - 09.4.2018

AH: Introduces context of the project / research ethics etc.

G: Fundamentally, trust is vital, and this is what you are exploring? For us... it's.... well, if you look at the history of Estonia, we have been ruled and governed by people we did not trust. Nearly everyone has a grandparent who was deported, or was a refugee, or whatever. I have a total of 3 of my 4 grandparents who were refugees of war, who by sheer luck ended up in Estonia, rather than a camp in Siberia or in Germany... and some of them also became potential deportees but things happened.... so coming from that, it's the sheer miracle of having a democratically elected, rule based government, that generally doesn't do anything terribly wrong.... it's a frickin miracle in itself. So the trust isn't in the devices, it's in the institution of government itself. So, on a purely emotive level, this isn't about devices, or technology, but the trust in a democratic government.

AH: Yes

G: Secondly, it is important to remember we built the nation from scratch in the 90's, and there is a great sense of ownership. There was very little in the way of existing infrastructure.... we did not have a lot of legacy to carry over. We had to develop from scratch.

AH: So famously you turned down a lot of old hardware offered by Finland around the time of independence, right?

G: Every dentist had a chair that had been used in Sweden before... so it's not just the digital side of things. But in terms of government, we just couldn't afford paper based, very distributed bureaucracy. We were too small a country. So there's all of those things. There's the internet as an ecosystem... so what Estonia does, and not a lot of other governments do... although the Georgians, the French, the Italians to a degree, you will notice they have this fetish for technology, without properly thinking about what it means. But for Estonia, there are very few things that are duplicated, very little that you can't do digitally. So property... and something else

AH: Marriage and divorce, right?

G: Actually, so those are all maintained digitally... as my ex husband found out when we got divorced *laughter*.... and the purchase of large real estate... you have to show up in person, and will be identified by a civil servant or someone mandated by the government present. But yes, it is not solely digital. So when there are updates, on laws relating to digital services for example, these are done digitally. It no longer comes out in paper form at all. The land registry, or property registry... you don't actually get the paper records unless you specifically request them, and you don't need them. So when i bought my first apartment a few years ago, i was actually quite excited to get them, and to have the physical piece of paper... and you have to pay extra for this. We've been doing all this for a few years, but we've built trust relatively quickly. Also, you can't access the population registry... it is all online. The thing for Estonia... it's been a very logical sequence... the government provided the secure digital identity, attached to the mandatory ID cards

AH: Which is one of the problems in the UK for example, as we do not have mandatory ID cards

G: Yes, and part of the benefit of our cards is that, because they were mandatory, the private sector was more willing to develop solutions using this technology, as they knew everyone had them. Getting the private sector on board was a big deal. But the services themselves were also developed gradually over time, with the option of doing it online, or offline. So the census for example, last done in 2010, was an example of this. You could do it the way it had always been done, or you could declare it online. Something ridiculously high number wise did it online, when they realised they could do it themselves, with minimum interaction with the government. So everyone was reaching for the codes for their cards, to do it online, and there was a big spike in people using online services because of this. It's so important we have this ecosystem, we have the x-road, we have the secure identities, based on census information... so people trust it. Other places, like India, are starting to try and replicate this, but with some difficulty.

AH: Yes i've read about this before, but they have issues with no registry of many people, people without official addresses because they live in informal housing...

G: Exactly. They're still in the stage where you need to be able to offer it offline too. Here, you still can, but honestly, why the hell would you, when it's so simple using our systems? I'm not sure even doctors carry prescription pads here anymore, as it's all done online, but technically it can still be done offline on paper. You can register anything with the population registry, which is where a resident interacts with the government, and you can do it all online... even registering the birth of a child.... there's a ritualistic element, there's a security element... and whatever is easiest, you know. It's the trust, and then it's that the digital has always been an option, which is why i think Estonia has been so successful... because if it's your only option, it creates a negative reaction. Trust is by its nature, built slowly.

AH: So you touched upon a few reasons why you think the systems are trusted, do you think that through this e-governance, and the whole digital identities scheme, do you think this actually makes Estonian citizens feel more secure?

G: If security is done properly then you don't worry, i mean, it's clearly.... when people talk about 'big brother' security... that's security not being done right. The amount of cameras, in the UK for example... might be security gone wrong. It's... you have to have the security present, but it has to fulfil legal requirements... anything you do digitally has to be as secure as anything you do in person

G: So for us, because digital identities provide another option, and there haven't been major security incidents... i mean there's always issues, but it's whether an issue becomes a major incident.... and *taps the table* we've had the fix when required, before it has become an incident

AH: What about the flaw in the cards last year? Do you think the way that was dealt with helped maintain public trust

G: Ummm i don't think we particularly suffered, but i am the point of contact in this department for that incident, so i might be slightly biased... but all in all, we were successful for a couple of reasons. One - if you look at trust in i-voting, it was 32-33 percent that voted in this way, very slightly higher than last time... we knew there was an issue, and vulnerabilities are hard to communicate... in the corporate world, you generally get an update, but the vulnerability isn't explicitly told to you.... it might say that it's a critical update, you know... then it's on you. As a government, we picked the more transparent communication approach.... and had a fix before we had an incident. We've not had an incident, that we know of *taps wood*

AH: So in some of the English speaking media, there was a certain triumphalism around these flaws, that Estonia wasn't doing cyber security quite as well as they claimed...

G: and it wasn't our flaw! The flaw was in the crypto library, in the deep mathematics of the card... it was within this library, there was a mathematical shortcut, which made breaking keys slightly faster... and Estonia had used every single best practice, including.... generating the private key on the chip, which is slower but also more secure, because the private key is never transmitted. You can't have a man in the middle if there is no transmission, it happens on the chip. So... since 2007... this vulnerability... the way we have dealt with things, we have been very open with our communication. The critical sectors, those dependent upon cyber security, cross borders of course. We work with a lot of Nordic corporations, and you must familiar with the new legislation coming in this May?

AH: GDPR?

G: GDPR also, but i mean the NIS directive also... as this comes in first. The minimum standards of this directive are protecting critical infrastructure... it outlines six sectors it considers critical, and where you have to have business continuity planning, risk management, crisis planning... all of that. Banking... medical... and a couple of more sectors... um and for us, after the emergency act of 2009, we have another one coming into power now... this emergency act took care of all that... you can have your emergency services across borders. To provide those services in Estonia, you have to be able to provide these services even if international connections are cut. You need to have a back up in Estonia. We have had a very risk management driven approach. The ID card was one of those. Trust... elections are the best test of trust. You get the timeline, and you can compare. We have two sets of elections coming up next year... Use has been just slightly below one their for the past few elections... and of course vulnerabilities are complicated. Crises are easy in a way, because you have clear routines and procedures for crises. Vulnerabilities are one incident, not a crisis, and you're trying to ensure that crisis doesn't happen.

AH: Is this achieved through educational processes, and encouraging hygiene processes?

G: That is one, secondly it is as a government. We have taken “aggressively transparent” and open approach. That’s why the vulnerabilities with the cards... because it was a vulnerability, not a crisis... the identification mechanisms didn’t pick it up because it wasn’t a crisis... and we, unlike other governments were open.... those chips that were faulty, was less than 1% of those chips globally.

AH: Only those produced after a certain date, right?

G: Right. But there is at least a million of them used globally. It’s part of the hardware of devices used globally. Many e-solutions use these chips... for banking, for example. and because of how fundamental this is to many solutions, other governments ended up revoking those certificates... Austria, Spain, Poland and Slovakia.... the we know of, of the EU member states... Estonia suspended and remotely updated them. Which is, if you compare... we had the legal possibility to suspend... and we had technically the possibility of updating, by which we essentially created, even though the flaw was two or three layers below. We only had the card validation issue, everything else else was universally used... and there’s a few providers. So we, in our software, provided a way of bypassing this, and based the cryptography on a different way of doing that. So, all in all, compared to others, we did well... and if you look at the feedback from users, we did alright.

AH: Do you think Estonians are perhaps more security “aware”... especially from a cyber security perspective, than other European nations? The overall impression I sometimes get, is often the opposite, that many Estonians are quite relaxed about this

G: I would say we are less digitally sceptical. I think it’s that. We are more aware of the risks being everywhere... i mean, if you’ve had elections... to quote Stalin... “it doesn’t matter if you control how they vote... as long as you control who counts the votes”... and if you come from that... anything is an improvement... I mean you look at Lukashenko now (Belarus)... or Castro (Cuba)... or Mugabe (Zimbabwe)... they all hold ‘elections’..... so yes, we’re less digitally sceptical, and we accept security as part of the digital world, as we would in the physical.

AH: Out of curiosity, how do you define ‘cyber security’... this is a deliberately open question...

G: For the government, there’s basic definitions in the strategy. It defines many different cyber terms... so the one that’s still valid, it’s in there. For me, it’s the security of data and information networks... and the systems that carry them. Also, i would say it is distinct from data protection.

AH: Do you feel there is a difference between this governmental interpretation of cyber security, and your own personal take on cyber security?

G: Yes, it’s also the set up of the networks for me... Security not being an afterthought, but part of the design process. Having procedural controls... you cannot behave better, as a user, than the system allows you to behave. If the system doesn’t have two factor authentication, as a user you’re going to have to rely on one factor, and if that’s the password, then as a user... you’re forced into a not ideal situation.

AH: In terms of perceived threats... do you think there might be a disconnect. So for the government, what is to be protected is essential services and usability... does this change for citizens? (What must be protected)

G: Estonia doesn’t look at it as protecting citizens, Estonia looks at it as really as providing a highly digital way of life. You’re providing a lifestyle. So, providing flexibility to file taxes at your own convenience... rather than 5 days a week from 9-5. To be able to do all this, you have to have the correct processes in place... so the government doesn’t see it as providing security... it is in the comprehensive, military sense, absolutely... but when you look at the services... it’s about having the services delivered with appropriate security.

AH: No concerns at all regarding personal data or potential manipulation or misappropriation of it?

G: We have safeguards in place for that. That’s why we use encryption...

AH: Does the Estonian government cater for the less technically capable do you think? Those who cannot encrypt their own data, or are perhaps not as aware of security processes?

G: So, if your bank only works on a secure encrypted connection... using the identity the bank or the government has given you, then... well, you cannot put the burden of security onto the average user. You also can't put it solely upon an institution... in hospitals, for example. They are not in the business of providing security, they provide healthcare. The NHS, for example in the UK... and the recent wanna cry attacks. Do you know how many victims we had of wanna cry attacks in Estonia?

AH: Haha I'm not sure, but I'm going to guess this is a loaded question, and it is zero

G: Absolutely right... one the of main ways this remained at zero.... for key government services and systems, we phased out these outdated operating systems when they ceased to be supported for updates. So while the UK was running these XP systems, we had already moved on, so we were not vulnerable. So when it was announced these were obsolete in 2013, we even ran public awareness campaigns to highlight the risks of continuing to use these systems to users. It would have been unthought of to have XP running a government system here... it's stupid. I understand what the British government did was buy some patches for a few years, with the price frequently rising for these... and then when that stopped, they just kept running these older systems in good faith. Which isn't security, it's just stupidity. So Estonia phased it out, advised government managers on how to do it, and notified users. When you went online to portals in 2014, and you were running XP after this point, you received a notification saying something along the lines of "seriously?" and after that we significantly reduced the number of systems running on XP way back in 2014, 3 years before wanna cry was an issue... and also, we audited places like hospitals, realising the people there have other priorities. We can't expect them to have the burden of cyber security, they are in the business of saving lives. So the state assisted them, advised them, offered audits... It's a question of wisely spending money as well. So while a car or ambulance with faulty brakes might be cheaper, it isn't the wisest way to go about things...

AH: Yes, so it's raising awareness...

G: Also, it's a question of accepting risk, and knowing which risks are and aren't acceptable. So acknowledging which levels or risk are acceptable and unacceptable.... with any solution, paper based, digital or somewhere in between... this happens. This however, wasn't so much a vulnerability acceptance... it was leaving the door open.

AH: How have you raised issues of accountability? Why do people trust these systems?

G: So it is achieved by transparently dealing with abuses of the system.... so every now and then you see a police officer who has missed the system end up in jail thanks to our data protection laws. If you catch people who abuse the system and punish them, it shows you take this seriously.

AH: So you think publicising these abuses actually helps enhance public trust?

G: I think so... it shows we are not trying to cover things up. It's the same as the Skripal case I suppose... the UK government has been clear on what the substance is, and the public trust the governments version of events, as they have dealt with the issue in a reasonably transparent way. That's a non cyber case of course....

AH: I wanted to go back to the security by design comments you made earlier. So I am interested in the public relationship with, and the proliferation of connected devices and the IoT. Obviously they are a major concern, identified in both the British and Estonian cyber security strategies, and the lack of security by design within them...

G: Well, I think this is almost a question of how far can a government go? It's.... uh... its not ... it's a global, corporate vulnerability also. So you can't have a nation state solution to it. With a lot of these other issues it's the same. You can have European standards for example... but no nation state, particularly one of Estonias size... probably not even a nation state of the UK's size alone, would be large enough to enforce industry standards by itself... so, it's not a nation state solution. It's an issue of products and services, and questions of accreditation, so we need a situation where you require certification and accreditation for that market. So America, or the EU can set standards for products to circulate within their environment, and if products do not meet these standards, they cannot be available for retail.

AH: Yes, the British decision to leave the digital single market is baffling to me in this regard...

G: Yes, so if we have global products, it is difficult to control, but things can be done through cooperation at an international level.

AH: We also have the issue that a lot of these products... smart phones, smart cards... they're almost essential services... it seems unwise to me to have these being developed, and expecting the industry to self regulate, when so much money is involved

G: Yes, and our identities are an essential service... with the IoT there are things which are inherently insecure... things like toothbrushes with USB chargers... kids toys, smart tv's... no one is thinking about security when they design these things.

AH: Heating controls from phones...

G: Yes, so this is often something that crops up. The idea that instead of attacking essential government infrastructure, but instead attacking seemingly mundane things... like the ventilation systems in a server room for example... it will self destruct in a relatively small time frame. Things like this are scenarios which are often discussed

AH: How do we ensure developers, if not through legislation, act responsibly in regards to security. Do you think the government should regulate security by design, or enforce it?

G: Its a layered question, with layers of responses. The first thing is things that the government itself develops... or buys. That's a whole other discussion, whether the government should be a vendor, or the government should be a developer itself. That's a very different relationship. However, once you get to consumer products... health and safety wise, you cannot allow unsafe products, and this applies within a cyber security context also... but how far can you go? You can't expect the customer to be a cyber security expert... i mean, I'm not a dentistry expert, i have a person who does my teeth. Now I can see her diploma and certification on the wall, and she certainly seems to know what she is talking about when she explains things, so that is good enough for me. We also know her family, so if she was making it all up, it would be quite an intricate lie.... *laughs* so yes... while the customer has a right to be stupid and reckless... they can buy a more or less expensive lock, for example. We don't mandate home security systems... when i moved house, i had my home security installed before my kitchen. Security comes first! but not everyone does that...

AH: So to a point, you think this is a personal choice... for example, i don't know if you've noticed i have a camera cover on this laptop... that's a security choice as well, i guess? Do you have one?

G: Yes... and I worry if there isn't one.

AH: Is this almost security as a marketable commodity though? I almost wonder should these not be already included as part of the design process, so the user has ownership without having to go out and effectively customise the device themselves?

G: Perhaps.... I'm very aware of this. When working with others, I often tell them that they should not trust the 'on-off' camera light, as this can be taken control of.... so, I think you have to try to legislate as much as you can... without limiting access to innovation. Security only makes sense if there is a benefit for the consumer, through the service provided. We have to be conscious with regulation though, if it is too strong, it can become available elsewhere. Estonia is small, and will go to big markets first, logically. They have to earn back their investment. It's a delicate balance. I personally don't believe in nation state solutions, because it's not a nation state problem... it's a global problem, and it's a side effect of access to innovation... and a nation state solution would be to limit access to innovation, which is counterproductive.

AH: So another example is contactless cards which are being rolled out generally across Europe now. We've had them in the UK for a while, and they're becoming more common in Estonia. These are largely being issued without the option being given to the consumer now... you can actively ask the bank to disable it in your card, but they are issued with this functionality, if you asked for it or not

G: So banks tend to lead the industry in terms of risk driven and impact driven approaches. Which is why a lot of banks limit the amount of spend, varying by place to place, based on their analysis, and whether they think the risk is worth it for the benefit to consumers. Also, banks become liable if something goes wrong and it is their fault... so they are very aware of that. They are in the business of managing money. So they are more risk analysis driven than a lot of other places.

AH: So, I guess one of the big questions I ask, and it tends to be the last one, is that do you think that citizens have a role and a responsibility in ensuring cyber security.... both their own, and on a national level

G: Hmm... it's the same as physical security. You have your individual responsibility... so, you don't walk across the arch of the bridge in Tartu (a student tradition they have been trying to actively prevent by raising the height of the arch) without acknowledging you are putting yourself in a certain amount of danger by doing it... and it depends on the conditions you're doing it in as well. It's your responsibility.

AH: Yes, so i walked over the frozen river recently... possibly against general accepted safety expectations, but i made a decision that i could see footprints, so others had done it, and it had been extremely cold and frozen for some time... however i knew there was some risk involved in doing so

G: Yes, you're aware and you made that decision. So it's about the citizen, or the resident, they have to act according to best practices, and know the risks. Just like you don't hand out your ID to someone in a nightclub... if you did, you're giving them the possibility to pretend that they are you.

AH: So you do think that there is a responsibility of citizens to some degree.... I often approach this from a more general security perspective... and critical perspectives which suggest that the burden of security is increasingly being placed upon ordinary citizens to be active security actors... so in the UK we are encouraged to be vigilant, and to report 'suspicious' behaviour in public places.... critical studies have suggested there is too much of a burden being placed on ordinary citizens... do you think there is a risk of this happening in a cyber security context?

G: Yes, of course. I think it's a fine line. You cannot make security too complicated, because then it doesn't happen. Security has to be simple. At the moment... if we look at password guidance for example... it has always been to have digits, numbers, symbols, don't use common words... and what happens is that people use the minimum length, because you're asking them to do something that is very difficult to remember... they might also be repetitive in password use, or they do something else, like write them down. You also end up with common repetition... so numbers will be 1234 ... things like that. Regular patterns make them easier to guess of course. So then, we reach a point where we think actually, you know what... use something you'll remember. So if it's longer, but it maybe doesn't have symbols etc... so be it. It's harder to guess with brute force based on combinations of 6 or 8 characters, rather than a much longer, but perhaps less complex phrase. So something memorable and long, even if it is non-complex is actually better.

Participant H-03.04.2018

AH: what does cyber security mean to you

H: The words cyber will comes from this word cybernetics, which basically the discipline that studies how all the systems are government my top down governments. So basically if you talk about cyber security to already has this governance meaning that you want to control some systems and people in the systems and it's not like the like the grass roots are like...I think it's the opposite if you talk about cyber security, it did immediately gives me impression of that. And if you somehow look at the discussions that are about like internet and details vary in general then the cyber security kind of vocabulary.... like the Cyber like putting cyber beside every word. This is what government does and usually activists don't do it.

AH: So I must admit I've toyed with whether I want to use the terminology in my research and you go and you look at the history of what cyber isn't do do I want to use cyber security because you're either there's an association with government. I think absolutely for me I choose to use it. But just because I think it's more communicable. So if you know if I want to if I have to explain the someone who's not in Academia and has no particular interest in this field what I do if I see All I'm interested in matters relating to cyber security that's understandable to the majority of the population or at least they're familiar with point. It's kind of true.

H: You could also use some other words, depending. Well, I don't know. What's your exact title of a research and so on but it's somehow similar do all these discussions about. I don't know gender issues, for example, because if you use certain worrying you kind of helped to establish certain discourses and the ways of talking about cyber thing is it is the same distance so I kind of feel like what's it... Some sort of minority rights issue not healthy.

AH: So you would actually not use cyber. What would you use instead?

H: Once you're using usual government discussions accountability transparency, you have lots of other words, like reliability of the systems can use also this sustainability and resilience. Yeah, a little kind of words that can describe the systems and not use the Cyber thing.... is just it's it's into world in a sense, but it has this top-down connotation really strong. He had since it emptied it is also it's sort of invasive it brings you into certain way of thinking without you being able to be against it because it's a network. Yes. It's really not useful to start arguing about government. So fundamentally, I particularly dislike the term cyberspace but then I wrote something the other day and I ended up using it because I couldn't think of another way to explain it. Yeah, I've been lots of like trying to deal with this issue. How should you should call the digital thing that we have? So yeah, I use digital sphere and was told that it was too complex and I should use something communicable her cyberspace. You know, I'm not sure I also use something similar relate some digital sphere and other than information will Information Society a word I tend to use occasionally then about like digital systems digital digital whatever some sort of things. You can put digital also in front of everything lights on Cyber.

AH: Well, I did this at the beginning of my project and I just sort of started to realize that I'm just being abstract for the sake of it and that actually all I was I was making my work less easy to access for people.

H: Yeah, if you use it a lot and then you're like start to like find these nuances in this warnings. And then you find like some of the phrases that really work. And yeah for me as a philosopher from background, it's kind of something that I kind of like to do it. Yeah like to some of the ship the concepts and make some another use for them and which is more meaningful for me. And yeah and yeah, but yeah, it doesn't need mean anything about your work you can use this cyber. Whatever. Yeah, you can click. Yeah, like yeah, like I said I end up using it because it's a common term and it's become established in somehow. I like the words. I was facing for some reason because it's somehow connected to all this cyberpunk things and and it's kind of.... I think if you take this kind of artistic Movement Like a literary movement about cyberpunk, then you first of all you state that it says cyberspace its control space and your kind of opposing it from the beginning because if you're a kind of this and tank antagonist in this whatever novels like William Gibson, whoever there you are already considered as somehow in between there like the system and you are fighting against it and in this sense, it's this is the right is but that I'm a geographer as well. I have a background. So I'm starting to think that this is a space and I cannot conceptualise this as a separate space because ultimately this is connected

to our everyday lives every so you know, if we we can think about it as being dead real numbers on the screen or whatever but in some way shape or form there is a material object involved which is in this perfect place in some way or another.... now it will undoubtedly changes spaces with that we move through and I think it's transformative. But I'm sorry I'm becoming very abstract. But for me, I have to think of it as you know cyberspace is just space. Well, if you can talk about digital space, this is something that is not physical but science can be physical. I think yeah, I think it's I think it's I like to think of it as one and the same much like I like to think security and cyber security. They're all security and they taught, you know, a cyber security concern is security concern a question about this motor. Well, it can be verbal. It might also be some kind of my position on this site is cyber security. What what it is think well, they're ignorant least.... Like them there is this kind of proof they security basically like the risk analysis style analysis to see how this not requirements based on some similar role like the criteria based on standards. What's this?

AH: Yeah, I know in information security in particular the there's this idea of standards that you have to comply with.

H: Yeah. Well, there's also work how it's called in research or and also you have this all this organization that sell their will they will they sell basically the quality that the system is system is secure so they have to get out some give out some certificates and some sense. I'm a novice to do it and they comment a big somewhere check boxes. If you have like if you are servers are ventilated if you have like doors marked in the certain way that the will whatever basically

I have a friend who also worked in Japan for slits his 15 years older than me and he worked for banks in Japan and they basically created the security systems for the banks were like secure banking systems basically and he came back to Estonia at certain point and try to will convince Estonian officials and some companies to use the proof based security. Basically, what was all this something like you have like information systems is based on a mathematical system and when in mathematics you have proofs. Yeah, and there is a concept that you... You have these information systems that are proved to be sort of you can have these Integrity proofs and you can have something of running proofs for something and so on and there are mathematical formulas for that and for they do you believe that that's what cyber security is then or do you consider? Well, this person was trying to kind of convince current government and some companies that we should be something that should be done. And this is how it's done. Right and in Japan basically you had experience doing it because well in Japan, of course, there's lots of work for money and looked bigger ones bigger companies and Banks and they really need to pay attention to that and in Estonia will he was kind of Civic blows. We don't need that kind of assistance and they're probably too expensive and too will make you need too much research for that and we don't have that kind of passive in Estonia. So we will busy systems like when you will... instead of having this architecture, which is secure from this perspective. We can just have like we instead of one cable people to three of them then if one is one is broken into two others work and we kind of just stopped again systems and make this kind of security that's almost the idea behind the data Embassy initiative isn't it at the theater Embassy initiative that the Estonian government the rolling out with the moment. So they're basically putting hard, you know Hardware in a couple of the first one is in Luxembourg in their embassies. So if anything were to you know, if Estonia were to be occupied by a perceived threatening near but perhaps the data Embassy initiative

AH: Yeah. Yeah. That's that's how they branded as well. I have a colleague who's working on this.

AH: So, one of the things I always ask is do you take any measures to ensure your own cyber security which you have mentioned cyber hygiene and the side of this process based thing, but I suspect for you, there's much more to it than yeah following processes?

H: yeah this computer in I think I encrypt my home directory in this whole bunch of Link's which I have here and it's my not my personal computer is my work computer actually and I I but I'm quite a lot lousy in distance. I don't have too much measures about my my I don't know security because I use all this social media accounts and use them to communicate. I don't take any extra measures to encrypt my stuff except for like if I really need it. If I communicate with some kind of activists from other country than I tend to send this encrypted emails for Althea. I have my GP G key somewhere at the key server. So if somebody wants to send me something I can receive encrypted emails...vsome of the activists use also this crypto chats like signal or most of the other one of these, telegram. I use this. But I even don't have this custom operating system that are which I have just hooked on to install it because it's kind of a hassle so if my phone is my life.... but also a security risk

AH: Why do you consider that the biggest security risk?

H: Well in the sense that if somebody wanted to get into my information channels you get inside my I don't know well lots of people use Google account for something like it's if you get to somebody school account you probably get to a lot of other things too because they have the confirmation emails and so on. But yeah, I actually I use Google mail for like General stuff and I have my friend that she works at Google and then he's kind of the one who didn't go to study philosophy. So he's a security something of an expert and do we run our own family makes her so I use this for things that are really important. So this is also something of Chinese users from your phone as well.... I think I used one day but currently not use it from my computer. I do use a VPN or Soul when you know, why should I concerns around in Secure networks? I suppose but it depends where you connected. Of course. I assume he trusts one place ones but and then it depends on the data that you're accessing as well. So I mean, I have a VPN service and if I go and sit in a cafe, it gives me the little morning saying you are on an unsecure Network and I don't know what way should I use it? Like well, of course, there are some cases where I should use it globally but since most of the communication is already from through a browser and browser has all these HTTP like the protocols for all the things where you log into it's not that important for me I think but and I don't use... Which like all other applications that Community communicate through internet which where my might not be that sure if it's encrypted. So if I already used this secure HTTP, then I consider myself sort of on safe ground. And if I need to do something really and delicate or something like sensitive then I just use Tor Browser or something like that - you stole but you don't use a VPN with tall just you trust the time is suitably. Yeah, I usually don't have that kind of so critical things that I otherwise I know what to do. I should kind of go to random use some Modern to network go another part of the city where there are no security cameras who love me with my computer, which I should I don't know borrow some from somebody you wish.

AH: Also you thinking about the process and the other thing I always ask is what do you take any I mean, I've noticed you've got your laptop. Do you have any of these things like camera covers? For example?

H: No, I didn't quite common, especially when you spot speak to people like cryptographers which have done occasion. They and they always have them I was getting out of the conference to be just be honest, whether I would have gone out and boarded and I should also cover my film camera. Yeah. Well, I think my my other the thing I always follow up when people have one of these covers and I don't have it myself. I also have a mic blocker and I'm a bit dubious outside some of these work anywhere, but the the basically, you know, you insert them into the headphones lot and it to your computer to detect or whatever device it is that you have put headphones with a microphone in but obviously you haven't so trick sit there and certainly obviously your microphone theoretically can't be taken over the eye, you know how much I actually trust the this with work because I have to got someone to do it. I think I disconnected the camera and it wasn't really on purpose but since I had to open it, but I had to change something of LCD, whatever here. Yeah. I just took off the camera and since I didn't lose it. Anyway, probably this is the right way to do it. You don't take anything. I always see people with like plasters and things over there. So yeah, i don't put that much stress stress on this camera thing. I never even liked this Thomas Hendrik Ilves has this tape on camera. So he's kind of privacy is overrated. I don't know but I have noticed that some of my friends who have are political activists or like Workforce and political party at some point. These tapes have appeared on their computers and ask why did you do that? And then I get some answers but not really. So I mean for me it was almost because I speak to a lot of people with information security and speak to me of you attend conferences in the game for free which does help and it looks quite nice that one I must admit I quite like the look of it, but for me personally, I would be more bothered about someone recording my conversations

Flash the like them the voice recognition. No, I mean like that you have this basic components in computer which are have something too cheap to have inside and all they already they have some sort of software on it and it's usually written there in the factory and you don't get to the source code of this software anyway, and since if you want to understand why what to computers, do you and I'm to have this source code access and he promotes buying computers that you install the software into this really basic chips yourself.

AH: So you really like to get involved and have full control?

H: Yeah. You have control over that. Yeah, I kind of support the idea of very much and somehow I have been trying to think what I have been trying to do. I am kind of folks few obvious skating my kind of computer systems in the sense that I use different software that some other people use I use like user computers for some reason. I will this is what was really good and Linux. Yeah, and so I'm kind of feel that I'm not usual Target for whatever I can for whatever at-

tacks and if somebody really wanted to attack me like some bit of government this institution wanted to get inside my computer or wherever they probably will find a way. So yeah, I don't consider myself.

Defended for like the targets of the attack but I'm quite feel quite safe for making this random fishing kind of General attacks like when your computer is taking over. Yeah my trying to be at this level. Yeah. I mean, I'm much the same as well. I would feel generally and I'm pretty I mean, I feel a bit more secure than if I was using Windows and Linux is probably the next level but I'm not quite as technically kid warming that there's also an easy to use because I have an eye for I like that the device is talk to each other. But then also I back up all my things on the cloud which I trust to an extent, but I also have a non-networked copy of things as well. So there's another weak thing for me. If I have a new computer, I copy all the stuff to the old Tardis and in it is somewhere around then I do it once again, I get a new computer because you know, if you get new you complete computer, then you have new hard disk and the size is they grow and then they use what you have on your old hard drive. You can probably copy it to new ones because you want is that much bigger? So I have this strange accumulating back up. It's just getting bigger, but it's all in one place it somewhere I also keep it on the hard disk. And sometimes the hard disks. They stop working and you have I think I have you lost one of my kind of personal archive... That's the the you know, that there's other stuff on there that I said the email it to myself as well, especially my work just so that there's a copy of it there as well in the event of cloud failure and my laptop feel like that. There's constantly somewhere where I could rescue my life.

AH: I usually ask also, do you use a contactless bank card?

H: *nods*

AH: So no concerns with using it or not.

H: Really? I don't know why you think that should be concerned about is what's the it's an RFID and there's the potential that well but the most common concern would be if you you lose it and drop it in the street and someone picks it up like go and start buying stuff and they don't need any validation. I mean the limit is 20 Euro and 30 pounds of the UK's it's going to keep you can good. If you do it a lot then he said, isn't it somehow concentrated by some kind of Bank? Yeah, theoretically but I think you'd have to be able to prove that it wasn't you and I've never had to do this. I can't imagine it's a simple process know that knowing how Banks tend to work that you would get it back terribly quickly. I mean there is a there's a transaction maximum. So 20 apparently to 20 euros here. It's 30 on mine because do you care one and then there's a maximum number of times you can do it before the bank would be calling. Do you use it?

AH: personally I use Apple pay. It's exactly the same. It works on the same technology, but for me to actually authorize the pyramid it's a fingerprint personally. That's why I choose to use it. But I've heard various different people different backgrounds that they have a problem with the security involved with this system that they've asked the banks to disable it or they don't want a contactless card because of security concerns around it and then conversely I speak to other people and they're fine with it because ultimately the amount of money that can potentially be spent doesn't I wear the convenience?

H: Yeah. I mean, I think my last one stopped working. I think interestingly. It's actually hard just also will be didn't just stop working but I just gave it to what's the institution, you know, like the police and migration of is what was something like that, they claim that my ID card has technical issue and it should be replaced in the process of like warranty or something like that. And since I have this problem already two thousand fourteen or fifteen and when I got it. But it's connected to this certificate and renewing the certification which was their most important deadlines for March 31 or something like that. So I went there and said that I'm not well I'm saying that my car with the as technical issue and I want you to replace it for free as this warranty because will technical issues that are in the other periods already in 2015. I have locks for it and I've been bleep wanted to say that no, they won't replace it because I should have renewed my certificates earlier which doesn't still say that my car doesn't have this technical issue for because of what I couldn't renew the certificate. So it was kind of strange for me. And yeah, this is somehow also that somehow connected to this delegating security to people like the citizens that first will they have to take care of their will renew the certificates. They have to go the process install the software downloaded they download also some drivers or whatever and then they have to pay for the ID card and they have to pay for it every five years because you have to get the new cards for some reason even if it works and it's something like 25 years for the card and you don't think I'm to wait for three weeks to get a new one?

AH: Do you think there is something unique about Estonia and the attitude to cyber security here?

H: Like... it started to exist before Estonians didn't have any idea what we are as a nation, but just people care.... yeah for some reason but then I think e-residency thing is somehow like if it was the same thing. Something else because that the population is famously shrinking as well. There's some kind of feeling of inferiority that we are not that important and so on and probably the first instance when this digital approach was discovered for Estonia... so besides our existence, I think probably has people buy into it as a way of validation of value kind of....

Of course, if your interest is in International Affairs, I would argue the certainly lean West politically, you know along with the other Baltic Nations part of NATO and that's you know, part of you know, it's I don't think it's just a pragmatic security thing. There's also a want to disassociate with Russia almost. Yeah that the you know, the emphasis is that they are Western. It's also even though the discussion about this USSR passed, it's something that society as a whole has not really come over it somehow.

I'm not sure. It's basically we have some history like school books which are written in a way that the current situation in Estonia is a series of events that need to I mean in the meaning of progress like yeah we have now in we are now in the best possible situation that we could be and all the other steps were like the needed steps to get to the yeah and all this.

All the steps in the history beginning from minor note like the sober Revolution in Russia to know this is somehow describing this like this. You will direct the movement towards today and it's kind of will quite propagandistic I think and I think the first the ministers and first governments in Estonia, they kind of wanted to present themselves as well as they know the best. What's the like the future of Estonia and the reforms needed and so on so it's almost like they've tried to cultivate this. But we are very different to other places like the UK also

AH: Yeah, particularly in the use of ID of course?

H: Secure ID. This is why we also have this in voting and other countries don't have this ID digital ID. That's why they don't have voting but there are several countries who have this digital ideas, which are even like better from privacy and security point of view is that that's don't don't have anything. So it's kind of not. Yes say that even Finland has this ID card. Yeah, Austria Germany in Germany. The German one is slightly different. They certainly don't have the same e-government capacity. But again, they have a big resistance to this kind of thing. And I think that comes from the history as much as anything else from talking to German colleagues. There's an association with the war and that says they don't want this once even studied a bit about the whole this Jonah ID card works and they have this privacy-preserving sort.

architecture for it that you can either you don't if you use the card you don't need to identify yourself, but you can just basically

act as your even certain role so you can what's the otherworldly both indicate yourself as a citizen of for example, city of unknown billing, right? So you don't have to say that very close shooter or something like that, but it's just it has enough filling and you have to communicate with me be like based on that level of education and it has this kind of capability. So it's sort of privacy preserving but really since I don't have it myself and really tested. Yeah, I'll have to ask my colleagues about it actually just work but I've had this discussion particularly with one of my German colleagues in London, and she showed me her card and you know talk through it but generally their privacy. Yeah, I think it's the same time. It might be a bit later but this is basically like. Let's take a simple chip card put some keys on it and just use it. So it's like Midas technology. Basically. Yeah. Yeah. It's not the same capabilities via governance. Of course. I'm not the not to the same level anywhere.

AH: I believe Estonia still offers the most services?

H: Wait, you can even taking yeah even taking the evolving aside. Oh that I'm seeing this very confidently, I would have to double check but I'm happy very least do studies of people with it. Estonian eServices are not the top list actually and even the amount of this is I think disputed in some for someone who's having more easily. This is and they are somehow better organized and they don't use this ID card but some in a bank authentication and so on and yeah, it works other ways in other countries and Estonia is not that kind of special in the sense, But yeah, there are some stud-

ies that say that the quality of them is bad. Another thing that even Estonians say here like even in public they can say that they are not user friendly... in the center that you don't find the service that you need in a logical place and it's something you had something. I've kept like list of the services then you have to kind of figure out which service is that you actually need when there's some sort of a need for it. But yeah, the digital ID... Obviously, there's a huge convenience attached to them. But do you think they actually make people feel more secure as well? I'm not sure for me. Personally since my ID card has his had this technical issue and I meant the board of several ngos were shy should some sign some documents and make some benefit. No Trend prep Bank transfers, for example, so this technical issue with my ID card Skype is quite annoying for example.

AH: What do you think the key threats are in Estonian to you know, if we taking a cyber perspective?

H: Just curiosity brought this ID card, which I was also involved with the that we had Minister of Justice sign some documents with ID card thinking that his signing them but the software in Ministry was bought from some Latvia Lithuania and Company. I think like a contractor who had for some reason exchanged the certificates for this pin 1 and 2 1 is used for authentication this personal identification identification creation number used for authentication another rule for science documents. And they use the same certificate for authentication and signing which made actually the digital signatures Inlet. So the we have documents signed by the Minister of Justice forParliament like to extend to apartment which we've had faked the digital signature and I was the person to discover it because I was playing around with this software for ID cards, right and I will download it a bunch of documents from the site of the Minister of Justice and found out that there is like 10 documents which has this very digital signature and well there was a newspaper article about it and so on and some journalists wanted to cover it. But the main thing that happened after that this was only that will the mr. Than sign the documents.

Yeah, I guess where you're alluding to there is the potential for this to go undetected and then we first did this to be manipulated and official documents to be I don't think it would have been different if the minister science something thinks that she signs one document but science actually another document were a couple words have been changed and then who would tell that which one is a lot of drugs - just a minute sir that will I actually signed this one. I didn't put these words as well. It's kind of it would get interesting because nobody could tell which is there are talking about which is the original and then which one's the presumably legally binding one exactly because just the word by mr. That whoa, I didn't find this one but people would say that we'll probably just omitted these three words that were added they like probably use it yourself and I didn't feel it pull it away.

H: Sorry, that was a little off-topic, it was what are your key concerns? I mean, obviously we've talked about some of the little things that you do in terms of the soyuz and Linux and computer and dear. Do you think that any sort of what are the key threats to your own personal security in the digital sphere show we see and then you know, is there a big difference between you know, the national level and your own personal one...my personal method is with my phone because it's good on security and you can basically get into any kind of my network. So like identities on my phone I'm comfortable with. I should be more worried of and sometimes I'm not too much. But yeah, yeah, but I mean this is just think that you feel that threatens because I actually your personal data and personal information. No, I'm not so much worried about my own personal information both a bit maybe but information like other people's information that I have here because well I have friends. I have family related and so on and as I'm sort of activist anyway, so I'm sort of public person and have certain kind of reputation anyway, and the repetition of some kind of sort of this crazy digital rights activists activists and with some crazy opinions, so.... I don't know yet. How much do I have lose in this sense? I'm not well, I already had this kind of strange strange reputation. Of course, I could eat it could get even worse. Yeah in a sense or something might happen, but... But yeah, I'm more worried about other people for some reason. Yeah.

AH: I mean do you think people have a role of you know, your average citizen do they have a role and responsibility in ensuring, you know their cyber security and estonia's cyber security?

H: I think it's really right to expect people to deal with their cyber security... or like like like to choose the services that take care of the privacy, and I think actually government should do a lot about it to provide the.... I don't know....

the framework or like... like the requirements for the companies and its own institutions to publish the information for people to make like reasonable decisions about and you will if you ask it in a way that should people can be able to do it just by themselves probably not but I think very well I couldn't I can imagine a framework. Well, this could be actually a thing that people.... For example, actually what happened when I was developing this as to bulldoze operating system actually State Information Systems of authority started to promote it as secure like Computing system. Well, it wasn't really like but they had some certain like frequently asked questions page Pages were were asking what is the easiest way to evoked and then to do something and it was like you zest of 1/2 is just to put in the city in front of the computer. You don't have to install anything and you can just put it in this ID card early vote and well, it was really nice thing. Actually. I think if Government would prepare this kind of best practices and concealers them and will... Listing them in a sense, then it might and sense. And if somehow similar like we have in Estonia this defensively and people volunteers it can work also with all this digital spread things, but it it needs really dedication from the government. Yeah, and they have to provide this framework. Otherwise, it won't work. But it do we do that on a national level door.

AH: Do you think there is anything beyond a national level? Maybe even an international or European level

I think Advantage if European institutions paid very much attention on the like all these digital systems that people use here and also, you know a whole also like the government accountability things because I think Europe has something of a reputation of being like like sticking to some like democratic values of them. Yeah, and it's different compared to u.s. Or China or whatever. Well because I China and I suppose in the u.s. It's always this ideological deregulation....Here it's different. Like it's people are encouraged to have guns and do the training and be able to defend themselves or Estonia. Yeah. But cyber is important for Estonia. We can't be big.... but we can have influence... For Estonians, our e-governance... our cyber expertise... it's about proving our worth... So we want to be the first with this and that... There's this idea that we are threatened by our neighbour. There's maybe a feeling that no one would care about Estonians if we were not important for some other things... So we want the world to remember us if anything were to happen!

Participant I - 23.09.2019

AH: So, to begin, a deliberately open question - what does cyber security mean to you?

I: Uhhh.... there's a very simple answer to that. So, you know, that the Estonian dependency on IT systems is pretty high.... because of that, cyber security is one of the very important topics we pay attention to, so.... everything is related to the dependency on the ICT systems... to what we think cyber security is a very important aspect in our country

AH: So, it's about securing those systems to you?

I: Exactly... in Estonia, the logic is.... the development of ICT services and cyber security serves that idea. It's not a separated security area... it doesn't have a connection to the ICT world at all... it happens in many countries where the cyber security is given to the hands of the security services only... it's then very hard to establish the link between ICT development and cyber security. But in Estonia, the ICT the information cyber development strategy is the main thing, and cyber security should support it.

AH: Great... ok, so what measures do you then take to ensure your own personal cyber security?

I: Uh.... Personally, there is not much to do actually. It has to be systematic. The only thing that you could do is make sure that nobody has the simple access to your computers, don't leave it open, use strong passwords, and just obey all these regulations and guidance that they organisations are giving to you. So that's the main thing. Because, personally, you cannot really make sure that your personal devices are secure, the only thing you can do is use this infrastructure that has been given to you. So in Estonia mainly that means, when they use public services I use either my ID cards, or my mobile ID or smart ID, so i do the operations through the digital identification system... that, on a personal level, is what we can do

AH: Ok... can i ask, do you use a VPN at all?

I: Yeah sure, of course... but this is... lets say it this way, that's something that is provided by the organisation anyway when i use my computer, laptop... i certainly use a VPN yes.

AH: On your private time also? Or is this just for work purposes?

I: Uhhh... in private time. Maybe sometimes yes. But, it's uhh... for private communication, there's not so much need you know... private life... what do you do... you buy cinema tickets, you do ... you use government services when you use government services, you use your ID card for a secure connection anyway, and... uh... there's not much left when you do your private things

AH: Can i also ask, do you use a camera cover on your devices?

I: Yes, certainly

AH: Can I ask why?

I: Why? So, uhh that's the one thing... so i cannot personally control my computer. I don't know technically what my personal computer does, or does not, so it's always a possibility that someone hijacks the camera, so that's just from the privacy point of view, it's reasonable to use it

AH: and do you take any security precautions with your smartcards? So, for example, would you use anything like an RFID blocker?

I: Uhh yes, i have one in my wallet. So yes, I use that

AH: Is that a concern particularly relating to contactless bank cards?

I: Uhhh.. it is for the bank cards yes... but the security is always... it's layered. So the bank card itself is provided by a certain bank, who have already taken some security measures... so the limit i can pay with my contactless cards... also, you have to put your device very close to the device that takes the money out of your account... so of course, there are many, many security measures already taken, so this additional system that i use... it's just additional

AH: Ok, and do you use contactless payments?

I: Yes, of course i use them. It's very comfortable.

AH: and you don't have particular security concerns around that? (Other than what you already mentioned)

I: Uhhh... i mean, of course there are. So there's always the possibility if you keep your wallet in your pocket somewhere, and someone comes to close in public transportation for example, there is a possibility that they can take some money off the card. But as i said, there's also a limit. The maximum someone can get is 25 euros in Estonia... and for that reason, i use these cards (The RFID blocker) in my wallet to prevent this from happening. As always, there are many security measures, and you just have to calculate what is the risk, and what is... how much seamless operations you want to have. There's always the contradiction between doing things conveniently, and being totally secure, you have have to find the middle way

AH: Yeah... so, can i ask you on a personal level... what do you consider the key threats to your personal cyber security?

I: I think the key threat.... maybe I'm being pragmatic... the key threat is usually related to credit cards and bank cards basically... there is of course also... everything you relate to it... but threats as we have seen often seen target organisations more than single people.. there's the possibility always that someone hijacks your computer. But for that reason, when i use my personal computer, i don't keep anything private or expensive in there. I treat my personal devices as though they are public ones because there is simply no way you can secure them very well. The best security comes through security measures

AH: And, on an international level, regarding Estonia, what do you feel the key threats to cyber security are in Estonia?

I: Uhh the key threat is the... it's a little bit hard to generalise... there are different threats in different areas. So... uhhh... as you know, there is three aspects of cyber security. Confidentiality, integrity and availability of information... so i think one of the key concerns is that inavailability (sic) of services... uhhh the encryption, so the ID card is basically an encryption device, that allows us to encrypt the connectivity when we use public services... so there's no... not so much risk in this regard. But the availability, the availability of the network... when you are so dependent on the ICT infrastructure... and if something happens to the network, then that's a problem.... and also.. many things... a couple of years ago, as you know, we had the problem with the ID cards... we found the chip wasn't good enough, so you know, these kind of risks... how do you say, it's important for us to understand the basic infrastructure that allows us to use public services securely.... everything related to that is very very important

AH: Yes, so... just to pick up on the past events you mentioned there, and also the 2007 attacks, is there a fear that they could be replicated... or now because of these events, Estonia is more resilient to these weaknesses?

I: Uhh... I think there has to be a motivation behind such an attack as we saw in 2007... the attacker was able to get some sort of a result, but not too much actually... so we were still able to use everything, it was more or less disruptive. So now the question is what is the motivation to do it again? So of course we have implemented many measures how to ensure the availability of the network, and i always must say... it is not a problem inside the country... at all... in our jurisdiction we can do many things, but the 2007 attack mainly effected people who were outside of the country and wanted to have access to the electronic services... so, if you compare it to the conventional ways of providing services, so for example, when you physically have to go to a government office somewhere... so we can at least ensure this level of service in the country, via electronic means, but the problem is more with the use of internet outside of the country... so first of all, the short answer is that i don't see at the moment, the motivation to do this kind of attack again, we have already implemented many security measures to avoid that as well

AH: Can you possibly describe the Estonian approach to cyber security? A lot of discourse holds Estonians to be experts in this field, do you think this is accurate? Is there something unique?

I: I think the uniqueness is that we have implemented electronic ID at a national level, that is the really, really important security aspect, so basically when we issue ID cards... mobile ID's, people use smart ID's, the government gives the possibility to encrypt everything that a single person is doing on the internet while using government services or private services as well... so, this technology itself is not unique, it was invented decades ago, but just using it at a national level makes life much, much simpler and the security is not hard to use, from a single persons perspective. So i think that is one of the significant things in Estonia... and we are very much looking forward to every country using that in the future. EU has already going this direction - they adopted the e-id regulation about the electronic identification and trust services, so that is exactly the way to do the security.... so, because of that, we don't need to struggle with the consequences so much, but we can prevent cyber incidents from happening, so technology itself... there's nothing new, the uniqueness is how to use it at a national level I would say

AH: Do you think then that the e-governance available in Estonia, and the digital identities actually makes Estonian citizens feel more secure?

I: Absolutely, I think that's the only way you can make citizens secure in the networked environment... so, what else is there, what are the other options? When you use the internet you have to encrypt, you have to secure your data, and connectivity, and interactions, so uhh the ID card is, you know, we use it as a physical identification document as well of course, but the main thing is that the ID card is basically an encryption device that allows citizens to encrypt everything they do on the internet, so that's the idea, and the government provides that for everyone, and we are all in the same, data exchange environment, public sector, private sector, citizens, so that's the perfect solution i would say

AH: What in your experience do you think are the most common security concerns of Estonians?

I: Uhhh you mean, electronic or cyber concerns?

AH: Yes

I: Yeah uh... i mean, studies show that the trust level is very, very high and that one of the very clear indications is that after the problem with the ID card a couple of years ago, right after that, or during the same time we had local elections, and we get the most electronic voters at that time, it was a new record... so it seems that people trust the system, and there is not... lets say that publicly I don't think there are very concrete security concerns, we have just noticed that people are very aware that cyber security is an important thing, and people understand that they must use good passwords and do everything that is possible on a personal level. But i would still say, through the digital ID, we can make it so secure that the individual person doesn't need to feel insecure using the e-services.... so yeah, i can't actually point out any specific concerns of the population

AH: So... in regards to this acceptance... do you think there's something unique to the Estonian mindset that makes people willing to accept all of this? So, as you know, we couldn't implement something similar in the UK as we don't even have identity cards, for some of the trust reasons you have highlighted i suppose

I: Ummm, thats... probably... but not for some philosophical reasons, but pure pragmatism that this is the way... it is much easier to gain efficiency and comfort... so i certainly don't want to go to the government service centre to do some simple interaction with the government. So if i want to sell my card, why do i have to go physically? Whatever they do there, they just organise information. I can do it through my computer. Everything we can do through the computer, we want to do! So in that sense, I think Estonians are very... how to say? We feel comfortable using computers if the information systems make their life easier. So, I think that's somehow in the nature of our people. But i actually really can't understand why people in the UK, and also in North America are so much against electronic ID... because... it's just a way to secure interaction over the internet... so, it doesn't need to be related to control from the government and all that. We don't have all of that, an almighty government that can control everything. The presumption is divided between different state agencies, and everyones roles are specifically divided into what people can and cannot do. There is no, you know, all powerful person, or crook, who can control everything

AH: So you almost think, rather than Estonians being unique, that actually the UK and America in particular are unique because they won't?

I: So maybe... Estonia is using this (digital identity) a lot... the EU is going to over the years... the e-id legislation is not recognising that we should have mutual recognition of our electronic id's, and also ITU (the international telecommunication union) is promoting electronic ID in developing countries lot... so, i think the world is going in this direction, there is government provided security using electronic communication channels, just as the same way as the government provides security in the physical world... in exactly the same way... so i know, it depends a lot on lobby groups, opinion leaders and people who have these opinions on electronic ID, but absolutely i don't see that there is a question of total control by the government, its very easy to regulate... really really easy to regulate that no one has the power to control everything. In a lot of the political discussions, no one really has the time to go deep into the system and find out how it works *laughs* So that's why there's so much discussion... the right argument don't come out

AH: Do you think then that actually Estonians are more security aware than other European nations? Or actually, is it the opposite, and that people are less aware, but they just trust the government?

I: So I'm sure that in other countries there is less trust. The roles and responsibilities are divided in Estonia, in a way that it doesn't matter what the population trusts the government or not, because the system is decentralised. So i totally agree, that if there is no trust, people like to find other ways to do those operations. The need is still there. That's why all systems like blockchains and bitcoins came out, years ago now. But then the question is whom do you trust in this case? You trust the private company, and is that better? Or you can still trust a democratically elected government, so at least you can change something there. But with private business... i absolutely don't understand the logic that people are willing to put their trust in a private company whose only goal is to make more money, but they don't trust the system that is provided by the government. There is a contradiction in this logic.

AH: Do you think then, that citizens have a role and responsibility in ensuring their own cyber security?

I: I believe that is the role of the government, because single persons, simply cannot ensure the security of the cyber systems. They just don't have the knowledge, they don't know how to do it, they don't have the means. There has to be a more systematic way of making the cyber networks more secure. That's why we use this electronic ID. It's all about making the connectivity secure. This is something only governments can provide to citizens.

AH: Finally... it's sort of vague, but what do you believe the future holds for Estonia - and i say this in mind of some of your comments of wider implementation across Europe, and the interoperable developments with Finland and Iceland which are ongoing

I: It's hard to say what the future looks like, i think that the interconnectivity and the services that are shared by different countries... that's what we will see in the future. But i will say this, that i think the electronic ID and all of these measures... they were the influencers, or the basis to use the electronic environment, so cyber security measures actually made it possible to use a networked environment. So now we are seeing what different governments, what different businesses together can create... i don't know where it's going! But the possibilities are limitless. But they are limited by general culture in different countries, how much they want to cooperate with others etc etc. But the possibility is there, and the security is not a problem at the moment. So because of that, we're probably going to see all sorts of innovations. But the... i think, probably the innovation will probably come from the artificial intelligence side... and all of these kind of things. Robotics, 5G, connecting simply everything... so your toothbrush can be connected to the network etc. So i think we're going to see more connectivity, and more and more different services on the market!

Participant J - 29.02.2019

AH: So, my first question is always what does cyber security mean to you?

J: So it means the security of all my internet connected devices, and the device that are able to connect to the internet even when offline. So, the usual, book definition.

AH: and what measures do you take to ensure your own cyber security?

J: What don't I take would be the better question! So, i have two factor authentication, I keep my software on all of my devices that are connected up to date, uhh when i leave the house i shut the router down, surprise! ha, i use a VPN on all computers and all phones, so I also have paid antivirus subscriptions on each of the devices... and i avoid all unnecessary connections that aren't vital to the moment, so for example, if I'm not at home there's no internet connected device there... i keep the number of my devices to a minimum, and i also follow the principal of practising what you preach, and i also make sure that all the devices that are used in my family, and all the security policies that go with them and the hygiene rules are followed in my family, thereby whenever an IT person or a cyber security person comes over for dinner, they're not going to get on the Wifi until they have patched and updated everything.

AH: Do you ever use anything like a camera cover on your devices at all?

J: like this.... yes! I use it on all devices, on the one device i don't use it, i disconnected the wire to the camera... not this one (discussing phone) ... this one has a different cover, but since I'm about to change the security screen i managed to break because i dropped my damned phone, then i removed it... but it's gonna come back when i put the new screen on. So it's also privacy filters, and privacy filter for computers

AH: Can i ask why you use them?

J: Covers of the privacy filters?

AH: Well, i mean both

J: the covers, well thats for malware and cyber attacks where you can check in and spy on someone through their web-cam, if you want i can send you some cool links about what can possibly go wrong! uhhh and mainly i have a minimum number of applications on my phone, i actually only have four applications and i work for cyber security... and i only download from the official stores, and i know there are fancy things like supply chain attacks, like NotPetya and more... so if you go to the supply chain and someone takes it over you can inject some code there, and if someone has infected your devices with malware that remembers everything you do on a computer and you use Skype or any other video conferencing the camera light is supposed to be on... but this means that someone else can hijack the session and see everything that you're doing. What is really nice and protected about computers are on, usually when the camera is on, the light is on, that is not the case with mobile phones and tablets.

AH: So it's kind of an ownership thing - you have the cover so you know you control what can be seen?

J: Yes... and again whenever a crazy mind feels like i want to take the device with me to the toilet or whatever... which i don't! but there are people who do, and i feel really sorry for those people compromising themselves... but actually, a lot of money can be made on this on the dark web... so... good luck! I like my privacy like i like my meat; well done.

AH: Can i ask if you have any security concerns regarding your smart cards?

J: Uhhh you mean the national ID cards... or smart cards in the sense of sim cards on phones...

AH: So yeah.... so when i mean smart cards, i mean cards which have some connectivity, so yes absolutely the national ID card, but also bank cards as well

J: So, no contactless payments on bank cards... i already saw that question on your laptop... but the national card... i don't have any concerns... I'm fully confident in the people who developed the latest encryption, uhhh for the national card... and with the mobile ID with the sim card also... and also my phone cards... I since i know how much work has been put in there and which security standards and measures they must comply to, and what the security testing is then I... to Estonian nationally provided devices or cards that have smart card functionality, i have my trust in them... and if of course you're referring to the 2017 ID card crisis, ummm it.. if you've done some research on it... i was just talking to some masters students who wanted to do some research on it, on lessons learned... we've produced a 70 page document on this, on the vulnerability and what was done... it didn't impact only Estonian ID cards, but why it's such a big thing here is because we have secure logins everywhere that use these cards... so in Estonia we have approximately four thousand electronic services available to Estonians, and 800,000 cards impacted, so considering the population of Estonia is only 1.3 million it's a huge number... so.... when we take, for example Spain... where you have a couple million people.... well, I'm not so sure what the population is, but it's a lot bigger than Estonia... the number of e-services they are getting from the government is less than ten, so it doesn't really impact anything... so and in Estonia... i was still at National Cert at the time, and we discussed the possibility of the vulnerability and how it could be abused, but in the sense that you have an alternative in the form of mobile ID, so if you don't feel secure with the card, you have the two factor authentication... and if somebody didn't hold a grudge on you, and didn't have an extra 500,000 euros laying around and a couple of weeks to wait, so.... this could happen when you're the prime minister or someone very important an their signature is very important... but not to you or your neighbour... so... yes. In Estonian systems, i have confidence

AH: can i ask, what you think the key threats to cyber security are here in Estonia?

J: Ummm... the key threats, as in everywhere in the world... well, the attack vector is always the person. So the person is, and will always remain to be the weakest link. But, the biggest threat to Estonia is the high e-dependency, so we have everything online... and... so you were saying you've been here now twice, and quite a while... so the days this doesn't work... the ban e-services aren't working... it's a havoc and everybody is pissed off... even if they're not like usually using it... so it's the high e-dependency... and I guess you hear that a lot

AH: and what do you think is the link between the national level and personal level for you? Do you think your personal cyber threats are quite different?

J: Probably not any more... but i don't work for the government anymore!

AH: So you don't feel any particular cyber threats at all then?

J: Uhhh nobody is completely safe... there's no such thing as 100% security, there is no such thing as 100% safety... but I do know that uhhh being the spokesperson and incident manager at national cert... that put me onto some nice lists.... but now i work for an internationally known and recognised cyber security company, who write exercises for the NATO CCDCOE... so, also that puts me on some lists.... but uhhh... this... the best way of avoiding falling victim is good prevention, so always double check what a link is, double check, and then check it again before you send something

AH: Do you think theres anything unique to Estonia and how you do things here?

J: The unique thing is that first, we do *everything* online.... as I'm sure you noticed from spending so much time here, is that Estonians are really closed people.... so whenever you can avoid talking to other people, you just find the alternative... and we go crazy if, for whatever reason, things stop working! and this is actually why we do everything online... but what Estonia is doing very well is providing two factor authentication already, so with the ID cards in order to use it, you must know the pin and have the card... the mobile ID, you must have the device and know the pin, so it's basically two factor authentication that otherwise if you were using it for google or whatever, you need to set up for it to send you something via sms, so this is from different service providers located elsewhere. You get all of this here by being the owner of an ID card and a citizen

AH: You think these being given automatically builds a mindset and a trust among citizens?

J: Yeah, what else.... there's all government services, from the moment the ones in the last ten years, i can't recall one where you can log in with just a password and a username, or its limited functionality when you do that, so all our systems you need two factor authentication... and to take the ID topic further, when we talk about encryption of emails and documents, where internationally you would use end to end, so that the person you want to see it can only see it by decrypting it. So you take it from a national security perspective and Estonian defence league, where we have 26,000 volunteers who (sic - where?) by default, all the information relating to the association is sensitive, so if you send this information over the email, and even if the email account the person doesn't use two factor authentication or someone is reading those emails, unless they have the ID card of the other person and they know the pin code then they cannot open any files... if there's malware in the computer already, then its a different story of course

AH: Do you think the existence of the defence league is very uniquely Estonian?

J: Ummm... in this kind of sense... when we have 26,000 people.... uhhh i did these sums during a masters course... but it's something like 2% of the population. So pretty high

AH: And what in your opinion are the key security concerns?

J: Uhhh... people *laughs* ... people don't watch where they click, and fall for phishing emails too easily, but that's the same everywhere... if something.... uhh... what i've noticed in ten years of cyber security work... if something is advertised as 'click here and you may win'.... no. If something is advertised as 'you have won', people really click... so. There this. But it happens everywhere

AH: So you believe then that in Estonia that the situation is not that unique, and that threats are the same everywhere?

J: So, the difference in Estonia... to all other countries... is that the ID card is mandatory. So that what makes Estonia different to all other countries where it is optional. So a passport might be mandatory, but you can't log in anywhere. An ID card with a chip, you can... and, it really different between people because as you may know, Estonian, or Scandinavian banks they said no more code packs for the log in, so that is a security risk... but now half of the people complain you have to log in with the ID cards.

AH: Do you feel then that Estonian citizens are more security aware than other European nations?

J: Ummm, it actually depends. When you go ask that question in the big cities, and ask people what they know about security, do they know about two factor authentication, to always run updates, have secure passwords... the answer is usually yes. In smaller places, it actually depends... there are some rare exceptions where people have heard of these things, but sadly most Estonians... it can be said, compared to other countries, it's worse. They'll hear about some big data breaches... linked in, dropbox maybe, and they hear that their older passwords are available a couple of years later.... one of the most extreme cases i heard, someone logged into their account and when i was investigating it, she was using the same password she was using in her dropbox for everything.

AH: Do you think that individual citizens have a role and responsibility in ensuring their own cyber security?

J: I think everyone does. At work, you have the friendly IT department... at home, unless you marry an IT person, no. When you're at work, or school, whenever you have a problem with work property you can go to the IT department. You just have yourself to rely on. So cyber security in a sense is a shared responsibility, but it does start from individual control. If they're not paying attention to what is going on, and they click on everything that blinks and flashes, then it's a mindset... and when they say 'there's nothing interesting in my mailbox'... these people should sit down and hear some examples of what you can do just by taking over someones emails and the contents of them

AH: Do you think the state has a role in all of this, or is it very much an individuals responsibility?

J: Ummm... when i was still working for certteam, i did cyber security awareness schemes for regular people... I'm still doing that for one NGO, and ummm.... from the states perspective, what i think it the task of National cert, and their team in Estonia, when there's something going on in Estonia what i think they do really well is share that information. So for example, did you know that today, there are malware being circulated from university of Tartu emails?

AH: I was not aware, no! Fortunately, i don't have a UT email

J: It's just been sent out to ut.ee email addresses and it contains malware... and it was Tallinn last week, and it's often phishing scams as well. Here is the one from today *shows laptop*

AH: Thanks. Can i ask finally, what do you think the future is for e-Estonia? Or beyond Estonia?

J: I'm not sure about beyond Estonia. I think in future we should start better engagement when children are younger for sure. I'm sure you'd heard the legends that children learn to programme here from kindergarten, or in their earlier years? The sad truth is that they do not. I sometimes lecture kids on cyber security. The sad thing is, outside of Tallinn and Tartu, they know very little, other than sometimes how to report if someone is saying things to them online that they shouldn't be. In terms of basic security, they don't have the knowledge. I think this is one of the things that should be a future focus. Secondly, the people who are working, but not studying, we raise awareness campaigns for kids... but not those working... and if they want to attend courses, they have to pay. So I think it should receive some focus with the next strategy.

Participant K - 27.03.2018

AH: Okay. So the first thing I always ask in this is a super general question, I think but what does cyber security mean to you super general or temperature? You have some specific users a cryptographer. But when we talk about cyber security, is there a specific meaning to you?

K: Is it something more General? Yeah. I think it's the kind of collection of all methods techniques and to animal well of all for everything you do in order to make sure that there are no attacks on on your systems for whatever purpose be the purpose of stealing data of modifying data of disrupting processes or whatever. So any anything that is supposed to help against unauthorised attacks on our computer systems or computer in the general sense of anything than so specifically computers or systems or would you expand that out to Smart devices, but by computer I meant kind of any any digital Computing device.

AH: So what measures do you take to ensure your own cyber security?

K: So I mean there are certain procedures you do... All over so I know I mentioned when I was explaining things before this idea of cyber hygiene, you know, these everyday things don't mean to use things like a VPN anything like that. Yep. So I do make sure that I don't send any kind of confidential data what over uncooked connections since I have a better understanding than my kind of random user. I kind of usually know which kind of things I put so I don't lose for example a VPN normally because I know oh I see whether web connection is encrypted and so on so I don't have a systematic approach but I if I know that something is unencrypted then I don't use it ... for example for something involving my password. Additionally. I have an encrypted hard disk. So if someone physically steals my laptop they cannot get at the data from itI am also aware that I don't do it perfectly. I mean, I was just an example the hard disk encryption that leaves still the what's called what the name holder text or something warm water takes something like this when they are takes there were people studies take a laptop. That's the running and take all the memory like the not the hottest but the actual memory they they cool it first then take it out plug it into a different computer quickly and can still read all the data on the on the memory. So I'm aware that there are some effects. I can't protect myself again all, that begins only with very big effort. So I don't do that. Yeah. So this is the exact opposite, you can't be 100%. But yeah, I'm quite aware and using an encrypted browser for example, and you're browsing the indwelling more sides nowadays do it do it. Anyway, so there isn't so much to be paid attention to but for example, if a site would have a password field and we're not a couple game nowadays the browser's also warm, but in those cases, I wouldn't put my password now, but sometimes I just have to also make make a compromise that there are certain things where I know it's not perfect security, but it's too hot to make it work. Yeah, you can't ever be 100% especially if it depends on others... so for example, if I feel that a certain service doesn't do things right with my password, but I can't change that service and not some so service and we talking about social media perhaps here or what social media might be an example, but also for example either Rome. I'm so why I one problem I have is that I you would have to use the same password for a Jerome as I use for logging into all other University Systems and I consider this a weakness and I think it should be different password for all I don't want going to the reasons but I I think this is not a good choice the administration who administer that things it is an Overkill and therefore I have to live with that. Yeah. So that's an end. I just do it in instead of saying I won't use it or not at all, which would be very big drawback. I just say okay just accept that there is a weakness and then yeah if it goes wrong then I told you so kind yeah.

AH: Do you use a smart device? Would you use a smartphone?

For example, very little they may I have a my my normal form. It's old school. So I think technically speaking it is a spot home because you can install some very simple applications on it, but I don't think you can find them anymore... So for practical purposes it's not a smartphone.

AH: Is there a particular conscious reason you've made to have a phone like that rather than using a more modern one.

K: Yes. Although it has security Blanchard has to of course because you are saving against all the model attacks because they are just made for more modern fonts. Yeah, but the actual reason one reason is that I don't believe in throwing something away with it still work and just replace it because there's something somewhat improved forum

for that's one reason also modern phones do not beat this form in all aspects. For example battery life. The charge this of like well, I think by now it's gotten a bit weak, but I think it's still somewhere between one and two weeks.

AH: I mean I'm lucky if mine lasts two days.

K: Yeah, so of course yours yours will use more. So if you have would not use it, it will probably last several days, but I don't think it will. Yeah be able to compete either so there are even technical advantages and thirdly I don't actually use my phone very often anyway, so of my don't have it open or it switched the sound is Switched Off so which is a reason also independent of security but more in terms of trying to avoid being dominated by technology. So having a phone that is less fanciful makes it easier to when I'm just leaving home to be disconnected and do not be like addicted to things like social media and so on. Yes. Yeah. I'm aware of that struggle as well. So you make a conscious decision.

AH: You just you don't want to that's that's interesting. I was wondering actually I notice you've got a webcam then I don't know if you noticed on my laptop so I can use a camera cover on here. Is that something that you use at all?

K: I don't I'm sometimes wondering that's all for example. This webcam show a light when it's recording. Yeah, but I'm I don't know how this internally managed if the the right thing to do. It would be that the camp that this camera physically switches on this lamp whenever it accesses the thing, but it could also be that they just made it the simple way have a driver that has tells to come on off switch on the lamp which is independent of the recording and could to be circumvented. I don't know.

AH: So, yeah, so supposedly with a Macbook there's a little green lines here. So it's not over the moment the lights of the supposedly. Well, I believe that it switches on when it's recording,

K: but the question is on which level is this implemented? So if your operating system makes sure of that then something that some malware that has taken over your operating system could just disable that feature. Yeah on the other hand if it's something that just built in like there's some electric circuit that cannot connect to the camera without switching on this lamp. That would be a reasonable solution in my eyes, but I don't even know how to find out fear. They've done this. Yeah having personally for me I was actually giving out of the conference but I think I probably would investing one anyway, and I think for me it's like having an ownership over it because I know you can't see anything if that's all over it. I mean I've seen a lot of people government departments where they'll just have like a plaster or yeah, that's another sticker over that as well.

AH: Do you do anything with the microphones - use a mic blocker for example?

K: Well actually dubious that it would work. I don't personally have one but I'm not sure that again for similar reasons so many plugin for example of a physical microphone and then the computer switches to that microphone, but the question is is that the like really physical connection or is it just that the operating system is told hey now they have practicing in please switch to the other thing because I know that my computer and turn over the microphone, but I think I've had situations when I plug in a headphone and do to somebody or something. It was still going through the loudspeakers.

AH: Hmm

K: The same thing could work the other way around I mean with the microphone as well. So again, I would only trust it if there will be some real physical switch for it. Yeah, but you do have one in there or do you not have a microphone in your computer at all? And there's Mike well as Mom in the webcam for example, so that's again the case of I don't really have I mean I could disconnect it. Yeah each time I reconnected whenever I have a call now, but that's kind of so annoying. Yeah, I would be a proper switch. I might prompt possibly use it. Yeah, but right now because since there's not a built-in feature to automatically disable one... i've seen people manually remove the microphone and use headphones with a microphone in because you then have the ownership of when you can connect and disconnect that but the only way to actually disable the one in your phone itself is to actually pull the hardware out possibly a little bit too far for me. I just don't think that I really want to do that. But yeah, I've seen it done. Let's things that might at least think about them might not do it. I mean, I've also thought about microwaving my ID card at some point down to kill the chip with it in terms of the Chip. Like I mean, I haven't done it but I mean things like that passed through a my mind

AH: well actually brings me on neatly to what I had to ask... So I am interested in smart cards as well and some of the security concerns around them is it's very interesting. Would you ever consider using an ID blocker? I'm sure you've seen them online, here's an example of one.... You can buy the little sleeves, and you can buy wallets that supposedly block them. Is that something that you use or would you use?

K: No, I don't.... And again, I'm aware that it might be used to kind of track me and so on. I don't know whether it can be practically used for for example stealing valuable private information like from my passport, but I don't carry it around usually. Yeah, and my ID card doesn't have it. My credit card does not.. I'm not sure what distance it works fro,. I mean I have to be put on this device the door the card for the door for this building has it and then what is is a bit farther distance with the current record car because the credit card I have to take all of my wallet from effort a while this thing. I usually have to cut in one of the auto focus of the backpack and I just turn around I know what you can do that with the transport cards here as well as I'm telling you it happens that the sensor or downstairs exactly the same height as the pocket of my backpack. I just have to turn it on and kind of move my back. It's quite convenient but secure? Yeah. Well, I mean at the end of the day, it's just to the building.... That's also the thing. It's the same with my banking for example, if someone could steal money from my account remotely... Well, they're not getting a big stealing... and I will probably notice it and then probably complain with the bank until I get it back, because it's a technology that's messed up and you think you can pay only 25 Euro anyway.

AH: So this is leading on perfectly to my next question because it was going to be do you use contactless payment. So you do?

K: Yeah, but the thing is that I think that the thing is that whether you use them or not.

Is that your another for your security? I think because the question is whether you have them because if you have a cop that can do it and you don't use them. You still have the card that can do it. So all the threats are there whether you do it or not.

K: Yeah, I mean I also see those concerns. But again, it's also the bank never asked me. Yeah, if they would have asked me. I don't know what I would have said yes or no, but Jesus would you bank with an Estonian Bank? Yeah, because I've heard different also the German bank and even by any credit card from Germany, which also British ones have them as well, but I was led to believe by some people being forced to marry bank to bank here. Sometimes you basically you have to actually request these contactless cards, but I don't know if that very well perhaps perhaps if you don't have one without and you wanted update it. Yeah, that's then. I mean it just happened that my cart reached. It its validity date. Yeah, and they issued me a new one and that happened to have the contact list feature. So, I don't know whether what you were told was really about going to get a new car.

The directory busted over here just means if you don't have it yet and you want a new card issues with the feature? Yeah. Well, I was told that you had to actually specially requested. I thought that was unusual because in the UK they are issued automatically. So every card is contact us now pretty much but you can request the bank to turn it off if you want to yeah, but you wouldn't use an RFID blocker

AH: I appreciate your not Estonian, but obviously, I'm sure you're aware of the security context here. I mean, what do you think the key threats to cyber security are in Estonia?

K: As opposed to another place as it was opposed to your own personal cyber security as areas because there's what I'm trying to pick apart is this differentiation between priorities of National Security and the perceived threats and then actually what matters to you know everyday people because I think it's a bit of a Divergence. Yeah. I'm actually not sure. I mean what whatever have met us to every day is people is of course also a console. So I think the government has the job because the everyday people cannot understand. I mean the main understand what they were protected but you that is tricky but they certainly are not the ones to find out what measures to take for that because if they don't have the expertise, so that's something that I think is also problems the dominant but besides that there's obviously also the kind of cyber conflict kind of respect I'm down. I don't really know..... How relevant that is, it's much less of technological issue than a political issue. Yeah to tell about that like How likely is it that the mother government is actually using this thing. I know that the possibility is there and I don't know do for example the Russians

do it all the time. Is it likely is it like that? They don't seem to be afraid to be... to be caught in the act and so on all these things are very relevant and totally out of my knowledge.

AH: Yeah, no still do I think you've touched upon the key concerns and one of the things that people sort of the idea of hacking and the Russia might bring down the government systems are common one obviously there's a legacy of that because that did happen in 2007. So I mean do you think that the use of these digital identities and obviously that the technology behind the mix Estonians feel more secure. I mean, I know I do you use a digital card here yourself on occasion (that the one you're going to put in the microwave)

K: but that doesn't make you feel more secure than in all the opposite. I mean having a digital ID that you can use online and so on it's a plus for convenient, but it's kill you - for security and I said, I don't see how this can make anything more secure because I mean if for no signing a contract I have to go to some new terrorist or something. That's quite annoying but no one can send me my with it does it for me? Yeah. I mean you you know that the its probably being done above board. I mean, I feel like I've been early you stored your showroom. I don't know if you ever have been at some point but they're very proud of the only things that you can't do in the store you digitally I believe a sign for a house and get married. Yeah, but basically everything else is fair game online.

AH: So you actually think you feel that that process is less secure because it's online and it's very much a convenience?

K: Yeah, so I think if people say that the ID card or something makes things more secure first are twisting things. I mean depends what you compare. You should compare a system like everything online but we don't have an ID card for securing was obviously having the ID card and everything online is more secure than not having the ID card and everything online because then you would need to I don't know fall back to things like you remember your password and you have to use the same one also for and glue it on your fridge or things like that. So that's the comparison then it's true. But if the comparison is having the ID card and online service for the weather's not having the ID card and not having all those online services, I don't even see how one would come to the conclusion that it's easier to hack a service that doesn't exist again because I mean, I guess they think the issue is maybe your personal ID... We join them thinking about the e-governance system and I mean that the one that comes to mind is Medical Records, I guess so say they're not online you get that you still have to have a medical record. So in the UK a lot of them are still unclear but they are gradually no one can make a mother to get it to just or at least of what you would have to I mean there may be already in the computers of individual doctors offices. But well then you need to help you find that doctor's office hectare in and so on. So there's a lot of practical inverter advantage of having a centralised medical office data, but it's not a security Advantage. So you have to just trust the relationship with everybody who is involved, whether it's whoever's maintaining the it system ,or whether it's the individual doctor in their office.

Now. This is the thing is if someone I mean when I'm going to the doctor and I'm handing out giving them my ID card and model for putting in some possible that they can access my data or something. So that means that probably anyone who has access to the doctor's office and borrows my ID card can ring up my medical details day.

AH: Hmm. All right, but you stood so the whole justification of this system is that they use technology which notifies you if your data is accessed.

K: Yeah, I mean I basically because of the system itself. I don't know which doctors are looking at it. But I think the meant the biggest use at the moment is pure trust... I mean, the e-governance thing, it's very slick, and they are good at giving evidence. If you go to a governance office, I think that's the best example of PR.

AH: Do you think there's actually something unique about Estonia or Estonian mindsets that makes them more willing to accept this position of this technology?

K: I have the feeling. I don't know what that it's it's it's kind of true. It's just a gut feeling whats is behind the this willingness to the depth like e-governance and then ID card ... I think it's there are two reasons... one is a feasibility if you are small nation.... It's just easier to do it. Yeah, so that's a very practical reason for a reason.... but I think the other one is more of national pride reason that if you are very small country. You have to prove yourself. Yeah, I mean in the same way as estonians are considering more worried about for example language issues like that.... The language might not be preserved enough. Then English people will probably have I don't think you will find much Eng-

lish people who worry about English language dialogue. Exactly. So if you have this threat of dying out in a sense of your own of going of becoming insignificant and my feeling is that part of this is that you adapt these kind of Technologies. So for example, Estonia was very very proud of we are the first one to have IT. We have we have e-voting because it's useful but

We have we are the first that is the end of the big thing and I feel that that's kind of the main reason actually. Yeah that it takes almost a selling point.

Of course people will try to make it as secure as possible, but it's an impossibility to admit if you can't do it, like if there's a problem such as the ID card flaw... and Yeah, you can't go and it's distracting Estonia is in the situation that they cannot admit the system to be not top-notch.

AH: Yeah, absolutely because they're sold themselves on it. Yeah. I mean this does tie into the next question is well, we did you think that Estonian was are actually more security aware than most of the European issues by having for example, the UK or Germany. Do you think Estonians are aware of their cyber security or actually do you think on the flip side that they're actually too trusting whether you know, I have no clue on the security side specifically but a related area I can give you feeling namely the privacy concerns, which is not exactly the same. I mean one is the like it

K: It's like us and the others is against throwing my data around to let you move to the reporters who then do possibly some people don't and comparing it with Germany where this before I think Germans are considerably more sensitive to these issues. Also the government as much more data protection laws and so on. So my feeling from being here is that this is all handled like very kind of color. So for example in Germany, there are these rules like if you have a company and you have some account accompany you to your contract stops. There's a time limit a relatively short time ago a few months by then they need to do to raise your data and all those kinds of things like that. And I think Estonia doesn't have much in that respect and also sometimes when... I mean many of the other scientists talk about. Yeah, we want to do this study on the mobile phones and then fit it sounds like I don't think you could have done that study in Germany because you would just have gotten stuck with the fact of having to use this much data without the a possibility to ask a re-envisioning. Of course, they are limits but they seem to be much softer than they would be Germany... Yeah, and I guess that I mean that's more something which I observe about. What is what the other processes and regulations they seem to be much more relaxed. But I guess they wouldn't be so relaxed. If the population would be with more fearful about the data privacy. Yeah. Yeah.

AH: It just seemed to me that they just have this establish trust and I can't quite pin down where it comes from... the recent past perhaps?

K: That's a good question because the communism is not something that would build h much trust, you know, but maybe they used to being watched and therefore they feel the people who are now watching the my more trustworthy congressionally also not clear how much this affects the younger generation who grew up Post-Soviet. So there's a big difference between people who grow up Soviet and those who engage in everyday Behavior. Also, I think so my girlfriend claims that people who grew up in Soviet times. They are much more distrusting also distrust not just to get the I distrust against your neighbor and against so kind of being careful that you're not cheated. He's kind of attitudes seem to be something that are bred in by the communist regime regime. Yeah, so she's actually doing research in areas like that. Oh, I'll be fascinating. Actually. She researcher talk to us. No, she finished her master and she's trying to go.

Saint Andrews oh, but there's trouble with the funny hair easiest position but no funding. Yeah. Hello. We it's not clear yet on this one. Yeah. Well, good luck Koosh. Yeah. It's a great universities and under is as well never personally being but he's got a great reputation. But and we fascinating.

AH: Yeah and my final question. I'm sorry for we've run over a little bit on the time the final one is do you think that citizens actually have a role and responsibility in ensuring their own cyber security or on the flip side of that? We think that it should be that we should trust the processes and the technology behind it or do you think it's the government's

K: I think it's the government who has a big responsibility also because failure to do proper cyber security on an individual level often does not affect necessarily the person who does it. I need a little bit perhaps but It is not that if I if I would run around and not have any passwords and whatever what would happen to be personally possibly not that big a drama you have two cases, but perhaps some date of that someone else the same. I mean if I would just take the attitude. Okay, I don't think you're anything but I don't keep any because I have nothing to hide. Yeah. Well someone

else by Saving send me something that's confidential. It's also so failure to paint. And also if I get a virus, I increase the probability with other viruses and cancer. I see this a bit similar aspect like this vaccination because vaccine and if I get vaccinated this is not something specifically for my health. I mean it helps minor but it's also important to ensure her community. So if I don't vaccinate I am actually damaging endangering the health of the Society of all to contribute.

It's damaging it which is an argument why the government has the the right or the responsibility to make monetary vaccinations? I mean it's is not uncontested. But yeah, that's what is my command of the argument. Is there while it with something else the government may not have the right in my view if it's just about something that will make me personally sick. Yeah, but I want to be sick. Yeah, I have to write to be sick as a free citizen. Yeah, I mean seatbelts and so on again something Well, which yeah, I have the right to be Reckless, but then I suppose the flip side of that is you could hurt someone else as well. I don't know risking my health.

I damaged the budget of the I mean if I if I break my bone, it costs actually the all depend whether it's the government or not depends on the particular system, but kind of the government or something similar is actually paying for my increased Health costs. Yeah, so these are all on you but back to the service of you so it's a bit like the vaccination thing. Yeah. If I don't do provide cyber hygiene this Dimensions others as well and the in these kinds of settings. I find that this is exactly the things why we have government's when when actions to regulate actions, which are marked where people are not damaging themselves, but damaging people around them are so encouraging people to take responsibility on Earth.

Communitarian basis whereas IRB maybe you don't care because you only you have anything to hide but then actually if you laps with this and another people are laps with glittering as mother is also an example. If a litter of course the place where it just littered is less pretty but if but the the damage for me in terms of Hope or less pretty the city is by one chewing gum that I throw on the ground it's worth the it's worth the avoiding the trouble of finding a treasure but the community effect is damaging therefore we have rules against littering so you could see it in and that and I've been really interesting way of putting it actually because I haven't heard anyone describe it like that yet and you're right and I forgot what the name was but there was this argument exists also on the company level because they are you have this I think even more strongly

If one company doesn't pay attention to my data this may not damage that company as much as it. Kind of because of all interconnected. So they are personal damage by not paying attention to security is what is basically limited to their overall value. Yeah, they can't lose more and if it's something that happens occasionally but temperatures them only to a limited extent. I mean, for example, they are sometimes these cases like company loses millions of passwords. Yeah. Well they are own damage is pretty small in comparison to the damage.

Participant L - 31.10.2017

AH: What does cyber security mean to you?

L: cyber security is a road set of actions... it also covers privacy issues... if i am secure... cyber secure... it means that my data and personal information are secured...

AH: do you take any measures personally to ensure your own cyber security?

L: yes definitely it's... I'm permanently looking at wireless protection and whatever... and workstation security.... I'm making sure that in my own ocean a measures I have in place... whether it's a firewall whether it's somebody's responsible for the cyber security activities on a daily basis... whether it's internal, or a contracted company... and also got my staff are aware of what is going on and how it works... what they can do what they can't do... how they should behave... just to do as a coincidence we had some cyber security training.... not too much practical but just making people aware of what are the latest cyber risks and has cyber terrorists criminals hooligans are acting... the latest phishing techniques, making sure you're not responding to the wrong emails and so on, and what is happening... how your identities can be stolen and so on. so this kind of stuff.

AH: so you have regular meetings in the department to make sure everyone is up to date?

L: Yes... or at least we are trying... of course our organisation is perhaps dealing with a little bit more than a regular organisation so... ummm... we are maybe disgusting in more as part of the daily basis we share the latest news and so on but anyway it is about humans.

AH: could you maybe describe the Estonian approach to cyber security? I know you've already talked about education keeping people up to date and also the human side of things do you think there's a particular focus on this in the Estonian way of doing things?

L: I think there are definitely some social and cultural issues that... you know Being Digital means not being Soviet somehow? I think especially for younger people it's an identity thing you know, Being Digital... doing everything digitally and selling to the rest of the world... also have a pragmatic approach... you... it means you don't have to go anywhere you know.... you don't have to sit in an office a government office, I wait in a queue.... so it's a really pragmatic approach also

AH: like service-based you would say?

L: yes exactly We can't be bothered with waiting for officials to have time for us you know... *laughs* ... but it's all connected now to cyber security in the sense that we consider by default that these transactions we make must be secured. and the cyber security element is an integral part of this... I think this trust aspect affect many kinds of internet services... all service is not just online government services.... it comes from the end of the 1990s when I first internet banking services were appearing... so the biggest bank in those days was Hansa bank, these days it's known as swedbank... they made a lot of innovation and they were really pushing people to use internet banking... it might be a cultural issue but I think in Estonia people think that if they can do financial transactions online and your money is not lost in that transaction, no one is stealing it you know, so after that, the it's peanuts you know.

AH: so you think once people were more comfortable with this financial aspect the governmental side was easier to introduce?

L: yeah yeah exactly, you do your transactions online and you see that your money is still there, or I can transfer it and the other person receives in the telling you that they have received it or you can get it from an ATM or whatever so this built Trust. I think for estonians Trust Started From banking... I think even in the cases where money has been lost online banks generally recover it and through this process this is built Trust. something like that. think that the government has made all these online services for Citizens in a secure manner so other people are really trusting of these online services.

AH: do you think that the governance and all of these online services have actually made Estonians feel more secure then?

L: I cannot see more or something like it, but I think trust in the perception surveys for example, the European Union is doing, you can see comparatively that the trust in government institutions in Estonia is pretty high, and I think maybe it's because they don't have to actually meet officials... *laughs*

AH: so perhaps limited interaction face to face is a good thing?

L: absolutely perhaps you're more likely to be upset if you meet somebody and things aren't resolved as you would like, or they annoy you... it's harder to blame the government online... it's like you have to finish this f***** application form, and there's no one else to blame but yourself if it isn't done....

AH: so the onus is on you as opposed to the person behind a desk

L: yeah yeah, most of the online services are pretty well organised so always it could be better but pretty much most of them are good and acceptable to people.

AH: what do you consider are the key threats to Estonian cyber security?

L: as usual the main threat is between the chair and the desk.... it's the human... so failures tend to start from Small Things... you know the classic example of people picking up a flash stick from the street or one they've just found and then sticking it in the computer..... and infecting the system.... or someone in an ICT department just ignoring the rules and doing whatever updates ... But like the recent issues with the ID card the problem was not that something went wrong... now everybody has updated the software to fix it anyway... but we had to make this understandable on easy for the public so they didn't think it was too complicated to do this it has to be convenient. they don't have to go say to a police station to get this sorted out, you can do it easily yourself.

AH: so you have to cater for the human error aspect?

L: Yes... I don't have the clear statistics around it... but we can see how often people are using their ID cards and what the overall picture is... but ok I use it on a daily basis. granted I'm probably not one of the risk because of what I do. the less frequent users... makes it more difficult.

AH: ok so the type of threat you are describing seems very different to the 2007 attacks and the denial of service that way

L: Yes so the smaller scale attacks happen more frequently I guess. but we reacted so what happened in 2007 and learnt from it so we have secure backup data and we also updated our procedures and we're generally more aware

AH: so the backing up aspect is what has inspired this data embassy idea right?

L: yes exactly and this also provides physical location outside of Estonia's borders. so I face the same kind of risks digitally as we do with physical records of course, so paper records in the past could have been threatened by the potential of, say, the building burning down... If anything backing up these things digitally is easier. I'm not so worried about it I think the guys that are dealing with these things are doing it properly, and it's beyond my control, so I need to believe it's ok.

AH: so when you implement these new services do you ever consult citizens?

L: so sometimes we can sort with private companies and consultancies of course to build up feedback from ordinary citizens... also whenever a risk or a threat appears we make sure we publicize it to make it relatable to Ordinary citizens and make sure we communicate with them as well as possible... sometimes we have to be reactive to new threats. but we're very open we don't say to government secret... and also just the final mention of this ID card software, it was pretty openly published and perhaps in some aspects we overreacted, but it was publicly discussed so everyone

can ask questions and the media was very openly involved in it. We're also permanently working with the younger generation, with kids in school, and we start so early, once they get a 7 or 8 years old you wouldn't believe the level of knowledge.

AH: do you think the Estonian government cyber security strategies are closely aligned with citizens security concerns anywhere then?

L: I think it's been very open... cyber security is a strong part of national Security here. it's becoming more and more so a part of national Security because it's not that someone is just attacking your computer, are stealing your data, but they like water networks of power stations... so the dangers of this are also communicated... people understand it but I don't think anyone's panicking. perhaps make with other countries when talking about normal security, it's part of the game and we have to be confident in her own strengths.

AH: Yes and as a unique historical context there no? so different places have different priorities?

L: yes so in the US and the UK of course there's the Legacy of terrorist attacks something which isn't really a problem here... it's easier in Estonia and we're discussing it... it's also not only cyber attacks... in it's almost is sort of Media War... the use of social media... all those trolls and so on.... all this is part of a game and it's discussed more than actual cyber security, or cyber attacks per se. so thinking about these recent attacks that have come out of Ukraine... I can't remember the names exactly (NotPetya)... Anyway it was discussed widely and a big supermarket chain their systems were brought down for 3 days here because of it... they were part of a French company... so they get it from France not from Estonia... *laughs* but what is maybe the issue... disclosure is one of the more visible... you know effects of a cyber attack against the company. but Estonian companies generally I would say feel pretty secure... perhaps generally they're too small so they don't think they would be targeted... but we have to remain vigilant.

AH: I wanted to ask regarding Mobile Technologies... so I am interested in the internet of things and connected devices and how this is changing the security environment. is the Estonian government doing anything to account for threats coming from connected devices?

L: yes mobile threats are not as discussed.... private companies are working on there but I'm not aware of how successful they have been right now. so I know there has been some issues with Android devices accessing our services... apple devices I can see the little more secure but they're only around 20 to 25% of the market share in Estonia. things could be better, can you still can't vote from a mobile device for example, we don't think it's secure enough right now. who knows in future. so just today in our training the guy delivering it was saying how many attacks are coming from mobile devices now and specifically targeting mobile devices because why not as secure as we could be. the main threat through mobile devices is your own personal data and private networks. we make sure people are careful when accessing things like public Wi-Fi with their mobile devices for example.

Participant M-07.03.2018

AH: What does cyber security mean to you?

M: Well... I think key aspects are privacy and integrity of data are very important, but nowadays its full of government and national approaches, not only the technical side, but also coordination of statecraft and management policies.... moving todays a national or state perspective or view.... if you ask me personally.... i would say.... it's many things. It's not only state-level policies and how to organise it.... it's not either only security of your devices.... umm... i think it's you know... I don't have a definition, I think there are about fifty different definitions.... but some of them are better than the others.... but ummm... i would define it from my work or professional point of view.... it's one thing. On my individual level, it's different. Maybe it's less technical.... it's data protection, protecting my devices.... from the governments perspective, it's sort of how to manage this... cyber defence.... so i don't know that I can fully answer your question!

AH: Well, I think you sort of have in a way, it is undoubtedly complex and contested... so you're saying you think there are two levels almost; personal and national? I guess as a quick follow up, i'd like to know if you think these are two different things?

M: Well they both have technical and non technical aspects... I think it's different viewpoints... if you have cyber security, it includes information security, data security, uhhh policies... maybe it's a different kind of things that are in there... it depends where you look, and what is relevant for you...

Just to add.... perhaps a helpful way of looking at this, is what is 'cyber space' you know... people, technology, places... you secure that... and whether that... its kind of the process... i think it's the process, to give a very broad view of how to comprehend it

AH: And can i ask, what measures you take personally to ensure your own cyber security?

M: Well... at work we procedures... but me personally... for me it also comes down to convenience you know... uhh of course i try to use 2 factor authentications.... for services.... i know SMS is not secure.... so there are limits to what you can do.... I'm careful with what i download, i don't share map private data.... some of my colleagues, some in and some out of cyber security.... i would say they are paranoid *laughs* they won't even use a smart phone! I will say, though, as an Estonian... I am not *that* concerned about my privacy than perhaps older generations of people... i would not use an app that shows what you're doing with everyone... but I do use iCloud to back up things and my personal emails are there, my folders are there.... i know many others who would never, ever do that....

AH: Do you make hard copy back ups of everything?

M: *laughs* not as much as I should

AH: Do you think you accept that you can't be 100% secure then?

M: Yeah sure. So it's usually referred to as resilience right? So at some point, big companies and so on know they will be hacked, so have procedures in place... and even on a personal level, i know my data can never be completely secure. Everybody assumes that not everything is 100% sure.... there's a difference when we talk about things like our e-identity.... we are pretty sure in general that we have the confidence because of measures our government has put in place... and in a way, the e-identity card crisis was kind of something, you know a wake up call for many. Ok, it's possible that you could actually access and fabricate documents.... but umm... i think people. Maybe... there's no statistics.... but i think people have started to think about these issues more. If we take into account the development of different things.... quantum computers etc. So we think about the development of things... everyday internet use. I think people realise it's not secure. Things like digital banking, they think are secure, otherwise you wouldn't do it... and in Estonia it's pretty secure, you know we don't use those code cards. Actually quite a lot of old people are using

the old systems according to a recent Swedbank announcement, but it's being made obsolete, so those people will now have to learn how to do it using an e-ID card.

AH: So one of my follow up questions in this.... I mentioned I have an interest in the Internet of Things... I mean, obviously that is huge, and there are varying definitions of what the IoT *is*, I'm generally thinking about our everyday connected devices, like smart cards, smart phones etc. Can I ask if you take any security measures with your smart devices at all? Your bank cards, for example, do you use RFID blocking sleeves...

M: Actually.... so me personally? No, i don't have a contactless card yet. I think in a way I'm kind of conservative as well, for example we have those smart cards from Swedbank... so it's kind of the same chip I think. I didn't get it yet because it's easier to log in, and I think there's a limit to how much you can pay with it.

AH: Yes, I'm told they're 20 Euro here. In the UK it has gradually increased over the last few years, and it's gone up to 30 GBP. My card has it, but personally I use apple pay instead when possible

M: Yeah so I think you need to opt in here... right now, I don't really want one... I don't trust it... but I don't know, if they just sent it to my house, i'd probably start using it *laughs*

Also there is the potential to track your movements or paying for things with your contactless card, we have similar things in Tallinn like your Oyster cards in London, and these can be linked to your digital identity cards. so the potential is there.

AH: yes in the UK we are quite resistant to the imposition of ID cards, but then we all quite happily use an Oyster card, and some of the issues people have with ID cards can quite easily be levelled at Oyster Cards also.

M: yes I think Trust is key.... if you look at the cultural the Social and historical aspects of had this was built in Estonia these are important. in 2001 we introduced this digital signature act and there were no major attacks you know you look now and everybody is concerned with major data leaks, cyber criminals, hacking... the awareness is much higher than it was then. at that time 2007 was Yet to Come.... I mean even the US didn't introduce its first cyber strategy until I think 2003? so there wasn't really the awareness... it was more that we had no Legacy technology and we needed a new one... because we had limited resources we were able to cooperate with the private sector... a lot of this knowledge came from the banks... it was companies like cybernetica ... and we started to use this blockchain technology and banks accept this... the government guarantee that everybody would have one... and in the beginning as I remember and I think there are some articles about this, not everyone began to use this immediately. yes it was mandatory but electronic used was fairly low, so people thought well I have a passport already why do I need this? so it started because banks accepted this and then it was realised there are other things that you could do with this, like the tax authority using it, so you can do your taxes in 5 minutes. some people saw that it was beneficial... but I think in 2018 if it wasn't already in place you couldn't if you didn't already have that... I think now it would be very difficult to establish this. the other thing that came to mind when I listen to your introduction was trust and security and individual security and also how these things are different in the UK and Germany for example... people see the government as something to oppose... here I think it's related to are geopolitical situation, because we are concerned about Russia... so we tend to trust our civil defence forces or police, and even the Estonian Defence League, even if trust in the political parties themselves might be low... or lower.

I think also the 2007 experience... the systems can be abused and a target. so I think in this sense yes we trust government vis a vie Russia, to take care of a physical security... and I think this translates into Cyberspace as well. so we trust the system as well because we also know it used in banks and the private sector... the private companies actually established it.... I think it's a bit more grill when it comes to internet elections and e-voting... it's down party Lines, like the central party, so they have opposed this because they do not get many votes this way. So I don't mind it but it's not totally 100% secure. voting is something different to me, it's not an E service. it's the basis of our democracy... its kind of... well it is critical infrastructure... so it requires extra security, and we need to be able to protect against people interfering in it or altering votes. for example in the US I think there are two or three states where they don't have paper copies as well... they have the electronic voting machines... so I think it's a fundamental and philosophical issue... so whatever system you have you explain to people how it's used and how it's done... so... I mean I'm sort of one side of paper... but of course it's possible to steal those papers... but there are checks and balances...

AH: so to pick up on one point you mentioned there... you talked about trust in government institutions... and I noticed you mentioned Russia as well which is a significant perceived threat... Do you think the existence of this threat, perceived or otherwise, effects how likely is still onions are to place trust in their institutions?

M: well there's no kind of quantitative statistics for this... I think if you think about offline and online it's not two separate worlds you know... if you think about the Internet it's kind of a mediator for social interaction but of course technology brings new potential fall backs as well... I think you also need to look at the geopolitical concerns and it's not only business or economic... you need to look more broadly and see the social and cultural context... I can't really relate it exactly but I think in general the government is trusted and law enforcement as trusted here... it has to have an effect on this as well... I think it's about timing as well like I said before, I think right now the concerns with privacy are much higher. especially because there's more knowledge about it. there's also been cases in private Media, which have reported abuses of privacy, which have raised the public's awareness of these concerns.

AH: so you think gradually estonians Have Become more aware?

M: Yes but I don't have the data on this, it is just a suspicion or an observation

AH: so just to briefly go back to your own personal security there, do you use a camera cover at all on your devices?

M: I do yes, the sort of started many years ago... I think in 2008 after the Georgian case which was widely published everywhere...

AH: any reason why you decided to start using it?

M: well basically given that there may be malware in my computer... I know it's possible to hack the camera... and I don't want anyone to see what I'm doing... so it's kind of silly... because of they were going to hack my computer there would be more valuable things than being able to access the camera and see my face... but at least there's some reassurance they can't.

AH: does the microphone bother you at all... and the potential for hackers to take control of this?

M: to be honest I've never really thought about it... and I also have no knowledge how to disable it but yeah I can see why this could be more of a concern than the camera been taken over... so it's interesting you go to conferences and they hand out these camera covers and people talk about them but nobody really Focuses on the microphone... probably because it's not so easy to do It's also convenient you know because I use Skype every day... the camera cover is easy to move... the microphone how to block it... it doesn't seem so convenient... and you also want to listen to things all the time as well so if it interferes with the sound... that's a problem.

AH: yeah I mean I spoken to other people and the cover it's almost like a comfort blanket but it's also showing that you're aware of the existence of the Threat your camera can be taken over...

M: yeah I get that it's a status thing too right... showing that you know what you're talking about

AH: I was wondering then... what you thought the key threats to cyber security in Estonia were... talking on a national level... and also on an individual level

M: I think state sponsored offensive activity is certainly a concern.. espionage or attacking key infrastructure... ok so people say it's not all about confidentiality or availability, cyber security is all about integrity. so the potential to change personal details if your account was hacked, so your blood type... I think all of these are relevant... so I think maybe the main threat is that we actually with so dependent now on these ID cards... so we should have alternatives or backups... is everything is based on this and if something happens.... so it's not just the card it's the services and the supply chain... we had the issue with the chip... even if you take card payments, if you take that as an example, so there are backups in other countries... overall ok *laughs* I think I would say it's are increasing dependence on cyber matters... that's my key concern... also the recent trends using tools developed by cyber criminals... like ransomware... you can do a lot of damage. there's a huge economic cost involved as well...

on a personal level ... I don't know I guess some personal photos or sensitive photos leaking... *laughs* not that I have any... but it's the principle. also financial security... you know I'm concerned buy products online.. is it secure... so yeah I think those of the main issues for me

AH: so do you use a VPN whenever you're making financial transactions?

M: so I do when I'm at work, but at home now... I use credit cards for example for Amazon... for extra security... and I always check to see my bank accounts... to see nothing has been taken that shouldn't have been. I also don't make payments on public Wi-Fi.

AH: do you think e-governance and these secure digital identities makes estonians feel more secure?

M: so I think it goes both ways, I think we can feel safer than other countries who do not have these cards... but also that we can feel vulnerable because of them. the two Factor authentication definitely helps people feel more secure... I think in particular the younger generation are more concerned about the convenience side of all of this than the security side.

AH: Great, so my final question was that do you think citizens have a role and a responsibility in ensuring cyber security, whether their own personal security, or on a national level

M: yeah so after the 2007 attacks I was in the Ministry of Defence, and part of this working group Who drafted the first strategy... and I think it's been in every strategy since, is that cyber security is everybody's responsibility from the beginning. in the government's at that time we didn't have any resources at all so how could we possibly.... so we had to make this an obligation citizens to secure their own devices... so whether it's individual Company level or state-level.... if you look at all legislation this emphasis of responsibility is everywhere. the state can help but it can only do so much... it can educate help assist where possible but ultimately it comes down to the individual.

Participant N - 26.02.2019

AH: What does cyber security mean to you?

N: Since I have been working in the field somewhat.... and i've worked in the defence forces in total for six years in total now. So, it's like a defence mindset, towards preserving my own country, or something like that. But if you know anything about the cyber defence league in general, it's basically a collection of people who have some time to contribute to the security of their nation, and cyber security is just an extension of that regular security of our country, right? So... if you've ever seen Die Hard 4?

AH: I actually don't think i've ever seen 4!

N: Well, as a person in IT, a system administrator, you know how vulnerable some systems could be if some malicious actor were to try and topple us... and since i've been in the defence league for a bit, I'm pretty knowledgeable on the damage that could be done... although no one has really tried to screw us over in cyber terms before... but we're especially susceptible to that. It's interesting to be in the field, and if the time comes when some of our systems are attacked, i could be a first responder, and try to protect our firewall, something like that. Also, since i am working in the public sector, it's become something of a hobby for me... I'm not sure if that answered your question at all?

AH: I think you were saying it's a duty for you then - what cyber security means for you?

N: Yeah, i guess like that

AH: And can I ask, what steps do you take to ensure your own cyber security?

N: Uhh... well there's two parts to that answer. First, I'm hardly findable on Google. If you type my name on there, you'll maybe find me on Facebook, but its all set to private. I have some other social media stuff, but they're more for checking out other peoples stuff than actually posting my own. I regularly do sanitation of my passwords... so i go over old accounts and my different emails, go back and change my own passwords... i dunno, yearly, or whenever i don't feel too good about them. Most of the places i don't even know my password, i just random generate a complex one, and the next time i use it i just go to change my password, go through the security questions and yeah. I don't actually know most of my passwords. So that's the social and the internet parts. Ummm, i also use VPN all the time to cover my tracks, and you know, to also help me buy things at a cheaper price when i know it's cheaper in another country for example, it has upsides. On my own... the hardware... so year, i don't use that much. Everything i own is encrypted, on the windows it's bitlocker, on the mac it's... i dunno what it is, but it's encrypted anyways... and what else? I manage my home... i manage everyones computer there, to some degree, to raise our general security there

AH: So you're responsible for the whole household as well

N: Yeah, i mean it's basic stuff. I mean if i really wanted to go at it, i should really put another router between mine and the ISP and track it, put some extra measures in place i haven't really bothered to do, but i should i guess. So.... i try do some things, but i could do much better

AH: Do you use a camera cover on your devices at all?

N: Yep, on everything. I mean, for the phones, i haven't really bought for them, seeing as I'm a MDM (mobile device management) guy... so i have a lot of phones... but my main one, i have at least one of... i can show you... but i haven't got around to all of them. Sometimes covers don't fit on some phones so it can be a little difficult to do

AH: and do you take any precautions with your smartcards?

N: It's one of the things I'm not really worried about. So my wallet has only three cards, the ID card, one is a supermarket loyalty card, and the third is my bank card. Sure, in terms of the contactless payments, i do use that... i men, as a computer guy and a security familiar person, i do get paranoid about it sometimes. But i do have all of the limits in

place that even if it were to be stolen, i wouldn't miss more than my limits allow... it's a risk I'm willing to accept for comfort, so

and to add to the last question, i have an app called MTasku, which allows me to put my bank cards and different other cards in it, and i can just use it from my phone and use a QR reader.

AH: Cool, can i ask then going back to the national level stuff, what do you think the key threats to Estonia are?

N: Uhhh i mean, there's quite a few. You probably know, as you study the topic, you'll probably know more than me... but one of the most serious threats would be lack of trust. If we don't trust our ID cards, we'll say that it ensures every security we can think of, right? If that trust goes away then maybe, you know it's like America, there's Donald Trump, and so maybe less people trust America as a firm ally... and we can't rely on them anymore as much as we could before right? So if you take away that trust in the system, whether bombarding it with ads, people think it's not secure, some vulnerabilities come up... i think there was something with the ID cards last year, where a specific set of cards were vulnerable to specific attacks, so if that were to keep happening... you know, like java updates right *laughs* ... yeah we find four new zero days... then we probably couldn't trust it as much as we do right now to run pretty much every part of our life as an estonian through it... so everything from drug store receipts, medical information, elections, you know a bit part of that credibility would be taken away from the platform if we didn't trust it. I guess also, there's foreign threats but they're most likely going to be in conjunction with other hostile activities... something along the lines of Krym (Author note: fairly certain participant means Крым - Crimea in Russian) and before anything happens the little green men appear, and they start to make something happen, to make a situation where people want to leave the Ukraine right? and join Russia again... and then, if Russian people in Estonia are not on the same boat, then it's easy then for them to say the Russians in Estonia would like to leave, right? That would probably cause a big uproar, and that'd be a good time to blow up some.... well, not blow up in a literal sense, but to take down some key services, access to banking, government things, it's probably not that hard depending on how much research you put into it, but that'd be the second threat. Right now, we're prepared for a war, but it's not imminent right now. It's more of a threat, but we want to be on top of security in case Russia is interested in taking us down. Or in general.

AH: So you're talking about this idea of 'hybrid' warfare right, as in Ukraine?

N: Yeah

AH: And you think that's possible here?

N: Well conventional warfare is probably not that smart of an idea... Ukraine also... it happened a little bit later. They started with riots and uproars and stuff, but the war came later. But i don't think it's a smart idea, maybe if you say Sundays parade (Editors note - independence day military parade in Tallinn), there were I think up to ten different nations that are fasciliatating? their troops here.. British, Danish, Latvia, Lithuania, Belgians, Canadians, Americans... a lot of people might get quite angry if they try to cross the border, and if any Americans get shot, there's problems! So, conventional warfare isn't so simple, but destroying a system and you can say 'wasn't us mate, what are you gonna do', and the cyber laws aren't really there, so it's easier in that way for Russia to conduct cyber attacks

AH: Yeah... do you think there's anything unique to the Estonian approach? After all, a lot of places seem to hold Estonia up as a world leader in this regard

N: To cyber security in Estonia?

AH: Yeah, sorry

N: Yeah, i mean, if we're going to be proud of these things, we were the first to be targeted by a cyber campaign or cyber war in 2007, from Russia, so Estonia was the first to be attacked this way by a foreign nation, or at least it was the first really recorded or we made something of it. Maybe we're just the first of many. Since then we established the cyber excellence... the NATO place (CCDCOE) located in Tallinn, they wrote the Tallinn manual, it's one of the first... i went through it just a little bit... it's extensive. There's a newer manual of it now as well (Editor note - 2.0), so maybe we're more interested in pushing it forward in that way. Also, the cyber defence league is one of its own... we're

not the only country with such defence forces, but the first cyber, with volunteers. And as this cyber stuff is new, we were innovative... I'm not sure if that's unique, but it's interesting, and we're trying to get things started

AH: Do you think the digital identities and all of the extensive e-governance here actually makes Estonian citizens feel more secure?

N: I'm not sure, a regular person probably doesn't think about it too often, since most of the time everything just works, and it's simple. If you ever see any information about the elections, you can cast your vote in two minutes. The trust for it is good. I'm not familiar with any real attacks on it, I'm not too familiar with incidents that have reached the media anyway, so the trust is pretty good. But if you're worried about it, it's unusual. People don't want to go back to the old way of doing it. Sure, there's relatively few people in Estonia, so we don't have enough resources to make it super big, or put the best developers on it, but with the resources we do have, it's pretty good. We're also promoting information on the same system for other countries as well... i think Uzbekistan is one of them... and I think other European nations too. Slovenia maybe it was? But maybe not to the extent we use it. In Europe we are starting to talk about connecting our systems a little bit, i mean it's probably related to specific IT systems, but there's talk of being able to sign things in other countries with your ID cards and it's still valid... i don't know where that is right now, but that would be helpful for sure

AH: On the subject of Europe, do you think Estonians are more security aware than other European countries?

N: I feel that most of Northern Europe is more interested in it... but since I have taken part in some of the cyber defence or security related exercises, i can say there's also a few other southern counties interested, but i do feel the north, it's my own feeling these countries have more interest in these things than southern europe, but it's just a hunch, i don't really have solid arguments to back myself up here. I know France does take part in these exercises, for example, but most of the southern countries don't seem to cooperate. It seems out closer neighbours are more interested

AH: Do you think then that individual citizens have a role and responsibility in ensuring their own cyber security?

N: Well, the government for sure can't be in charge of everything, seen as there is too little human resources... and also, in the grand scheme of things, the individual approaches definitely work better. That's why the defence league and also the police and public sector organisations definitely do all sorts of, so there's quite a few free courses for security on computers, smartphones... you know, the government doesn't make it everywhere. They can't come to your home and say hey, why haven't you installed antivirus or whatever. So the best they can do is education. So know they do provide some basic computer and programming lessons, but cyber security is not as easy you know... it could probably be easy to sell, it sounds cool... but then fo the average person some of it will fly over their heads... so they're like, what do you mean i have to change my passwords to be more complex... i mean, the country probably can do it, but it can't afford it, and they don't have time. Education makes more sense i guess. Easy example, i would live with someone who wouldn't update their computer, and who would download things from torrents all the time, things that could compromise our network, so these things are on everyones mind that you have to teach the public to use their computers better, but also there's a limit to what you can do.... and resources, and peoples interest are limited.

AH: Finally, what do you think the future is like for e-Estonia? Do you think it will spread beyond Estonia?

N: Well, i do hope... you know, Finland has already adopted some them... so it can be interoperable... so that's maybe the difficult bit, when we have to start trusting other countries to do other stuff, and actually recently i read a paper on the drug... what do you call the thing you take to the pharmacy.... or get from there?

AH: A prescription

N: Yeah, so apparently that's been an issue because the systems for these things are different a lot over Europe, so if other countries do their own e-citizenship systems, it's probably not so easy to make them work together, so connecting systems is probably the hardest part. We have that now between Estonia and Finland. The rest, who knows. But security for the cards is so important, to keep trust.

Participant O - 06.02.2019

AH: What does cyber security mean to you?

O: Oof... it's a very broad subject... essentially, if i define it for myself, i suppose its means all the different tools which ensure the continuity of the digital ecosystem. So, that's ensuring all of the digital lifestyle for us. I realise that's a very Estonian answer.... but so much of our lives are now integrated with the digital sphere. That's become separate and important. For us, it's making sure life goes on and continues without disruption in this regard. It's not only the technical tools, but it's creating the legal environment, having the tools, and making sure that everyone is sharing information on the threats.. we need to create that environment. To ensure the functionality and continuity.

AH: What measures do you take to ensure your own cyber security?

O: That's again a range of different tools... one that is fundamental is the capacity and capability to be able to prevent and detect, and respond on a technical level... but the other is the entire procedure to it... so you know how to deal with the incidents. Who needs to know, who to engage, how to be involved in responding, mitigating, and preventing in no particular order... and having a public sector to that is capable of responding. Then, having a private sector that is well engaged, understands what their own systems are, how to defend them and the services that they provide, and having an ecosystem where those different needs and abilities link together. So you don't try to advance your needs in a way that affects citizens negatively. So in total that involves having a technologically literate society, more or less, and a legal and policy environment that moulds this together

AH: On a personal level, is there anything you do to ensure your own cyber security? Do you use a camera cover or VPN?

O: So i try to practice what I preach, so i use two factor authentication, I don't use a password manager... but i have invented a method where i can remember over a 100 complex passwords myself. So in the most, for the most critical services, they are memorised. The others are linked to my other accounts so i can reset them by requests, usually by my google account which has two factor authentication linked to it.

AH: So you prioritise higher and lower risks?

O: Yeah exactly, and i guess also it's about practising what you preach there as well. I try to teach good cyber hygiene to my kids also, and hopefully they teach their classmates too, so yeah. On a personal level, it's a risk management thing. So there's services you like, and you consider and acknowledge that you're giving up a bit of control... so you buy a smart TV or use a smart phone because you like them, but I'm reluctant to buy like these IoT vacuum cleaners, and things like that *laughs*

AH: Do you take any security precautions with your smart cards? Would you use an RFID block for example.

O: Of course i do consider everything that can be used and abused, and i manage my risks, i keep the limits low, I'm careful where i store my cards, an i know what to do incase they wander away elsewhere.

AH: And you use contactless payments?

O: I do, but again, there is limits issued by the banks

AH: So regarding security in Estonia, what do you think the key threats are?

O: Hmm... well. For that, as of last year, i have a quite compressive view... i was the lead author for this (Annual report)... i was posted to the national cyber security authority a year ago, and part of i wanted to do that is to see what real life looks like... and what you see is an incredible amount of mundane, silly incidents which is a combination of people being careless and not thinking. Careless people not updating their software, and then careless in their behaviour. So the vast majority, over eighty percent each year are a combination of outdated software and poorly configured services. So most of what you see is really mundane, and really silly that can be prevented by better cyber hygiene and having better attention to the process. So very basic security can prevent most of what happens

AH: So you think there's a connection between these mundane things and then a national level of cyber security?

O: It's interesting. So each case on their own doesn't really add up to anything you'd consider relevant to national cyber security.... but, if you saw the combined drain on the economy, and resources, then that drain is really significant. So on one hand, no its not... but it's not like it doesn't have any security impact at all. You're still paying for it. Death by a thousand cuts or whatever.

AH: Can you say if there's anything unique to the Estonian approach to cyber security?

O: What i do think is unique is our community.... our community and trust based approach. And this is difficult to scale. It boils down to being a small society, and in many cases people who have had experience tend to know each other and the trust is there. But it has very often proved to be our strength and a source of agility... and yes, you waste less resources on duplication, and you can be more agile and there's not several layers of administrative overheads to cut through to get somewhere. So when we had this ID security card vulnerability a year ago, the escalation up to a governmental level was very quick... and not just because it was a critical level, but because of the ways that these things work in Estonia. Everyone knows everyone and things become a common issue quickly

AH: Do you think the e-governance and digital identities actually makes Estonians feel more secure?

O: There's many layers.... on one hand, yes... but also, it's been so integrated... i don't think people always acknowledge these issues. So i think the technology and the banks have always been keen on this, but they've used the cryptographically secured means of authentication for over fifteen years now... so people use it, but they don't think about the security necessarily... as long as it keeps their money safe. So i mean, if it's been there, we have a secure starting point. I think most people are quite enthusiastic in general... or at least neutral. I mean, this openness to new technology and innovation that has always been there. It's a cultural issue, and embracing education and innovation to the extent we can.

AH: What do you think the common security concerns of Estonians are?

O: I think these are day to day... economic stability and it's being able to access medical care when it's needed... how we are doing with integrating our Russian-speaking minority for example... how.... are they as competitive in education and the labour market when they finish their studies... and of course we realise the part of the world we live in. So that's an acknowledged situation, it's a Geopolitical reality we are accustomed to... i think we are more aware of security here that somewhere in southern or central europe for example. For many, there's a history they have first hand and lived memory of

AH: Do you think there is a unique mindset in Estonia? Is the Estonian approach to cyber security unique?

O: I can't speak for society as a whole, but i see the mindset in the cyber security community... and that's something... we all know those people that developed the foundations of the digital ecosystem... so you know them, or you know those who know them... it gives you that trust... it's something we made ourselves... not a distance... and we have contributed to it. It validates and creates trust for ourselves... we have a sense that we know what we get, and we know what we have isn't perfect, but we know how and who put it together, and with what intentions... it's a huge aspect of trust, and it leaks into wider society as well

AH: Do you think Estonians are more security aware than others?

O: I think the awareness is good, but it's occasionally misplaced.... we are very attentive to cyber security in public services that the state provides... but we don't sometimes apply the same standards for private service providers or especially international service providers... so it varies... and also the expectations vary. The state is expected to act to a much higher standard than a web shop or something. Banks are different, probably they are held to the standard of the state, or higher, and thats because they are the ones who brought a lot of the services in. So there are high expectations of them.

AH: Do you think that individual citizens have a role and a responsibility in ensuring their own cyber security?

O: Of course

AH: Absolutely everything, or do you think there is anything the state should take care of?

O: No.... i think understanding.... it is pretty commonly held still that you are primarily responsible for yourself... and that applies online and in dealings in the digital space... and whether people are able to meet that obligation themselves... and how much is the cyber community doing to equip and assist people... theres awareness raising initiatives fairly regularly to engage with regular citizens. On one hand you this thing that it's your life, you are responsible for it... whether its the regular physical world, or online... but the other side of that is that service providers and the state provides tools, and education that enables that security online... and strengthens it when possible. But it's shared in this regard really.

Participant P - 11.04.2018

AH: What does cyber security mean to you

P: you could not be more open if you tried.... I suppose I haven't really thought about it in my personal perspective... cyber as a term is very vaguely defined... each organisation often has its own definition and each country has its own definition. if you look at the c c d c o e they have some definitions on there and they have some different countries definitions and they are often different, so this is a problem and something I have been thinking about a lot... I think about these problems all the time as the coordinator of estonia's strategy. I have little time to think about my own perspective as I am thinking about this professionally. it's a very good question where do you put the borders you have to agree on the borders. we often draw a line between cyber threats that result from technical concerns then we talk about false information or cyber bullying or cyber terrorists but these will not be in a cyber security strategy they will be dealt with in our internal security strategy but that does not mean they are less cyber in nature I think borders between these are necessary because so much of life is now lived in the digital sphere when you talk about cyberbullying it has nothing to do with digital technical threats... the same thing was done before simply without the technology. an email asking for money riding someone could previously have been sent by paper so as more and more of our lives are lived in the digital sphere the cyber security strategy will inevitably be everything and you're not able to cover everything in one document

AH: so you agree that the documents and strategies should be separated?

P: So I don't that sort of my point I think cyber is more and more a thing of everything we talk about internal security and cyber security is a key part of that it is a huge part of our national defence in Estonia it is already a big part of it and it belongs there. to me you don't need to put this in a separate document. it's already there.. cyber security is part of IT education it's less and less a thing of its own. it's part of everything... this is a vision IC for strategy planning as well for a developed Society I would like to see cyber integrated in all parts of life and you don't address it as a thing on its own... in Estonia as well as in other countries we are not that far yet it needs a dedicated detention in different places to put this together... I think the challenge is now in 2018 are very different to the challenges of 2013... when I last strategy was put together which was for the world as it was then... the threats are higher now with the amount of devices that they use now and the amount of different threats this generates in digital space... the threats have grown, but also the awareness has grown. Good examples of the technical and non technical working together might be information security or data protection Of course a lot of these things are stored digitally now... so these are two sides of the same coin... one of the girls has to have a more integral view of these aspects... I think it's a historical matter that these things are dealt with differently.... in Estonia we have the state information authority responsible for cyber security and information Security so the data information ministry belongs to the Ministry of Justice... so we have different Ministries working on roughly the same area but we could improve the dialogue.

AH: So can I ask on a personal level what measures do you take to ensure your own cyber security?

P: I think I don't think I'm a great example... I use my digital identity wherever as possible because I know it's secure I use passwords with the appropriate complexity.... I do prefer encrypted email exchanges... I use WhatsApp I'm not sure if it's the strongest and most trustworthy but we all use it... it's better than Skype.... properly protect my way to... router ID I use my hotspot on use VPN he's overstepped without it....

AH: have you picked up on these processes because of your line of work?

P: No... I think concerning encrypted communications and public Wi-Fi that's a general concern... not letting my kid download things on my device mean... it surprises me the right somebody school kids have... I treat my work devices with extra sensitivity. since I've learnt in the department that potentially my cables and chargers could be infected I make sure I don't leave these in public places.

AH: So you often differentiate between your own personal cyber security and that of your work?

P: so I do think about my personal data as well but I also use social media... I am careful but not as careful as I would be with my work computer or data

AH: do you use a camera cover on your devices?

P: yes I do

AH: why do you choose to do that?

P: it's simple security... I have one for my laptop and they distributes really cool covers in the department if they had given me one for my phone I would've put it on that as well.

AH: Do you have a mic blocker

P: no not at all... I'm aware of the possibility... but what can you do...

AH: Do you think they should be built in, so the user can disable these things? It's very difficult to manually turn it off

P: I understand. It's difficult. With every app it often can give access to things way beyond what the actual app needs... I suppose it does come down to policy and regulation, but you don't want to stifle innovation...

AH: It would make the private sectors lives more difficult?

P: Yes, and of course data is valuable... right now, it's not by design... but this might not be accidental. Smart and strong policy planning is required. In that sense, I do believe security and privacy by design is the future, and what you do by raising awareness with people is merely scratching the surface

AH: Another question I often ask is do you have any security precautions you take with your smart cards obviously in Estonia you have identity cards on but also you could potentially have a contactless bank card do you have a contactless bank card at all?

P: No

AH: would you choose not to have one

P: I would prefer not to have one myself the contactless cards I think there is too much comfort a head of security... I don't agree with the possibility that if someone finds one they can just use them and even the €20 limit in Estonia to a pensioner can be a lot of money

AH: so now in Estonia new cards being issued already have this built-in and you are not asked if you want it how do you feel about that?

P: yes I know and I don't agree with it I don't think it's right... it's difficult on a strategic level how we plan for this it's difficult to interfere... obviously banks have run calculations and are happy with the risk I'm not so sure we also have contactless travel cards and the technology isn't 100% secure with these... speaking with the financial sector is an important cultural aspect of being in cyber security... but it isn't something we have really touched at strategic level. but this would involve rules and nobody likes rules... when it goes wrong it's a lot of their credibility

AH: I mean a lot of people I speak to they say that they don't really trust it or feel it is secure but the use it anyway because it's convenient

P: everybody makes such compromises I think of different levels

AH: would you ever consider using an RFID blocker such as a sleeve for the card or a wallet which blocks the signal

P: no not particularly

AH: Ok so that sort of covers the part of the interview addressing personal cyber security I suppose I'm talking to the right person here for this next question can I ask you for some more details about the Estonian approach to cyber security? Some of the challenges you face?

P: I think if we think about problems they're not so much Estonia specific they're global problems and these Solutions we can also share with others. in Estonia we have AH: challenges with the workforce which is not necessarily prepared for some of these challenges that that is not unique to Estonia... cyber is not yet fully integrated... we separated due to the Digital complexities although I believe we were the first country in the world to put all the things concerning cyber security in One strategy... making connections between the different topics whether they are data protection information security internal security electronic identification critical infrastructure.... there are many different points of contact. there are many ways in which people should work things out together, we recognise this is not ideal that these different aspects do not always speak to one another and it is something we are trying to address in the next strategy. what it leads to is creating parallel Solutions instead of one solution this is expensive and also problematic everyone does things in their own house ... the capacities of different organisations a different... some do it very well... some of the weaker ones the level is not sufficient... but our integrated digital infrastructure is the same for everyone we all use it so even the weakest links need to have strong cyber security.... cooperation and interoperability are key. Estonia is not alone in identifying this need and I think it comes from the very nature of cyber security. something technical... something for some geeks or freaks *laughs* something that crawls into everyday life but it's so complex it's a different thing from it being integrated in every way so we're in something of a transition.

So we must create this infrastructure and ensure we're fully integrated. also across borders when we talk of critical dependencies and interdependencies... we have many private companies involved working across borders... it is important to understand this better. so I spoke of problems I think different countries have different maturity levels with this but a lot of these problems are global problems the most countries are facing... where is Estonia stands out is that we are a more effective digital domain at the moment... how digital dependency is so high... the highest in the world in terms of digital government and services we depend on... these threats are the same in other countries but in Estonia we are more dependent on these digital services. secure design makes infrastructure secure for Citizens. this is where is Estonia stands out... in design and infrastructure. we need to protect what we have but we cannot just stay with this technology we worked some of this out 10 years ago, we need to stay up to date. if we want to be a serious international actor and we want our companies to be strong this is key.

Also Estonia's smallness and flexibility is important... the trust of Citizens towards Digital Solutions... and some appreciation for cyber security does exist within Society... this may be special (unique) to Estonia.

AH: do you think there's anything unique to the Estonian approach to do in cyber security?

P: Unique today... or unique in how we got to today?

AH: I think both? Is a very good question... both in the sense of the history involved and how e-Estonia came to be, and also do you think anything Has Changed? has the rest of the world caught up?

P: yes I think the rest of the world is catching up and Estonia has to put concentrated efforts to remain in the same category where we are perceived as experts... it's not right to think that we are somehow special... it's very different now than in 2008 and 2013... whether we are so special today... I don't know. I think what is Key about Estonia is the secure infrastructure which allows us to offer services and this is based on digital identity... it started out with the opportunities being a newly independent and small country presented, we had no Legacy issues... we also had a bunch of very smart people left from Soviet times.... we put together something very clever but not something that was totally unique... the possibility from being able to put numbers to people, and from the trust of a new country to a new government... this was our brand new freedom ... uhhh... that's the greatest example that cyber security didn't come from technological advancement but from procedural advancement... the possibility to make something work... this is an asset and... we have worked for other on it... the possibility to digitally identify yourself, is key. it's simple as well... if security is too complex it is not really security.

AH: So you believe procedures are important and that they are simple for ordinary citizens?

P: yes this is important... it is all because of the secure digital identities and it comes from being able to put numbers to people... so with country struggle *laughter* ... but how we do this technologically... we can't stay with yesterday... the same as other countries we must continue to develop and that's what makes this such a fascinating area of research.

AH: do you believe that the secure digital identities and the e-government systems make Estonian citizens feel more secure?

P: in short yes yes I do.

AH: why do you think that is?

P: why do people trust?

AH: Yes

P: Estonia as a young country... it had this trust credit... we didn't have the political Legacy of creating distrust... we didn't have the same technical Legacy as other countries if you have old systems it's much harder to change things... if you can build something from zero that works... we could build a system that spoke for itself and works. the openness of the Estonian government is also ok when things went wrong with the cards previously we already spoke about that weed out with this is an open and clear with... the accountability is key as well I can see who has access to my data... this was thought of from the beginning as well. I don't use a lot of talking about it things were implemented and they worked and they made people's lives easier and people accepted them for it. this for example would be a considerable barrier in the UK I imagine...

AH: Yes

P: and the resistance in the UK to such an aversion is strange to estonians it's an emotional argument the data we're talking about still exist for UK citizens it's just on some paper in her cupboard somewhere... and often much less protected... and you have no idea if someone has looked at them... I know if and when someone has looked at my private data

AH: yes but in the UK we often hand over rights to on personal data through services such as applications and two private companies...

Do you think Estonians are more security aware than other European Nations? I sometimes get the impression especially with cyber security concerns that you're quite relaxed...

P: I would be speculating... I don't know about every Estonian and their awareness.... I think we use more digital services... I don't think measuring it can be trivial... one of the goals of our last strategy was that people would be more aware by the time that strategy expired... so we used questionnaires to gather data I believe it was 50% as measured by euro barometer who believed they were cyber literate and it was recently measured as 40% to now agree... although I would have been worried if 90% said they felt they had sufficient knowledge... I would say my knowledge is sufficient but I think people are maybe Now more aware of the complexity and the whole spectrum of ways side of threats can affect my life... I would certainly like to see the figures in a few years if this was possible to see how this pans out... I think it would come from something like the questions you have asked me and specific measures that you take... do you use contactless cards vpns how many characters is your password... even test that you pass... I think that could show you something... I think you can do it at intervals and have a system for that.

AH: perhaps my next research project?

P: you should do that... if and making it comparable... it would be a great piece of research!

AH: who knows what the future holds... if someone would fund it... maybe!

AH: So the final question i have to ask, citizens are now often said to have a role and a responsibility in ensuring cyber security.... Do you agree with that? Do you think citizens have a responsibility for their own personal, and then national security?

P: Uhhh *hesitates* The obvious answer is yes... if people have no awareness at all... start replying to every fake email this will start showing up in GDP... *laughs* ... I think yes definitely... people should take personal responsibility the state can't be a babysitter... but it can't end and everyone knows.... it comes back to this by Design principle... it has to be natural and easy to use.... and this is done by governments and organisations...

AH: so yes but there has to be a limit, and at some point this requires state and international cooperation as well?

P: Absolutely... if security is always a compromise with convenience people will always make that choice... that's natural...

Participant Q - 10.04.2018

AH: I always ask all interviewees a deliberately open question to begin, and I'm aware this is very open to interpretation, but what do you understand to be 'cyber security'?

Q: So it means many things... so for example, do you mean from a citizens perspective, do you mean a governments perspective, or from a companies perspective...

AH: Ha, well I try to leave that open deliberately so people make their own choices, which I think is interesting in itself, rather than deliberately leading you into one of them... i mean, whichever you feel best placed, or happiest to comment upon?

Q: So I guess for myself it's being , self aware, it means cyber hygiene, it means acting responsibly in an online world... but it also means that the state has to ensure your critical security, i would say. From a governmental perspective, it means you have to have a proper cyber strategy in place to know what you're dealing with in the first place... otherwise, i mean, you can define cyber security in so many different ways. Do you mean technical security, do you mean like policy security, etc... so, it could mean a lot of things, depending on which perspective you're looking at it from. But it all comes down to the government being able to take care of their infrastructure, their citizens, and the citizens themselves being aware themselves of cyber hygiene, awareness etc.

AH: Ha, a very comprehensive answer. So going back to your own personal security, if i may, what measures do you take to ensure your own cyber security?

Q: Ok, a) so now I'm on a Skype conversation with you, i had to open the lid for the webcam... but working for the government, you have certain measures you have to take. For instance, so from a personal perspective, i have to change my password to log in to the computer every now and then, so it needs to be updated. It also means I cannot have the same password for my work email, and my personal accounts. It also means that when my work email comes to my phone, i have to have a certain digit length password, which i have to update every now and then. So this is just like basic cyber hygiene, right? Things like this. It also means we have to undergo various levels of cyber security training... since I'm a trained lawyer, i actually studied cyber laws at a masters level, so this all means a lot of things to me.

AH: So, for example, you mentioned the camera cover, do you use a vpn as well...

Q: We do, yes. So whenever I'm not in the ministry network, we use something called pulse... so this is one thing. There are so many things! It's difficult, because we have so many things that we just do and don't think about. I don't fall for phishing *laughs*, ok i do still, unfortunately, use different platforms such as facebook... i use different apps on my phone which i know could potentially access my camera or conversations... but i still use them... because, you know, in todays digital society, I'm not sure you can live without instagram, skype... all these things nearly everyone uses.

AH: I must admit I live without instagram, but the rest of it... yep. Same.

Q: I mean even Skype, even when I installed my new phone... oh and I have a phone which is able to send end to end encrypted messages... for work communication, for example, if we don't send an email, we use whatsapp. So this is the means of communication for us.

AH: So you differentiate between personal and professional time, and consequently personal and professional cyber security?

Q: They do seem to flow in to one *laughs* ... you know, i work in the ministry, i work in the university, I'm also doing my PhD at another university.... uhhh so i think there's no personal time for me!

AH: So even, theoretically, *if* we removed all of these work factors... you'd still use a VPN, an encrypted messaging service...?

Q: Encrypted messaging yes, definitely... VPN, maybe not so much. It'd depend where I was... like China... uhhh but not at all times, probably.... or you know, say I'm travelling abroad, i wouldn't connect to the random cafe wifi to access work stuff, i'd turn my VPN on... or even for financial transactions. I use mobile banking on my phones, but we authenticate this with our mobile ID also, so i can securely do this on my own mobile network secure.

AH: On the subject of financial transactions... Do you have a contactless bank card at all?

Q: I don't have one because I have an out of date card but if I would receive a new one I would turn this feature off

AH: is that because of a concern around the technology itself

Q: no it's just Anything Could Happen right I could lose my card and even though it's limit is around €25 or whatever it could still do quite huge damage within hours until I realised my card is gone or as technology evolves I could have this in my bag and someone with a scanner could potentially read this through my bag... I don't have it and if I had it I would deactivate this

AH: So actually, going back to what you mentioned at the beginning of the call; the camera cover... what made you choose to apply one of those?

Q: It's common knowledge... I think?

AH: Do you think it's perhaps common in your line of work, as opposed to in general life? For example, I have one too, but i wouldn't say it's common most people I know have them...

Q: So sure, a lot of people I work with have these things... but I think they're quite common in Estonia anyway. So, I think I got this from our last president, Toomas Hendrik Ilves... he was a very public figure here, and he sort of popularised this, maybe?

AH: You have a proper one, or just a plaster?

Q: Yeah, i have a proper one, not a sticky one, but that is one of the things Ilves suggested. Have you seen those Black Mirror episodes?

AH: No, i haven't actually. A couple of people have mentioned now that i might like it...

Q: So there are a couple of very good episodes, and one of them has to do with webcam covers basically... for me, i think it's common knowledge, because i watched documentaries about Edward Snowden.... I've been teaching, and i've been learning law and cyber security as a subject, so... yes. I think they're quite commonplace here. I think we're also entitled to be sceptical about these things...

AH: I noticed you mentioned Snowden.... do you have a mic blocker at all? There is that famous Snowden video with John Oliver where he shows you how to disable the mic on a phone by taking it apart and just using headphones with a mic....

Q: Yeah, so Snowden said the only safe way is to remove this... so, I'm aware the mic is always on, and i've read the terms and condition on instagram... and all these apps... and yeah, I'm aware

AH: I mean for me, i'd be more bothered if someone took over my mic, but I'm pretty concerned about both, and do what I can to mitigate the possibility, no matter how unlikely it is, or how unlikely a target I am personally

Q: and that's very interesting because I teach the legal framework of e-governance... and I always get around 50% of a class who will say I don't have anything to hide... so basically I don't care if they watch me... but do you really want to be observed at all times? someone who can access your camera or your audio when they choose? now combined with the Cambridge analytica stuff... profiling people... even if they know what series I'm watching what I'm eating at home or what kind of wine and drinking... I mean I know to appoint some of this information will be out there but it shouldn't be easily accessible.... easy for them to collect and potentially manipulate.

AH: would you like ownership of that process?

Q: Yes... so in Estonia it's the individual not the company that own the data. so we are on the data and we can turn it off if necessary.

AH: so how does that work with companies not based in Estonia than? of course Facebook isn't an Estonian company but nearly everyone here seems to use it... Facebook argue they own that data don't they?

Q: are you familiar with the privacy framework here?

AH: not particularly...

SS; so Facebook is a US company right... so under the European Union data protection framework... to supply their services to European countries, and to send their data to third countries, they have to be any data adequacy granted country or you have to have certain binding corporate rules... or different types of negotiated contracts with those.. so the US has a negotiated privacy shield between themselves and the EU, and companies such as Facebook must self certify themselves that dated here to the eu's data protection rules. otherwise we would not be able to even transfer our data there?

AH: so quite often the US Falls short of those data adequacy rules, no?

SS; Yes, so this went to court in light of the Snowden Revelations, that us laws did not offer adequate protection to EU citizens and that their data could be transferred to the NSA And that there was inadequate protection sending from the EU to the US data... now we have a dual frameworks of this and that companies in the US can self certify that they adhere to EU data protection rules... and only if they self certify they can offer their services to EU citizens.

AH: and the gdpr also comes into effect in the next few weeks?

Q: yes the 25th of May

Q: yes and Zuckerberg has confirmed that he will apply the EU regulations to all countries in which Facebook is operating... of course it's very nice statement and at this point he has to say stuff like this... we will see

AH: What do you think of the key threats or concerns to Estonian cyber security?

Q: So personal data is definitely a concern estonians we have a medical data online for access to prescriptions etc... so in theory this could be a concern right... having all of this data online... but we use blockchain technology to secure match of that data... so this is you know... mitigating it... secondly we don't have one server where all this data is held... so we have this distributed data storage system called The X Road... so we take care that everything is as distributed as possible. as a country we always have to be afraid... or aware of potential cyber attacks from other countries... so for one thing Estonia has secured themselves or ourselves against... have you heard of the data embassy Project?

AH: Yes

Q: so basically we going to have a data Embassy in Luxembourg... what all the critical data will be stored... so even if there would be an attack on servers or you know whatever, in Estonia, even combined with a physical attack, basically Our Data would still be safe and stored somewhere else as well. you have to be aware of those risks definitely ... but you also have to be able to mitigate them I would say

AH: do you think this requires the average citizen, not to understand how blockchain of the X road works, but they have to at least Trust that is doing what they're being told that it is doing

Q: yes but in Estonia people trust the government for similar reasons... we've never had data breaches or identity thefts... over 90% of Estonians use their ID cards... you know how the ID card functions right? Basically you have two pins, authenticating yourself twice with your digital signature, also we have this landing page eesti.ee so even if a Doctor accesses your medical data, as I said we own the data.... The companies own the data... so i can check which med-

ical professional has accessed my data. I can check this, i can challenge this... i can turn it off... even though we're small, we only have 1.3 million people... it was less than 1% of people who have turned this access off... these things have been developed for convenience anyway. So you're unconscious on the street, but they find you have your card with you... they know who you are, and then can access your records, find out not to give you something you're allergic too right? So x Road it is functioning since 2001 without being down ... at any point whatsoever. of course having all this data online is a security risk but also it's just living and functioning as a country in a very strategically located place in Europe

AH: do you think the geographical location of Estonia has made its citizens security aware and more likely to trust the government... so to your average person they have to trust that these services function the way they are told they do... if that makes sense?

Q: UK citizens use Facebook they use Gmail they use all kinds of online services why would they trust those? why Trust private companies with our data but then say we cannot trust our government? a lot of this is about mindset... it may have something to do with Estonia being occupied by a different country recently for 50 years... then finally having her own country back... offering us these services making our lives easier... he could be this... comparing what we had a couple of decades ago to what we have now. so we've had relatively few data breaches, the last major attacks were in 2007 as I'm sure you're aware, and after this Estonia immediately took steps... we had started testing blockchain technology back then... we develop with guard time, a private company based in Estonia, and we implemented this technology after 2007. things like the ID card people use it they trust it if there are no problems occurring people continue using it... where is big service providers Facebook apple Yahoo whoever... who ever.... every now and again at least once a year you read something about new data breaches... you use Tinder, services like this... it gives so much of your data away... and then suddenly, it's your government, who are tasked with taking by the constitution... well not in the UK, you don't have one, but they're there to take care of you... and them having this.. it's a problem? For me, it's very strange.

AH: Sure, I get it, but we have had different instances in the UK, historically, which have perhaps undermined trust in government. Not necessarily just in regard to cyber security, but more generally. Yet UK users, we still use apps which grant these freedoms, such as Uber, as they provide a service... so yeah, you're right.

AH: Do you think, the way things are, with digital identities... do you think that makes Estonians feel more secure?

Q: So digital identities... yeah. So whenever we access our services... we don't use bank links... they're becoming extinct. We don't use them anymore. We use or e-id's, or mobile ID's, or smart ID' offered by the private sector, because we know that they are trusted... they're provided by a trusted service provider, our government. So yeah you can only login when you have the physical ID card with you all the mobile ID... so so knew your pin1, they would not be able to go so far. so even if they could access your physical ID card they wouldn't be able to complete a bank transaction let's say... you still need to seal the deal or provide the digital signature with PIN 2. to complete the transaction.

AH: But it has happened occasionally where for example elderly people can't remember all of the codes so they've written them down and kept them with the physical card, and people have gained access that way?

Q: yes but in Estonia and I'm sad to say, that most of those elderly people don't have access to more than a couple of €100 in their bank accounts anyway... it's still tragic but... yes it's the job of the government to keep people aware of what they should and should not do... how they should behave what is and is not acceptable, how to not put themselves under threat etc.

AH: yes so you believe the government has this role in terms of education?

Q: yes so this comes from schools... from workplace... and the next step is public awareness programs... so on raising awareness of AI. so you can do all these things with technology but you have to justify why and to who this benefits.

AH: so you think it needs to be explained why... for example... you should set complex passwords...

Q: Absolutely... so yeah, like my sisters, they're probably not all that cyber aware, but they're still setting passwords for phones that aren't easy to guess... maybe that comes from them not wanting my mum to see photos on there or whatever *laughs* but they see the benefit

AH: Do you think there's something to Estonian mindsets that make them more willing to Estonian mindsets to take on technology, particularly in governance?

Q: Ok, so these cards were introduced in 2002, but they came with different services. So if you make something mandatory you have to give something for this. so at first we offered citizens the opportunity to declare taxes online. so instead of physically declaring taxes on paper which might take you days, if not more, you give them the possibility to login online and pay their taxes within 3 to 5 minutes. so it's already giving something back for something... so now everything is online... starting from checking your kids grades... two voting over the internet. so you just have to give the benefits to the citizen. but it can't just be for the sake of it... you can't just do digitalization for the sake of it the citizen has to see the benefits... with each new service we offer we're trying to see... each time we develop that new service we're thinking how it will benefit the user. you have to put the user at the centre of this digitalisation process.

AH: Do you think it was easier to sell in 2002? Because independence was still relatively new? People trusted the government?

Q: at the same time we re-gained our independence in 1991, we issued the first passports in 1992, with 10-year expiry dates, so the 2002 cards were issued as mandatory documents after this... so for us identification is mandatory the passport is a nice thing to have but we don't usually need it... if you travel to the US you do need one. otherwise you can just use your ID card.

AH: Yes part of the problem in the UK is theoretically we don't need to have any identification at all if I don't want to leave the country I don't need a passport if I do not want to drive I don't need a driving licence

Q: I think the future of digital identities will change. so these identities will not be tied to a plastic document... with chips under the skin is the next step probably. so it's not about having physical documents it's about having personal unique identifiers

AH: is that not a bit dystopian?

Q: not really it's no different to the current system the card are issued at birth anyway, and they are how the government identifies you as a person... so in the UK you don't necessarily need a card the whole purpose of the identity is to identify you as a person it can be done in any innovative way... it could be using any new technology that doesn't actually exist yet. one size does not fit all, for us the ID cards worked, this was 16 years ago. people will come up with something new soon.

AH: do you think the people actually trust the physical document though, and the process behind this? I certainly wouldn't trust the chip under your skin..

Q: No, i don't like the idea either *laughs* and I hope we're not there any time soon. But technology changes, and what is acceptable over time changes. I'm just saying I can't predict the future I don't know what's going to happen.

AH: It's a little dystopian though, isn't it? I mean, even the access to your kids school files online. I was talking to someone the other day, and all communication is this way?

Q: That's right, yes

AH: Now, I used to forge my mums signature in my school diary sometimes... some weeks I genuinely forgot to get it signed, some weeks i'd done something wrong... so when i could get away with it... i would do this, to stay out of trouble.... I'll admit it rarely worked, but i think it definitely did at least once... That's not possible here?

Q: No, Estonian kids can't misbehave *laughs* ... so all the marks, all the comments, parents just look online and can see this. So it works both ways, so kids can't make things up, parents will be able to check online... so if a kid comes home and says he needs a flying fish for his school project, or whatever, they will know.

AH: Is this not... I don't know how i feel about that...

Q: Well, you can only see your own kids grades and notes of course. I mean, if you're a careful parent, you're going to know anyway.... Those who don't care, i guess they're not going to check... or they're just going to trust the kids. That's their own responsibility... it's giving the same possibility in the digital world as there is in the physical world.

AH: But then does the child not have a right to privacy?

Q: *laughs* no they don't, not under this

AH: *laughs* the naughty child in me is outraged

Q: So yes, under the GDPR, if you're under this age, you can't give consent to certain things... so the parent has to give consent to you... countries can choose the age... but yeah, anything up to 18, it's the parents responsibility. But we live in a different era, right? So today, parents our age, they might post their kids pictures online, maybe naked or whatever when they're very young, and in this way i think the kids should have a right to privacy. Uhhh being a parent, i would not post this... because... you know, they can't consent about it... and down the line, they could be very angry about this... so yes, i agree with you, some should belong to the child, but legally... you have to have a legal guardian under a certain age... it's the same with a physical diary though. It'd be the same going home and having to show the diary

AH: It might just breed a generation of children who want to hack the system? I know I hated having to hand over the diary if i'd done something wrong... and at least i had the possibiilty, however bad an idea it was, to try and hide it....

Q: Yes... so i don't believe there are more threats in the digital world to the physical world still. They're just different.

AH: Yes, I understand. I would just worry about the mindset it can create.

Q: Well, Estonians come out as some of the top behaved children in the world, so...

AH: Because they have no way to misbehave!

Q: You should see my sisters!

AH: Well, yes but they get caught every single time, surely?!

Q: Yeah, i mean children are smart. I guess they'll figure out new ways to hide things from their parents

AH: We'll wait and see I guess!

AH: Can I ask one quick question before we go, as our time is nearly up and I need to vacate this room, can I just ask, do you think Estonians are more likely to be security aware than other European nations?

Q: I like to think so... so when the 2007 the attacks against Estonia... when they happened.... We didn't keep it a secret. It was very well communicated to the citizens.... And to the public. So during the attacks, in the immediate aftermath etc... we found out ways to make them more aware... and to keep themselves more secure as well... so this was one thing back then... sorry, what was the question again?

AH: So do you think Estonians are more cyber security aware? Maybe because of the events you just mentioned

Q: Yeah, so this is one thing... but yeah... it's drilled into us from school.... We've had our national cyber security strategy.... I think the first one was in 2008, and I'm sure Liis (Rebane) will tell you more about this... everytime

something like this goes on... it's open to the public... so if you are a user who is aware of... and they know what they do... you're aware of it all. Last year we had the problem with the ID cards... it wasn't actually the government but the private company involved in manufacturing the chip for the physical cards... instead of hiding this, we immediately told the public... we communicated it to everyone. It's not about one press conference... it's media everywhere. Issuing guides to fix this, communicating it through different means, digitally etc... so yes. It's not easy, but I think we're very good at this

Participants R & S - 01.03.2018

AH: So I think maybe it's best if I'd sort of introduce myself in the project. Obviously. I'm a PhD researcher. I'm at Royal Holloway University of London. I am working with the University of tartu at the moment. I'm doing a placement here for three months and my research is interested in cyber security in Estonia chiefly. I'm interested in why Estonia there exists such a welcoming attitude to technological innovation and widespread sort of acceptance of it with in daily life.

AH: I think the first thing I really wanted to ask is what does cyber security mean to you because obviously it's a bit of a contested term and it's a very open question

R: Okay cyber security in I mean kind of like a strange position here in CGI Estonia. I'm leading three different teams one is testing teams of software testing team. The other one is usability ux and UI design team and the third one is cyber security, which is a new thing for us to compare or actually it's something that comes with both of them. If you want more usability you lose security if you want more security you lose usability. So it's for I think it's the challenge for everyone for every service provider to find the balance between usability and security. Because you can you can make many things automatic that will do stuff for you, but it's not secure if it does that so there is this kind of balance here always seeking. I didn't know that before starting dealing with both of them.

AH: Yeah, so the famous Benjamin Franklin quote, you may have heard of people who would sacrifice some Liberty for temporary security deserve neither so that there's this idea of balance that sort of I think that transcends really neatly into cyber security at them?

R: but yes service security for me is actually finding the balance and how to put it in words cyber security is everything to do with my security my friends family Security in in cyber areas. So that's that's interesting. I think it should So when you say the balance those they're almost an acceptance that you can never be completely secure. I think it's not that you can never be but it's you don't want to be because otherwise you would lose so much usability so much Liberty that you don't want to do it.

AH: Karen. And what are your thoughts ?

S: you guys are just getting off mute on cyber security. I guess it's made up of largely three major components being people networks. And I think the third one is systems and the weakest link of course is people.... cyber security now that we've entered the realm where our stuff is no longer in a piece of paper (like it is) with the UK... It's about safeguarding the Digital Data that we have and in the similar way that would Safeguard our hard copies of critical information so that cyber security its security just in a digital world

AH: Yeah, so I my next follow-up question to that is what measures do you take to ensure your own cyber security?

R: That's a good one. Not much mostly what's been forced by CGI....

AH? you have quite a relaxed attitude?

R: Hey, I'm very relaxed about it... Actually. I'm not afraid to lose any of my accounts on the internet on Facebook and I'm I don't really care if I lose it. I just make another one don't care.

AH: What about things that contain Bank details and so on?

R: Yeah. Okay Bank details. Yeah, I think that's that's one thing where I use separate passwords, even if there are passwords, they're actually... it's quite limited things you can do on internet Bank using just the password. Mmm,... You have read only for some banks. You can only do have to 200 Euros worth of transactions

So it's limited.. Limited. Yes, it's using either mobile idea smart ID or the ID cards to login. So yeah, these are secure these I kind of like trust maybe maybe because I know there are holes in it as well and they come up every now and then but not not too often, but I kind of like can't worry about them because I can't do anything to fix or anything,

too. To prevent them. So I just what I do is I don't click on suspicious links if I click. I'm really suspicious there and just probably close the browser. Yeah. I'm kind of I'm not using like firewalls, but I'm using Common Sense

AH: do use a VPN

R: VPN. I know I'm not using it at home. We only have VPN if you want to connect to our CGI Network... it's questionable whether it could be better but I'm quite relaxed. I'm not to like scared of sharing my personal data do it do what you want with it. It's worth nothing. Nothing to hide Let Me Tell Ya, that's it.

AH: How about you Karen? Do you take any special measures to ensure your own cyber security?

S: Yeah. I use VPN. I when I'm at work and I browse and websites that are not related to work. So for example, daily papers are Facebook. I open a separate browser window for that. I keep a lot of my critical paperwork like all the purchase papers for my property and stuff in hard copy notarized and stamps in a box at my mom's house. It's also quite old school. Yeah, and because I know that they won't walk if there are mum and dads and birth certificates all that stuff's here. Yeah, and I have an external hard drive. So a lot of stuff is backed up onto that then I keep it I don't plug it into a network. So that's completely separate and then else do I do and I also used the ID card and mobile idea and so forth to log into internet banking and then I do I think that one of the really big key things in Estonia is trust and a lot of people do trust the government eServices, so he wouldn't even question how safe and secure they are I guess because you just trust them but yeah, I do. ... recently because when I was working away, and then I had to use a we had to use our personal email address for work for sensitive stuff. So that had to be backed up so I wouldn't get sued so that that's one of the reasons I had to have so many copies of stuff actually now that you mention it I have copies on my hard drive that is not connected as well. But it's kind of think of it as like a subscriber security aspect. It's like again consensus.

R: Yeah it is because if it Leak you never know what people could do with your with your data. It's maybe being a bit paranoid but and I never clicked on suspicious links and so forth and I really want to close my Facebook account. But because Estonians use it more than they use LinkedIn for self-promotion and so forth. I'm kind of forced to keep it open because of that. I'm kind of old school with with Facebook. I still use it for sharing photos. I only share articles and no work stuff there. It's just like only only the real personal life and only friends like sharing photos of parties and getting swimming naked and stuff like that.

AH: So nothing that connects it to your work?

R: Yeah. I'm sure I'm not using my middle name there either. Older accounts set to private... Probably probably that there was if I remember correctly there was a level of like friends of friends can But not public.

S: So yeah, I go through my phone regularly on settings and check which applications have access to my location and data and camera and microphone and often closing down and I never go through those stupid Facebook games where you can modify your face and stuff, but I do regularly check my phone.

R: Yeah. It's I'm avoiding these things as well. I'm not yeah not sharing information where it's not needed ... but I'm not afraid of couple weeks. I have nothing to hide

S: I just don't like the idea of somebody listening to me. Whatever we write whatever I have something to hide or not.

AH: Yeah. Well that actually brings me neatly onto the next question then so I mean actually what I was going to ask is do you actually utilises a camera cover for any of your smart devices so I can see that you do and then also so do I do to you.

R: Yeah.

AH: Why do you choose to do that?

R: there is Too much evidence that it's a weak spot. And I don't like the idea that someone can just watch me without me knowing that's the reason and of course because each eye is providing such nice covers

AH: mine came from a conference as well. But you would you have gone bought one were the company not providing them?

R: them probably just have would have used good ol sticky.

S: Yeah the sticky note on it.... It's the sticky actually it makes the camera go kind of foggy. Yeah, because the glue sticks on it. Yeah, so When I used to sticking out, I just didn't use my camera at all. Yeah, but now sometimes I use my camera.

S: Yeah, I must have been at you. I don't really use it on my laptop. Anyway, I don't know so much. But but on my phone, yeah on the phone, it's kind of if I would stick it on my phone. It would be just like what is this?

R: Well, I had one and it fell off

S: Yeah, it's obviously because of the revelations I think Yahoo... but I was making a few years ago where people have been spied on through their webcam and the data bus then leaked images were leaked as well. I do not want to be you know, In that segment of people who gets their face thrown into The Ether

AH: question I had so I don't actually have mine with me today, but you can buy small devices which you can plug into the microphone socket of your computer and your smart devices and it recognises that you've actually inserted a microphone in there - a 'mic blocker'. But obviously it isn't recording because it's not actually a microphone to block out sound. Is that something that you use or ?

R: no big deal don't have a microphone plug in the laptop. That's just like it could be now that I think of it we could make a USB device that you could put into one of your USB sockets that thinks it's a microphone but records nothing. Yeah, then you would fool the laptop. Yeah, that's so that that's that's the entire day. So it basically mimic apparently that really cheap way to do it is to buy so the headphones with a microphone just cut them cut them and would leave it plugged in and Device thinks that there's a microphone inserted but it's obviously not recording in that with blanks it out.

AH: But is that something you would consider using or that you think about even?

R: Mmm-hmm? I think I'm not doing sensitive stuff. Yeah, procurements and projects but I didn't know if we would even use anything in our laptop. We probably do a lot of stuff on hard copy. I think both of them together would be really really bad. Yeah video, but actually there are I read an article about People making tests about they were logged in to Facebook chat. I think there's another app for that which I'm not using and the is just starting speaking at home to each other about I think what's it cats or dogs? Right? So like making the conversation look like they have a cat or dog whichever it was but never saying in writing anything about it. Mmm and in a few weeks Facebook started showing ads about animal food.

AH: It wasn't one of these Amazon devices was it?

S: I mean it only responds if you address it put it to function that has to be constantly recording. That's that's different because the study I read about was just about Facebook Messenger app.

R: Yeah, and that's even more of an invasion isn't anything but yeah, I mean that this thing is basically records and then you can have a conversation about something you've never put in your computer and then it gives you a targeted Amazon at that product and it does except try I've tried it and people

S: voluntarily take at least. Yeah, this is something that you know, it is recording because it's listening to it is recording everything because it has to listen to you to respond to but with with the Facebook Messenger app Unless you are on a call. It shouldn't be even listening to anything now and it is but that's the trouble with having a smartphone and especially if it's an Android device because there's so much malware's come out for it, but they could be record-

ing all the time and you wouldn't even know the laptops that the big worry this Smartphone... And the smart phone is always with you on your table, seeing your face and listening to what you're saying as he puts it in his pocket.

R: and actually some of those applications that are constantly recording your location and connections and everything gar is again, the usability versus security issue because it's really cool. If you open Apple Maps and you ask where my car is are you can ask Siri. Where did I park my car and Siri can show it on your map because it's always monitoring your speed and location. And and when your car has the Bluetooth connection when this one got disconnected, where were you when it got disconnected and it can show you where your car is. Where did you park your car? Its usability? It's really useful but security again.

S: Yeah, and I suppose that is also I mean it I do agree with the ethical concerns around you but they're not particularly nice company, but they function on the basis of the service that they offer. Because some people a lot of the a lot of the time I would imagine actually don't read the terms and conditions. I think your average person in the street doesn't read the terms and conditions.... but it does it does it depends what your trade against it? So for example, the new iPhone 8 and above they offer the security feature, whereby you can set to 999 call by pressing a combination of buttons or in your pocket on the phone, for example, so you don't have to take your phone out to make a 999 call and it might be dangerous to do so in certain situations and once it's dialed the emergency call it sends your Two three or four preset numbers so, you know your husband and your kids will know your mother will know where you are when you made that 999: that you've made it so is that a trade of people are willing to accept that you're constantly monitored and when something happens then people will know your location. I would happily accept this in a big city.... but again to come to these permissions, it's good thing that those operation in operation systems in smartphones show which permissions these apps ask because if a flashlight I used to be a flashlight that because there wasn't any like on the operation system for Android downloaded the flashlight app and it requested it requested like everything. Yeah. I was like, you know flashlight. Why do you need my contacts my location... more like

R: Mmm Yeah. Well, I mean if you look at a lot of services that you sign up for now, but I've got online how many times did it ask would you like to log in through Facebook? Even though you haven't ever used the service before and then it's all linked to you know, if you agree to this we get all your contact details and this and that's also something I never do I always go through the hassle. Yeah to creating a profile and if it doesn't affect that I don't use the service.

S: Yeah again something I do but I did they offer that as a service and yeah, it's slightly scary.

R: I actually like to not to think of it. I've been separating my two identities over the Internet. Hmm one is my like Marty. One is another identity, which I work with, I use for like LinkedIn for work and stuff like that and I've even checked every now if there is a link between my Alias and my real account... Look just like Googling both of them seeing if they link to each other and if there is a link somewhere than I just deleted them. Hmm, so probably if you Google my name you won't find my alias accounts anywhere.... but it's not a conscious decision because you know on the earliest account that there's not really anything sensitive. I think it came with like the birth of the internet. Well, I only was another person on the internet bringing Marty to internet. It was like late thing. Yeah. I never it's I think it's like maybe five years ago... but i mean, if anyone really looked...

AH: Yeah. I have a few friends who are teachers are used to be a high school teacher myself ,and certainly on Facebook you had to change your name because the kids would go and look for it ...and they would still find you. I had them pull out smartphones of break time and find my accounts, in spite of checking all the privacy settings. The only was was to change the name of your accounts.

R: Another thing is that I think Facebook pertains your old comments. So I was definitely have found stuff that I should be on Facebook asking, you know restaurants. Are you open at certain times and so forth and I think that was a big issue with the historical data that it retains because you know, it depends on what you've typed and how you've changed your name it still possible to find your brain location and through mutual friends and there's tons of ways to find find people from Facebook... but Yeah, and and the Google search history as well, so you know the incognito mode on Chrome and you Yeah, so it's that's also something that can be used to go online. I still don't trust in those. I use a VPN

AH: I'm gonna bring the conversation back slightly to Smart devices, but not not so much forms this time. Do you take any security precautions with your smart cards? So when I say smart cards mean anything from a bank card to obviously your national identity cards D take any special precautions with them?

R: The only thing I do is I keep I never leave my wallet in the you know in the car and stuff like that. But otherwise Depends if I'm traveling then I will I keep some document separately. So I'll have maybe two wallets with me, but that's because I've lived in South Africa and then you kind of Safeguard against tests and so forth through the use of two separate wallets and highlighting some of your documents and that always taken them with you when I'm in a hotel. I always leave my passport and larger sums of money in a car and a safe if the room has won the stuff like that. But otherwise when traveling I'm also more like mmm awake about these things where I keep my wallet. There's actually good trick that these are doing they put out the sign that saying watch out there are themes around or something like that pickpockets are something that and then what people do it's just check if there are things are if the wallet is still If this phone is still there, and then the thieves see where they are. ... Yeah, I reveal the location. You're amazing location. Yeah, but I'd also do is when I go and take out money from an ATM machine at check the card slot because it was a really big thing that when I lived in the UK yes where they would show I think it was all over the news about how thieves with the slot something into the card slot and then copy your stuff. So I actually always do check that now.

AH: Yeah. No, that's that's yeah 100% to them in your bank card is obviously a key importance of the other thing. I was going to ask out as I know this contactless payments of grown in importance here as well. And in the UK also, do you utilise the contactless feature on your card?

R: Yes, and I used to use in the UK but I held off here until I possibly could I'm only had the contacts contactless card for about a month what I use is I know if you have heard of it. It's a revolute up. Yeah. Yeah there it's really comfortable whenever you pay instantly comes on your phone. Yeah, and you can see here I paid and then the it's like matter of two seconds to shut the shut the car down.

KD: : actually in Estonia can just log onto the internet bank and disable it and change it yourself how you choose to change the limit. You can change the limit you can shut it off you can turn it on with just one click. I must admit I use it all the time though, but I use my is that

AH: You can get an RFID blocker even wallets the block themselves or little individual sleeves that you can put the Cards into something that you've ever considered?

R: we use our cards (CGI cards for building access) also to coming from the door and it's so comfortable just show the whole world. And yeah, if it's all blocked and it wouldn't work

KD: Yeah, yeah. So I've never used those blockers, but I know they exist I haven't really needed run until now. I knew my mom and dad wanted to get my husband a wallet that blocked these things for his Christmas present, but I know he'd never used one and it's just the again usability gets have participated. You want to swipe your oyster card or yeah, you just have to take everything out and then put it back in. It's just annoying.

AH: Ok, so to move on to the Wider state of Security in Estonia, and I wondered if I could ask what you thought the key threats to cyber security?

S: I think complacency maybe could be one because our estate sector is one of the top in the you and one of the Trailblazers, but our pop-up private sector is actually quite bad in terms of cyber security investments in the tension to the to the field. I think we ranked 23rd position somewhere between Bulgaria and Romania when it comes to our private sector safeguarding data... but people still trust it because they trust the government. With services you kind of automatically trust their private sector as well when in fact our data is not secure with all these small. Small or large medium companies here because the day the practice of safeguarding data customer data is not very good.

AH: Do you ever think of threats sort of to Estonia as a country or is it not really the focus on of your own personal cyber security than

S: I guess if you work in the field, I definitely do it, what about you Martii?

R: I think that. Personal cyber security something to worry about if the question was about do I think or do worry about it the national cyber security? I don't really worry about it because I'm there's nothing I can do about it. I don't know too much about it. It so it's rather. It's rather if there's something to worry about and it's a personal part of it. Hmm.

AH: So there's no extra concerns, even though I've seen you have digital identities here?

S: I mean, I'm in charge of this working group in the defence industry Association and we deal with within this working group. We look at ICT and cyber stuff. And as part of that working group, we were definitely worried if you look at Ukraine. I had two major heating failure in my flat in Tallinn over the weekend. I've had to come to talk to Tartu to be warm! So when that happened I thought what if we had a major great failure like happened over there and whether that's - 29, you know, what what would you do and how can we Safeguard against the I don't know how it's being done as I know... The large Etonian companies, They invest in cyber security. Yes, but what about the other ones? How is the whole grid maintained? I don't actually know so there I have as part of that working group.... they are really worried about it as well. But again, there's nothing you can do about it, but you still worried. So... with Ukraine what happened was at the controls were completely taken over by spyware or malware. So now we're that was installed on the controlling PCS and it shows how the controls from the grid side or completely disabled and somebody else's menu is basically manually not mine delivered switching off one by one. Yeah the entire Grant and then people would have to go and switch it on manually and the u.s. Voiced concern over it because in Ukraine being technicians and Engineers still know how to do This manually on site but then the US everything so digital now that a lot of the engineers when they actually showed up on site would know which buttons to press. I think there was to attack some Ukrainians ... They have been having about 15 of them regularly for the past two years,

S: but I think it's both of the big ones. They started from still the weakest link, which is the human being pressing pressing enable content button on Excel sheet,

Speaker 2: maybe but it's basically Russia using Ukraine as a cyber cyber warfare training ground because the researchers have said that they could have gone much much further in the damage. But but it's not been done. It still takes various. Yeah various kind of been techniques and tactics are just test it out to see you know, what will happen. Nearly a quarter of a million households were without electricity in 2016, and the biggest attacks have been in December.

S: I suppose like the stuxnet attacks as wel... I mean, obviously that was a bit more deadly but the potential to replicate that was clear, and usually there's a human error somewhere. That's the trouble with it. Cyber security Experts are hoping that one day humans will be the last,

AH: Stuff like podesta emails are always one of the key of the illustrations when talking about the human side of things, right, because it was it was a phishing scam wasn't it?

S: So well Depending on your viewpoint that it could be replicated here in an Estonian context where an outside actor could potentially influence an election ... I mean definitely. Yeah, I think it's already being done because half a third of us join us. It's in a completely different media space and you can see that very clearly on New Year's Eve when the part of talent has New Year's Eve at 11 p.m. Which is midnight in Moscow. And then the rest of the country has an hour later.

AH: Wow, I didn't know this

S: So they live in a very different information sphere. I know this is anecdotal. But my cleaner is Russian and she's good. She's stateless. She's got the grey passport. Yeah. She doesn't speak a word of Estonian, not even numbers and days of the week... well, you know as a couple, but not really and she's lived here all her life. Yeah, and she sits in a Basically the stuff that she would say to me about the elections and political parties and so at odds with what I would read and think it's quite interesting to witness.

Speaker 3: That's sad that such a huge divide as well.

KH: Yeah, my husband lives in Moscow. So he sees the it was telling me about how he watched the parade and the Pomp and bravado they're attached to it and how they brag about the border with Europe being very weak from Estonia we have a differently guarded border. It's a lot more high-tech. They just deploy a ton of Tanks there and think that this is super secure.

AH: Interesting. So the next thing was going to sort of asked was do you think there's a an Estonian approach to cyber security anything that makes it unique?

S: I personally think it's what's was quite unique to us doing as a country. It's being able to take very Swift action because we're so small. So it's a very agile very fast-moving. I just hate we are able to move fast and in an agile way to threats and a really good example was how the ID card chip issue was handled and because everybody is at such a short distance away from you. You can utilize a lot of experts meet up quickly work through the issues very quickly in the UK, you know, they're 65 million people. It's a big big country. You wouldn't be able to properly move as swiftly.

AH: Yeah

S: here it's a lot. It's just accepted and it's a lot quicker things happen a lot quicker. ... I mean people to set up because people saw the central agency set up ID card renewal stations in shops within days of the fixed coming out. I mean, that's something that would cost a massive amount of money in a bigger country. If you had to do it nationwide, of course here it still cost money, but with Swift the... the overheads are not so bad. So was handled hands of actually really well. Hmm. So I guess that kind of summarises the approach to the cyber security force the issue and that's deal with

Ah: it. Do you think there's also a sort of cultural reason why things are this way? Is it rooted in the history of the country as well why you're able to implement these things?

S: I mean, I have a theory.... I did do a keynote once about why we started as a digital society... And I think a lot of it is to do with the fact that we've only been independent for 25 years. And in the Soviet days, you just had to get stuff done. There wasn't everybody had the same kind of curtains and if your coffee machine a radio broadcast to fix it yourself, my dad used to build TVs out of scratch and it's nothing special. A lot of people could do that. So it's this kind can do make make you know, fixing kind of mentality. That's why I stole and I think has a lot of entrepreneurs as well. One of the highest numbers of startups per capita. People are just very self-sufficient entrepreneurial here and want to get stuff done rather than wait around. You just kind of put your hands to the issue and try and fix it. I think that's maybe it's more may be culturally rooted. We have something here called darn good as well, which doesn't translate into anything. I think in the UK Sweden and didn't have it have it as well. It's when for example, you need your firewood done for the winter and the entire Village would chip in so you basically utilise your community to fix an issue and the most basic example of that would be farm work.

R: I actually think the roots of it are quite far away in history back in the Iron Age where Estonians were living in Huts that burned down every 30 years. Hmm. So basically every year one hopped in a village burned down and they utilised all the village to build it up and it took only like a week to build up again.

S: Yeah, but it's still done. I mean, I used a start a farm and we had everybody came and helped us pick potatoes and get the Harvest in and so forth. There's almost a collectivism as well as a willingness for change.

R: I think yeah, there's and also the change part is got a mentioned. We've only been like independent for 25 years. So if you think of like a national ID coming out mmm think how bad can it be actually can't be worse than like 10 years ago. Yeah.

S: I think it's waning I think the whole Collective thing is waiting like it is globally we're not always the Untouched by all the changes that are going on, but definitely 10-15 years ago. This sense of collectivism and Community wasn't was very strong.

R: yeah and people feel removed and skeptical from the powers that be I suppose. I thought it was an interesting point. Are you saying you could speak to someone who's an MP and then you have those sort of steps of removal. So I when I spoke to someone else they said that they if they wanted to speak to the Prime Minister here within about two or three steps. I guess it's an awful lot more in the UK

AH: Yeah, for sure. I also wonder as well you always say that Scandinavian countries that have this higher level of trust in government. And is there an identity thing? Estonia wanting to be Nordic also?

S: I think they're completely different. Anyway, I mean the whole welfare state that looks after you. I think it's built up in a way where you have to in return trust the government and because it's such a more soft way of governing. It becomes more naturally to people mmm. Yeah, I don't know what with Marty would think of this but I feel it's a very culturally a quite a convenient trade-off in a way because I don't mind the trust the then again leaving independent independent was such a short time that we have known any any different everything difference been worse.

AH: And no real scandals?

S: Yeah, and I don't know if that there's no because there isn't the same level of previous negative experiences here in the independent do our last 25 years. We've been more or less governed by the same political party do it for the whole duration. Of this time and it's the first time now that the more left centre-left parties in power. Mmm. So if you look at the over the last 20 years the format, I went to always been the majority government. It's always been a centre right

R: it's been in the government for 17 years. I think it was yeah straight 17 years. Yeah off the 25 the same sort of powers ideologically. Yeah. I sent her right has been governing this country since

Speaker 1: 1991 more or less. Yeah, but then again now that the left part is on power has been for two years now think about two years year and a half two years. Yeah, not long not long after two years already seems that it's getting worse,

S: but I think the reason is that it's very healthy and necessary for a country to have a balance of powers. So both left and right and the shift here has so thoroughly ingrained certain attitudes in people. That's very very hard to change them and also in the early 90s if you were, you know, a hard bastard, Could you could make it in the business world and other people were left behind and there's a still a very strong sense here that it's like if I could do it you can do it. Everybody is the master of their own fortune and so forth when we are finally now getting into a society where economic relationships are more settled. So people who are wealthy will have children who have access to better education and so forth... the society is kind of layering how the way everybody has an equal starting point in the 90s, but now we don't anymore people want you to think that you can still Get there purely through your own Merit, but it's not really like that anymore. I started actually I think there was a research. I can't remember which you need Cambridge or Oxford that right before the financial crisis Estonia was one of the countries in Europe that had the biggest wealth Gap lastly I think was in the top three with us, but we have a very very big wealth Gap in this country. Hmm. Yeah. It's very easy for for for billionaire to get more billions millionaire to get more Millions than to get the first million. Hmm because

you here with me recently written about this well and this Capital book, but Yeah, I think they the attitudes that those are now being shifted the whole sorry tax the changes and so forth. I mean they've not been implemented that well as either because some of the industry Lobby groups have a lot of say in how policies are enacted and what's put in place and some other groups don't and onto the working groups within so the whole one of the Troubles of agility and that being a fast legislator means that you don't consult with everybody that you maybe should be Consulting with so, you know, a lot of times you'd go into drafting the laws before they're actually put into place. I don't know if that's done here.

S: Is it going to be tough to decide if this technology leaves our ageing population aside that something when we I was in Scotland with a delegation from Estonia meeting the Scottish digital Ministry and so forth and one of the big criticisms they had and worries was that what happens to all be over 50 year olds or over 60 year olds who are completely unversed in any digital technology whatsoever. And we have that in Estonia where Granny's come and you know, give me or their children and their ID cards and access to absolutely all of their credentials to act on their behalf, but that can lead to property theft Financial theft Etc in our own family. Actually. My cousin was stealing from my grandmother because she had given her banking details to my cousin.

AH: really?

S: Yes, a lot of old people who don't know how to use this technology will be very vulnerable..... there was a digital program to train people and give them I think a lot of local councils put on like training courses and so forth, but it's something it's such a massive change in terms of using public services

AH: Yeah,

S: I do. I think the the way it will work here is that it would be a natural replacement. So the old people will die and we already have the skills. So just have to wait 20 years... it sounds cut throat, but it's how it is ...that's kind of how it is at the moment. There's and what's happened with the Services thing is the digital there is a face-to-face Services have been scaled back. The amount of post offices we now have is I think Tallinn has three tartu has one or two. And the customs office here and I've been to the customs office because I do have some I couldn't sort my paperwork out on-line and the queues are massive and they're mostly older people because they don't know how to use any of these services that they should be able to, but if you speak to people from the e-governance department. Oh, yeah, they think everything's hunky-dory.

AH: Thanks. The impression that people here are much more Tech capable. You don't hear the stories of where this system falls down. So that's that's really interesting. Thank you

S: and case with me was I was moving back the first time from South Africa from a third country being a relocation person. I was there was subsidies available to me to relocate without having to pay tax and the goods are imported the second time. I moved back from Dubai again outside of the EU and even the Customs lady herself can organise and work the digital system that we had. So I took me weeks and they're the removal moving company refused to do it for us because it was that complicated, but that might be just a customs thing, but just being there I witnessed a lot of All the people in the mother has worked in banking for 20 years. Yeah, and also a lot of all the people have to come in because they just don't know how to use the services another trouble is elections. So my grandmother for example will ask who should I vote for what number do I put in the box and they don't know how to use the e-voting services and you never know what they what they pop in there

R: I don't know. I'm pretty sure there are negative examples as well. But I only I also know positive examples where old people actually are getting along with it as well. So hmm, it's both ways. I think

S: yeah... I'm just providing the more skeptical views. Well, the thing is a nice PR and it's great and it does work but not for everybody.

AH: Yeah, absolutely. Could you sort of come back to your work? So then what sort of common security concerns do you come across whenever you're so I mean you mentioned there you're talking to the Scottish digital Minister and one of their concerns was with all people. Are there any other major concerns that come from accessibility of Internet? So in Scotland in remote areas, is connectivity an issue?

S: there are some areas where the Internet is slow. It's like 3G or even maybe to G. Yeah at some point so it is slow but mostly this country's covered with at least three G. Mmm. Some of this has been done because we haven't had Legacy infrastructure. There's no be no copper wiring. Yeah, we have we already went very quickly on to newer Technologies... And it's the same thing with banking. We skipped the what's the book called checkbook? Yeah. We skipped the checkbooks books.

AH: You want to read the cards?

S: Yep.

R: But the original question was about yeah, sorry... about the concerns that come up with security? I think bluntly to say stupid people are issue, yes ... a lack of Common Sense would be diplomatic. Yeah.

AH: Is that relating to human error? Then?

R: Yes, I think I agree with current that the weakest link in this cyber security chain is human at the moment. Yeah

S: and already we went over quite a while also in the private sector here. You can see an unwillingness to invest in big cyber security initiatives because it's like housework it never gets finished. But Tiber you can't just do a one-off investment wait five years and then, you know, maybe upgrade the bits and Bobs. It's a continuous improvement process and that's something that people have a hard time wrapping their heads around and their everybody prepares for the best-case scenario rather than for the worst-case scenario that comes out from client meeting

S: the trouble here is as well as that cyber security is still seen as the issue and matter for the IT guys

R: Yeah

S: when it's actually a business issue because of the major outfall as well as reputation as the bottom line that suffers and also in companies don't recover from this depending on how big the breaches... Lloyds is a good one right here when they didn't even disclose the massive data breach they had and I mean trust is very difficult to regain if your main business is selling trust obviously there. Yeah. So yeah, I think major think around it. This business doesn't understand and think that's a global issue. Business doesn't pick up but it's their problem to deal with not just the IT guy

AH: Interesting, and it really interesting into one of my final questions actually, which is do you think that citizens have a role and a responsibility in ensuring their cyber security?

R: Yeah. Yeah.

S: Yeah, absolutely

AH: Just their own, or linked to National Security as well?

S: Anything you would safeguards and paper you would have to safeguard and in the digital world as well. So if the data your own or have access to it implicate her have major major implications, then of course, you must be, you know versed enough in cyber security to safeguard it. Hmm. Otherwise, you should be trusted with it. I think that

AH: do you think it should be the state's responsibility to make sure the people are educated enough in these matters?

S: That's where state has to step in because I know that that's how we learn other things. It's through school and you know media and so forth, and I wanted to actually mention as well as strongly as doing a Big M. Discussion around the new and is directive cyber security directive and how to implement it and put it in practice here and it's brought together various State departments and private sector companies and Academia to debate over these issues. The first two days of debates happened in December and the second days are today, I think and tomorrow in an in an old Manor House in the north of a store near it's probably very romantic their love the snow and over there there the issue of Education was discussed and I saw the briefing paper yesterday and a lot of the original ideas that were discussed in December have dropped out of it sadly. It's thought that cyber security education should start in University and Academia has to be more involved to produce experts and so forth, but it's not just about experts and Academia are going to you need that's already too late. .

AH: Uh-huh

S: yeah, but then so I'm very critical about the way it's being implemented here because I think that the education should start from primary school and that would also mean that more girls would come into the field is currently the only concrete measure that's been entered into it is that we should be able to import Specialists staff from third countries in a more expedited way. that's politically but contentious because Estonia doesn't is not very welcoming to Migrants and rather I think we should educate the wrong people and the massive pool of women who've been untapped. Hmm and in this field and cyber doesn't have to be just coding. It can be a lot of fields legal to and is it a basic cyber hygiene as well? Cyber hygiene should start from primary school, especially if we want to protect our children from internet predators and so forth because they wanted they've been proposing to make the legal age of Internet purchasing here 12 years of age you're able to enter a contract as a purchaser online, but that dogs are means that as a twelve-year-old you should be educated in what how safely to let you do that you get your that doesn't start in University.

R: Yeah do something like with the cars you need a license to drive it. So you actually should need a license to use a computer.

S: Yeah education.

S: So I think it should start a lot earlier and luckily there's some progress has been made in high school level so a buncha gymnasium (high schools), which is the middle of Astoria. They have launched a cyber security track as an elective topic and there were a lot of people have been to make it happen. I think the neighbors - NATO cyber Center was part of it is doing in defense industry Association Minister of Defense. Everybody came together to make that track happen and it's been successfully taught there for quite a few years. So initiatives like this would be great and it also allows girls to enter the the field earlier and consider it as a career just and wise were quite quite bad here in terms of 79 percent of the sector is male

Participant T - 27.02.2019

AH: *Explains premise of the project*

T: I understand, you are rather interviewing me rather as a citizen who has a bigger exposure to tech than an ordinary guy from the street, but not so much the specifics of the technology of guard time

AH: *explains rationale of who is targeted by the research*

T: Yes this is fine, go ahead

AH: What does cyber security mean to you?

T: Well... it's.... i would need to think how to define it. I have been speaking about cyber security a lot, but what does it mean? I think the key, a thing that is often misunderstood, is that it is a process. A journey. Not a state or a solution. I'm not sure if it makes any sense, but essentially, any solution we have, such as our ID cards, our mobile ID's, we have the x-road and blockchain technology solutions. 1) all such solutions have a lifetime, and there will be a point where this is not secure any more. So the question is, cyber security for me is a philosophy of acknowledging that, which is fine, but proper cyber security is only possible when you recognise you will not have a solution which is will not be secure forever, and that you can never be totally secure.

AH: So, as technology constantly evolves, and your devices gradually grow old, updates cease to be published, so you accept this is no longer secure

T: So for example, as you will know, we had this issue with the ID cards recently.... I think in general we handled it very well... and I think that this was way more important for us... how this was handled, more so than the issue itself.... because of course we will have this issue again (another security threat) in the future in some form or another. So i believe this demonstrated that the State can handle these issues pretty well.

T: Then, from a personal perspective, i don't know... I think I just follow common, good practices. Whatever they are. From multi factor authentication, to encrypting your backup drives... but i mean... that's just hygiene.

AH: Cyber hygiene is a term that has come up quite frequently in my time in Estonia, the idea this is a constant process. It has of course been an issue in the UK, as you will know, with the recent wannacry ransomware and how it effected the NHS was a source of embarrassment for the UK government. I think this idea of hygiene probably feeds into my next question to a great extent, which is what methods do you personally take to ensure your own cyber security?

T: I don't think I'm.... well, I'm not paranoid.... i know that my back up drive is sat on my desk... i don't know how secure the encryption is, but I think generally, it's fine... for all relevant accounts, both personal and work, i have multi factor authentication... either via SMS or the authentication app. Well, what else? In general, i am very unhappy with Apple... and every update seems to screw something more usually, it doesn't fix many things. I do the updates... such as an incident a few months ago when we had an issue with wifi security. You essentially shouldn't use wifi in public spaces.... for anything... I still do that. I think there is always a trade off... between usability and security. Maybe I wouldn't do something super sensitive on public wifi in an airport... but reading news online on these connections is fine

AH: Would you not, for example, not make payments on public wifi - such as in a coffee shop?

T: I think i would. It depends, but i think if you use an encrypted channel for it, although it's absolutely possible for a middle man to overhear the traffic... perhaps I'm naive, but as long as the channel is encrypted, i feel it is relatively safe. I still would trust it. There's always trade offs you have to make. The risk of someone looking over your shoulder is probably higher.

AH: Do you use a VPN at all?

T: We do... I do if i need to connect to company services... but for personal reasons... actually i don't. But I have been travelling quite a lot with work, to lets say unusual places... and there i have needed the VPN to access 'normal' internet. In Iran, Sudan, Saudi Arabia... or places like that, for example. However ordinarily, day to day, no. However the company policy is very strict that we do use it for work purposes.

AH: So i noticed before, you have a cover on your laptop camera. Can I ask why?

T: I do. It's a well known concern, I guess. Perhaps the most common is that people can film you watching porn. I don't know how likely, or feasible it is. Whether it's while watching porn, or something more sensitive or relevant... well. I have no practical means to control it. I can't tell if i turn off the camera fully in any other way. I do believe that when these were designed, windows did not intend to include the possibility this could happen, so it is an oversight... I'd almost say that this is verging on not being a cyber security risk, but a matter of potential personal embarrassment. I use conference calls frequently, so i am conscious of the camera more than most I guess.

AH: Do you have any other concerns, such as the security of your microphone. For example, would you use a Mic blocker?

T: Actually, this would be more relevant, as i feel what someone could get from listening to my calls is more relevant than seeing my face. But no, i don't. From a personal perspective though, I think this would be quite paranoid. For work purposes, yes, i see the point a little more, but I think on a personal level, it's not important.

AH: On a similar line of thinking, do you take any precautions with your smart cards. For example, if the cards utilise RFID / contactless, such as your bank cards

T: Not particularly. I do use contactless payments. Again, there is the trade off. The maximum on one transaction is 25 euro.... for me personally, i'd be comfortable with up to 100, but that will vary for others

AH: Would you use an RFID blocker?

T: Not particular, i think these might also be paranoid

AH: Coming away from personal security, and more relating to Estonia as a whole, what do you think are the most important threats to Estonia

T: Outside attacks such as denial of service, the mixed threat of an outside attack and an insider leaking data.... this is an international thing. I am a little biased, as this is what i am working on, but the threat to the integrity of your data, and data manipulation... this is the key threat for me, but I'm not sure if this is number one overall, but for me it is not acknowledged enough. On a smaller scale, small scale attacks in general are possible, but on larger scale, the government systems are well maintained and robust, so I'm not sure there is anything super specific in this regard. We have invested a lot in improving cyber security the other stuff like targeted propaganda is important. It's harder to counter, and it's growing in importance... but I can't really suggest how to counter it. For sure, Russia is threatening in this regard, but I'm not an expert.

AH: Sure. So, i guess my follow up question to that, is what do you feel are the key threats to your personal cyber security?

T: So I'm a little concerned about some of the services i use.... so, i use things like gmail, dropbox and so on.... i do acknowledge these things do get hacked... lets say i took nude pictures.... *laughs* which i haven't... I'm not sure i would trust them to dropbox or google drive, or icloud... so in the back of my head, i do have this potential threat -

usability trade off, and there are certain things i would be cautious of, if these things were to leak, and i would take additional measures

AH: Do you believe there is a uniquely Estonian approach to cyber security? So a lot of outside discourse holds up Estonia as an example, as world leaders in this regard. Do you think there is a unique mindset here which has fostered this approach?

T: Yes.... I do think that this approach is characterising by maximum transparency.... I also think because we make these incidents public... i can't prove nothing has been covered up of course, but I think generally, as we publicise these incidents, it enhances the publics trust. So they trust the e-services because the government acts in an accountable way. It's widely published and shared what has happened, and how it was resolved... and also past incidents where people have been prosecuted for breaking data protection laws... as well as things like someone running bitcoin mining procedures in a hospital. I think this transparency, ever since 2007 (the bronze soldier attacks) has helped. Then, the services were interrupted for a few days, but the more important aspect as the politics behind it. So we have learned from this. Then with e-governance, we have aimed to keep things as transparent as possible. Citizens don't blindly believe everything is secure... but they trust it because things have not been covered up

AH: So you believe there is fundamentally more trust because the government has been transparent in the past?

T: Yes. I think the ability to see your own data, who has seen it, how it has been used... this makes a big difference. Whether the average citizen trusts this, or understands the technology, I'm not so sure, but i do, and i trust it as secure. So it has created this trust in government, and the e-governance model. So i don't think too many people in Estonia believe that whoever is in government can somehow manipulate this. I absolutely would want the current government gone yesterday... so while i don't trust them, i do trust the e-governance systems, and i don't believe they could manipulate it undetected.

AH: So there is obviously many differences between the UK and Estonia. Size of course is one aspect, but another which might have shaped our trust in government is prior scandals, not necessarily regarding cyber security concerns, but overall they undermine trust in public institutions. Do you think, due to the lack of these scandals, as well as the focus on transparency, this has enhanced public trust?

T: Sure. We're a young nation. Around 25 years, so we don't have this legacy... good or bad. But... i mean, when we regained independence, we didn't have anything... in the IT and government systems... but also the old Soviet politicians... most weren't active anymore... so we had very little separation between people and government was very small. We felt... and i suppose still do feel that we are governed by 'one of our own'.... where as in England... you have this legacy of governors... being the same class for hundreds of years... and there further away you are from governors themselves, the less trust you have. So even big incidents, even 50 years ago, not relating to IT at all, can still hurt public trust in the government to make decisions relating to IT in the publics interest. The people who have influenced and introduced these systems are our own... and we have no negative legacy in this regard.... so i can see how this would be difficult to introduce this way of doing things in a different country with its own different legacies.

AH: So, we've touched upon some of these issues anyway, but specifically relating to e-governance, and digital identities, do you believe these systems make Estonians feel more secure?

T: That's tricky.... more secure compared to what?

AH: So, as compared to the alternative, in the UK; we have no identity cards, very limited e-governance, as voters we can arrive at polls with a poll card and vote, so long as our name matches our address and polling card...

T: So i do think these things are more secure than paper, for example. It's easier to fake something on paper. More... or equally importantly.... this trade of between usability is so much better here... i feel it is more secure here.... I sort of accept some risks for the convenience provided by these services... such as the ease of paying my taxes so efficiently

AH: So you accept there are some security risks attached to these services, but opt to use them anyway?

T: Yes. I accept these risks exist, but not that they are higher than doing this on paper.

AH: *explains some of British context*

T: Yes, as a side comment, i have a hard time understanding foreign countries that think in this way. it is unusual to us, and it isn't just the British. I mean, you share so much with so many service providers... google... banks... but you won't share things with your government!?! I think i would trust the Estonian government as much, if not more, than these private companies

AH: Yes, so in Britain we use all of the smart services on smart devices you guys use here.. possibly even more so. Apps like Uber for example, its very popular and the permissions it grants are fairly sweeping, but we all sign up to use it, and no one really checks what happens with your data, so people are content using the service attached. With the government, the thought they could have access to this information is politically.... difficult. Even though, in reality, they probably do obtain it through private companies, if necessary.

T: Yes, it doesn't make sense to us here.

AH: So I'm hoping to discover some of the reasons why we have these differences. I suspect they are social and cultural. So, the final question i ask is that do you feel ordinary citizens have a role and a responsibility in ensuring their own, and the nations cyber security?

T: Definitely.... so i mean... this should be a no brainer.... but if you do not follow cyber hygiene... if things are bad... things can go wrong. Things like voter fraud are possible on a small scale... if i set up different keys, yes fraud is possible on a small level... but the general awareness needs to be there. Cyber security is relevant. Most people are not fluent, or could use more training. My parents, for example, use computers, e-services, banking and governance and even voting, and they are over 70. They often have questions, sure, but they have learned to use it. They have concerns, yes, but they ask me, and i think it's good they actively think about these things. So a certain amount of common sense is required, but where they get this common sense from... I'm not sure. Things are different here. Although sometimes I would rather they used it less... so facebook, using it very actively for example.... I blocked them a while ago *laughs* ... but in general, i think citizens have an important role. I think if people were somehow, inherently incompetent and stupid, and signed anything and everything... and you apply that to the real world... then bad things would happen. The same applies to digital space, so you can't be stupid, or cater for the stupidest things. You shouldn't have to design a system that caters to the very silliest examples. So you have to make a judgement call. You can't assume the user is an idiot all of the time... but of course, you can't assume they are an expert either.

Bibliography

- Aalto, P., 2013. *Constructing Post-Soviet geopolitics in Estonia*. Routledge.
- Abulof, U., 2014. Deep Securitization and Israel's "Demographic Demon". *International Political Sociology*, 8(4), pp.396-415.
- Adams, A. and Sasse, M.A., 1999. Users are not the enemy. *Communications of the ACM*, 42(12), pp.41-46.
- Adamson, L., 2019. Let Them Roar: Small States as Cyber Norm Entrepreneurs. *European Foreign Affairs Review*, 24(2).
- Adey, P. and Anderson, B., 2012. Anticipating emergencies: Technologies of preparedness and the matter of security. *Security Dialogue*, 43(2), pp.99-117.
- Ahn, J. and Jung, Y., 2016. The common sense of dependence on smartphone: A comparison between digital natives and digital immigrants. *New media & society*, 18(7), pp.1236-1256.
- Aistrope, T. and Bleiker, R., 2018. Conspiracy and foreign policy. *Security Dialogue*, 49(3), pp.165-182.
- Albrecht, J.P., 2016. How the GDPR will change the world. *Eur. Data Prot. L. Rev.*, 2, p.287.
- Amicelle, A., Aradau, C. and Jeandesboz, J., 2015. Questioning security devices: Performativity, resistance, politics. *Security dialogue*, 46(4), pp.293-306.
- Amin, A. 2012. *Land of Strangers*, Cambridge, Polity Press
- Amoore, L., 2008. 2 Governing by identity1. *Playing the Identity Card: Surveillance, Security and Identification in Global Perspective*, p.21.
- Amoore, L., 2009. Algorithmic war: Everyday geographies of the War on Terror. *Antipode*, 41(1), pp.49-69.
- Amoore, L., 2013. *The politics of possibility: risk and security beyond probability*. Duke University Press.
- Anderson, B. 2009. On Geography and Materiality, *Environment and Planning A*, 41: 318-335
- Anderson, B. and McFarlane, C., 2011. Assemblage and geography. *Area*, 43(2), pp.124-127.
- Anderson, B. and McFarlane, C. 2011b, Thinking with Assemblage, *Area*, 43: 162-127
- Anthes, G., 2015. Estonia: a model for e-government. *Communications of the ACM*, 58(6), pp.18-20.
- Aradau, C., 2010. Security that matters: Critical infrastructure and objects of protection. *Security Dialogue*, 41(5), pp.491-514.
- Aradau, C., Huysmans, J., Neal, A. and Voelkner, N., 2014. Introducing critical security methods. *Critical Security Methods: New Frameworks for Analysis*, pp.1-22.
- Aradau, C. and Blake, T., 2015. The (Big) Data-security assemblage: Knowledge and critique. *Big Data & Society*, 2(2), p.2053951715609066.
- Aradau, C. and Huysmans, J., 2014. Critical methods in International Relations: The politics of techniques, devices and acts 1. *European Journal of International Relations*, 20(3), pp.596-619.

- Aradau, Claudia. 2010. Security that matters: critical infrastructure and objects of protection. *Security Dialogue*, 41(5) pp. 491–514.
- Ash, J., Kitchin, R. and Leszczynski, A., 2016. Digital turn, digital geographies?. *Progress in Human Geography*, p.0309132516664800.
- Ashenden, D.M., Coles-Kemp, L. and O'Hara, K., 2018. Why Should I?: Cyber security, the security of the state and the insecurity of the citizen. *Politics & Governance*, 6(2), pp.41–48.
- Balzacq, T. and Cavelty, M.D., 2016. A theory of actor-network for cyber-security. *European Journal of International Security*, 1(2), pp.176–198.
- Barnard-Wills, D. and Ashenden, D., 2012. Securing virtual space cyber war, cyber terror, and risk. *Space and Culture*, 15(2), pp.110–123.
- Barnett, C. 2015. On the milieu of security: Situating the emergence of new spaces in public action, *Dialogues in Human Geography*, 5 (3), 257–270
- BBC, 2017. [online] *Could Estonia be the first digital country?*, >Available at: <http://www.bbc.com/future/story/20171019-could-estonia-be-the-first-digital-country>> [Last accessed 14.09.2019]
- BBC News, 2017. [Online] *Security flaw forces Estonia ID 'lockdown'*, <Available at: <https://www.bbc.com/news/technology-41858583>> [Last accessed 14.05.2019]
- Beck, U. 1992. *Risk Society*, London: Sage Publications.
- Beissinger, M. and Kotkin, S. eds., 2014. *Historical legacies of communism in Russia and Eastern Europe*. Cambridge University Press.
- Bélanger, F. and Carter, L., 2008. Trust and risk in e-government adoption. *The Journal of Strategic Information Systems*, 17(2), pp.165–176.
- Benwell, B. and Stokoe, E., 2006. *Discourse and identity*. Edinburgh University Press.
- Berg, B.L., 2004. *Methods for the social sciences*. Pearson Education Inc, United States of America.
- Berg, E., Piret Ehin, eds. 2009. *Identity and Foreign Policy: Baltic-Russian Relations and European Integration*.
- Berg, E. and Ehin, P., 2016. Incompatible identities? Baltic-Russian relations and the EU as an arena for identity conflict. In *Identity and Foreign Policy* (pp. 1–14). Routledge.
- Betz, D.J. and Stevens, T., 2013. Analogical reasoning and cyber security. *Security Dialogue*, 44(2), pp.147–164.
- Björklund, F., 2016. E-government and moral citizenship: The case of Estonia. *Citizenship studies*, 20(6–7), pp.914–931.
- Bloomberg [online], 2018. Lithuania warns Russian Taxi app could be snooping on users, Available online;<https://www.bloomberg.com/news/articles/2018-07-31/lithuania-warns-russian-taxi-app-could-be-snooping-on-users> [accessed 14/05/2019]
- Blue, A., 2020. Evaluating Estonian E-residency as a tool of soft power. *Place Branding and Public Diplomacy*, pp.1–9.
- Booth, K. 1991. 'Security and Emancipation', *Review of International Studies*, 17, 313–26

- Booth, K. 2011. Anchored in Tahrir, *European Security*, 20 (3), 473-479
- Brassett, J. and Vaughan-Williams, N., 2015. Security and the performative politics of resilience: Critical infrastructure protection and humanitarian emergency preparedness. *Security Dialogue*, 46(1), pp.32-50.
- Browning, C.S. and Joenniemi, P., 2004. Regionality beyond security? The Baltic Sea region after enlargement. *Cooperation and Conflict*, 39(3), pp.233-253.
- Browning, C.S. and Joenniemi, P., 2016. Ontological security, self-articulation and the securitization of identity. *Cooperation and Conflict*, p.0010836716653161.
- Browning, C.S. and McDonald, M., 2013. The future of critical security studies: Ethics and the politics of security. *European Journal of International Relations*, 19(2), pp.235-255.
- Buchanan, B., 2016. *The cyber security dilemma: Hacking, trust, and fear between nations*. Oxford University Press.
- Buchanan, B., 2016. *The cyber security dilemma: Hacking, trust, and fear between nations*. Oxford University Press.
- Buchanan, I., 2015. Assemblage theory and its discontents. *Deleuze Studies*, 9(3), pp.382-392.
- Bull, H., 2012. *The anarchical society: a study of order in world politics*. Palgrave Macmillan.
- Bult, J. 2019. Estonia Adrift: How a Digital Pioneer became a source of Political Anxiety, *LRT*[online] Available at: <<https://www.lrt.lt/en/news-in-english/19/1063301/estonia-adrift-how-a-digital-pioneer-became-a-source-of-political-anxiety-opinion>> Last accessed 01.07.2021
- Burlamaqui, L. and Kattel, R., 2016. Development as leapfrogging, not convergence, not catch-up: Towards Schumpeterian theories of finance and development. *Review of Political Economy*, 28(2), pp.270-288.
- Burton, J., 2013. Small states and cyber security: The case of New Zealand. *Political Science*, 65(2), pp.216-238.
- Butler, C., 2012. *Henri Lefebvre: Spatial politics, everyday life and the right to the city*. Routledge.
- Butler, J., 2010. Performative agency. *Journal of cultural economy*, 3(2), pp.147-161.
- Buzan, B., Wæver, O., Wæver, O. and De Wilde, J., 1998. *Security: a new framework for analysis*. Lynne Rienner Publishers.
- Buzan, B. 1991. *People, States and Fear*, 2nd ed.
- Buzan, B. and Hansen, L., 2009. *The evolution of international security studies*. Cambridge University Press.
- Buzan, B. and Wæver, O., 2009. Macrosecuritisation and security constellations: reconsidering scale in securitisation theory. *Review of international studies*, 35(2), pp.253-276.
- Bødker, S. and Greenbaum, J., 1993. Design of information systems: Things versus people. *Gendered by design*, pp.53-63.
- Calis, I., 2017. Routine and rupture: The everyday workings of abyssal (dis) order in the Palestinian food basket. *American Ethnologist*, 44(1), pp.65-76.
- Cameron, D.R. and Orenstein, M.A., 2012. Post-Soviet Authoritarianism: The Influence of Russia in Its "Near Abroad". *Post-Soviet Affairs*, 28(1), pp.1-44.

- Capellupo, M., Liranzo, J., Bhuiyan, M.Z.A., Hayajneh, T. and Wang, G., 2017, December. Security and attack vector analysis of IoT devices. In *International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage* (pp. 593-606). Springer, Cham.
- Cardash, S.L., Cilluffo, F.J. and Ottis, R., 2013. Estonia's cyber defence league: A model for the United States?. *Studies in Conflict & Terrorism*, 36(9), pp.777-787.
- Cavegn, D. 2018 Available at: <https://news.err.ee/866134/finnish-digital-prescriptions-to-become-valid-in-estonia-in-december> *ERR* [Accessed 04.10.18]
- Cavelty, M.D., 2007. *Cyber-security and threat politics: US efforts to secure the information age*. Routledge.
- Cavelty, M.D., 2014. Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. *Science and engineering ethics*, 20(3), pp.701-715.
- Cavelty, M.D. and Balzacq, T. eds., 2016. *Routledge handbook of security studies*. Routledge.
- Chadwick, A., 2003. Bringing e-democracy back in: Why it matters for future research on e-governance. *Social science computer review*, 21(4), pp.443-455.
- Chandler, D., 2012. Resilience and human security: The post-interventionist paradigm. *Security dialogue*, 43(3), pp.213-229.
- Cheskin, A., 2015. Identity and integration of Russian speakers in the Baltic States: A framework for analysis. *Ethnopolitics*, 14(1), pp.72-93.
- Cheskin, A. and Kachuyevski, A., 2019. The Russian-speaking populations in the Post-Soviet space: language, politics and identity.
- Cianetti, L., 2018. Consolidated technocratic and ethnic hollowness, but no backsliding: reassessing Europeanisation in Estonia and Latvia. *East European Politics*, 34(3), pp.317-336.
- Clark, A., 2006. Anonymising research data. Available at: http://eprints.ncrm.ac.uk/480/1/0706_anonymising_research_data.pdf [Last accessed 01.04.2020]
- Coffey & Kochis, 2016. The Role of Sweden and Finland in NATO's Defense of the Baltic States, *The Heritage Foundation* [online], Available at <<https://www.heritage.org/europe/the-role-of-sweden-and-finland-in-natos-defense-of-the-baltic-states>> [accessed 04.05.2021]
- Coleman, M., 2007. Immigration geopolitics beyond the Mexico–US border. *Antipode*, 39(1), pp.54-76.
- Coles-Kemp, L., Jensen, R.B. and Talhouk, R., 2018, April. In a New Land: Mobile Phones, Amplified Pressures and Reduced Capabilities. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (p. 584). ACM.
- Coles-Kemp, L. and Hansen, R.R., 2017, July. Walking the line: The everyday security ties that bind. In *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 464-480). Springer, Cham.
- Collier, J., 2018. Cyber security Assemblages: A Framework for Understanding the Dynamic and Contested Nature of Security Provision. *Politics and Governance*, 6(2), pp.13-21.
- Colwill, C., 2009. Human factors in information security: The insider threat—Who can you trust these days?. *Information security technical report*, 14(4), pp.186-196.
- Craig, A.J. and Valeriano, B., 2018. Realism and Cyber Conflict: Security in the Digital Age. *Realism in Practice*, 85.

- Crampton, J.W., 2015. Collect it all: national security, Big Data and governance. *GeoJournal*, 80(4), pp.519-531.
- Crandall, M. 2016. President Ilves Global Impact, ERR, 11 October 2016, Accessed 2 May 2017, Available at: <http://news.err.ee/119347/matthew-crandall-president-ilves-global-impact>
- Crandall, M. and Allan, C., 2015. Small States and Big Ideas: Estonia's Battle for Cyber security Norms. *Contemporary Security Policy*, 36(2), pp.346-368.
- Crawford, A. and Hutchinson, S., 2015. Mapping the contours of 'everyday security': Time, space and emotion. *British Journal of Criminology*, 56(6), pp.1184-1202.
- Creswell, J.W., 2014. A concise introduction to mixed methods research. SAGE publications.
- Dahl, A.S. and Järvenpää, P. eds., 2013. Northern Security and Global Politics: Nordic-Baltic strategic influence in a post-unipolar world. Routledge.
- Dalby, S., 1992. Security, modernity, ecology: the dilemmas of post-cold war security discourse. *Alternatives*, 17(1), pp.95-134.
- Danyk, Y., Maliarchuk, T. and Briggs, C., 2017. Hybrid war: High-tech, information and cyber conflicts. *Connections*, 16(2), pp.5-24.
- Deibert, R.J. and Rohozinski, R., 2010. Risking security: Policies and paradoxes of cyberspace security. *International Political Sociology*, 4(1), pp.15-32.
- DeLanda, M., 2006. A new philosophy of society: Assemblage theory and social complexity. A&C Black.
- de Leeuw, K.M.M. and Bergstra, J. eds., 2007. The history of information security: a comprehensive handbook. Elsevier.
- Deleuze, G and Guattari, F. 2003. A Thousand Plateaus, 10th printing. Minneapolis: University of Minneapolis Press
- Deleuze, G and Parnet, C. 1987. Dialogues. New York: Columbia University Press.
- Der Derian, J. 1995. The Value of Security: Hobbes, Marx, Nietzsche and Baudrillard in Lipshutz, R (eds) On Security, NY: Columbia University Press, pp 24-45
- Dittmer, J., 2005. Captain America's empire: Reflections on identity, popular culture, and post-9/11 geopolitics. *Annals of the Association of American Geographers*, 95(3), pp.626-643.
- Dittmer, J. 2010. Textual and Discourse Analysis. In DeLyser et al ed. The Sage Handbook of Qualitative Geography. Sage, London, pp 274-286
- Dittmer, J. and Bos, D., 2019. Popular culture, geopolitics, and identity. Rowman & Littlefield.
- Dittmer, J. and Dodds, K., 2008. Popular geopolitics past and future: Fandom, identities and audiences. *Geopolitics*, 13(3), pp.437-457.
- Dittmer, J. and Gray, N., 2010. Popular geopolitics 2.0: Towards new methodologies of the everyday. *Geography Compass*, 4(11), pp.1664-1677.
- Dittmer J. 2014. Geopolitical assemblages and complexity. *Progress in Human Geography* 38(3): 385-401.
- Dourish, P., Grinter, E., Delgado De La Flor, J. and Joseph, M., 2004. Security in the wild: user strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing*, 8(6), pp.391-401.

Drechsler, W., 2018. Pathfinder: e-Estonia as the β -version. *JeDEM-eJournal of eDemocracy and Open Government*, 10(2), pp.1-22.

DTH Azerbaijan. 2019 [online] *Become an e-resident of Azerbaijan*, Available at: <https://dth.azexport.az/become-resident.html> [Last accessed 07/09/2019]

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

Dunn-Cavelty, Kaufmann & Kristensenn. 2010. Resilience & (in)security: Practices, subjects, temporalities, *Security Dialogue*, 46 (1), 3-14

Dunn Cavelty, M., 2012. The militarisation of cyber security as a source of global tension. *Center for Security Studies*.

Dunn Cavelty, M., 2013. From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse. *International Studies Review*, 15(1), pp.105-122.

Dunn-Cavelty, M. 2018. Europe's cyber-power, *European Politics and Society*, 19 (3), 304-320

Duxbery, C. 2020 *Politico* Estonian Tech industry fears far-right <Available at: <https://www.politico.eu/article/estonia-tech-companies-digital-nomads-fear-the-far-right/>> Last accessed 01.04.2020

Dwyer, A.C., 2018. The NHS cyber-attack: A look at the complex environmental conditions of WannaCry. *RAD Magazine*, 44.

e-Estonia, 2018 [online]. Why X Road is not Blockchain <Available at: <https://e-estonia.com/why-x-road-is-not-blockchain/>> [Accessed 04/02/2019]

e-Estonia, 2018a [online] Estonia takes the top spot in the national cyber security index <Available at: <https://e-estonia.com/estonia-takes-the-top-spot-in-the-national-cyber-security-index/>> [Accessed -9/09/2019]

e-Estonia online: Interoperability Services ,2019. Available at: <https://e-estonia.com/solutions/interoperability-services/> e-Estonia.com [Accessed 08.01.19]

e-Estonia online (2018b) *e-Solutions and e-Estonia* <Available at: <https://e-estonia.com/solutions/>> [Accessed 01.10.18]

Eggert, K. 2019. Rise of Estonia's Populist right sends journalists packing , Available at: <https://www.dw.com/en/rise-of-estonias-populist-right-sends-journalists-packing/a-49376584-0> [Accessed 23.07.19]

Ehala, M., 2009. The bronze soldier: Identity threat and maintenance in Estonia. *Journal of Baltic Studies*, 40(1), pp.139-158.

Elden, S., 2004. Understanding Henri Lefebvre. A&C Black.

Elwood, S. and Leszczynski, A., 2013. New spatial media, new knowledge politics. *Transactions of the Institute of British Geographers*, 38(4), pp.544-559.

Enisa.Europa Online. 2018. *National Cyber security Strategies*, Available at: <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/cyber-security-strategy> [Accessed 06.01.18]

- Entman, R.M., 1993. Framing: Toward clarification of a fractured paradigm. *Journal of communication*, 43(4), pp.51-58.
- Erbesen, H., 2019. A parallel yet divided information space: testing the overlap of Yandex Russian language news media discourses in Estonia, Latvia, and Russia. *Russian Journal of Communication*, 11(3), pp.217-239.
- Eriksson, J. and Giacomello, G., 2006. The information revolution, security, and international relations:(IR) relevant theory?. *International political science review*, 27(3), pp.221-244.
- Erizanu, P. 2021. 30 Years After the Fall of the Soviet Union: Is it Finally Time to Stop using the term 'Post-Soviet'?, *Calvert Journal* [online] Available at: <<https://www.calvertjournal.com/features/show/13044/30-years-independence-ussr-term-Post-Soviet-use>> Last accessed 31.08.2021
- ERR, 2017. [online] *Estonia unable to maintain population size without immigration*, Available at: <https://news.err.ee/599528/report-estonia-unable-to-maintain-population-size-without-immigration> [Last accessed 04/04/2019]
- ERR, 2018 [online] *Estonia cancels Security Certificates of 11100 electronic id cards*, Available at: <https://news.err.ee/836259/estonia-cancels-security-certificates-of-11-100-electronic-id-cards> [Last accessed 04/04/2019]
- ERR, 2019 [online] *Number of Stateless Residents in Estonia drops by over 2,200* Available online at: <https://news.err.ee/891967/number-of-stateless-residents-in-estonia-drops-by-over-2-200-in-2018> [Accessed 22.03.2021]
- ERR, 2019a [online] *Juhan Lapassaar elected director of EU agency for cyber security*, <Available at: <https://news.err.ee/962076/juhan-lepassaar-elected-director-of-eu-agency-for-cybersecurity>> [Last accessed 14.09.2019]
- ERR. 2016. [online] *Inequalities holding back Estonia* Available at: <https://news.err.ee/118625/ossinovski-income-inequalities-holding-back-estonia-s-development> [Accessed 01.04.2020]
- ERR. 2021. [online] *Foreign minister: We can initiate ratifying Estonia-Russia border treaty* [Accessed 20.03.2021] Available at: <https://news.err.ee/1608113959/foreign-minister-we-can-initiate-ratifying-estonia-russia-border-treaty>
- Ertan, A., Crossland, G., Heath, C., Denny, D. and Jensen, R., 2020. Cyber security behaviour in organisations. *arXiv preprint arXiv:2004.11768*.
- Eslas, U. 2018. Estonia Neutralizes Sputniks Disinformation Attack. *CEPA* (online) <Available at: <http://www.infowar.cepa.org/Briefs/Est/Estonia-Neutralizes-Sputniks-Disinformation-Attack>> [Last accessed 01/06/2018]
- Estonian Annual Cyber Strategy Assessment, 2019. Available at: <https://e-estonia.com/annual-cyber-security-assessment-2019/> [Accessed 19.07.2019]
- Estonian Cyber security Strategy, 2014. Available at: <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ness-map/strategies/cyber-security-strategy> [Accessed 10.12.2018]
- Evans, M., Maglaras, L.A., He, Y. and Janicke, H., 2016. Human behaviour as an aspect of cyber security assurance. *Security and Communication Networks*, 9(17), pp.4667-4679.
- Finnish Cyber security Strategy, 2015. Available at: <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ness-map/strategies/cyber-security-strategy> [Accessed 10.12.2018]

- Finnish Implementation Programme for Cyber security Strategy, 2017. Available at: <https://turvallisuuskomitea.fi/wp-content/uploads/2018/10/Implementation-programme-for-Finlands-Cyber-Security-Strategy-for-2017-2020-final.pdf> [Accessed 13.12.2017]
- Flowerdew, R & Martin, D. 2013. *Methods in Human Geography*, Abingdon, Routledge
- Fontana, A., & Frey J. (2003). The interview: From structured questions to negotiated texts. In N. Denzin & Y. Lincoln (Eds.). *Collecting and interpreting qualitative materials* (2nd ed., pp. 645-672). Thousand Oaks, CA: Sage.
- Fregonese, S., 2015. Everyday Political Geographies. *The Wiley Blackwell Companion to Political Geography*, pp.493-505.
- Galeotti, M., 2016. Hybrid, ambiguous, and non-linear? How new is Russia's 'new way of war'?. *Small Wars & Insurgencies*, 27(2), pp.282-301.
- Galeotti, M., 2019. *Russian political war: moving beyond the hybrid*. Routledge.
- Galeotti, M., 2019. The Baltic States as Targets and Levers: The Role of the Region in Russian Strategy. *George Marshall European Center for Security Studies: Security Insights*.
- Galeotti, M. 2020. *A Short History of Russia: From the Pagans to Putin*. Ebury Publishing, London.
- Geertz, C., 1994. Thick description: Toward an interpretive theory of culture. *Readings in the philosophy of social science*, pp.213-231.
- Gibson, J.P., Krimmer, R., Teague, V. and Pomares, J., 2016. A review of e-voting: the past, present and future. *Annals of Telecommunications*, 71(7-8), pp.279-286.
- Giddens, A., 1991. *Modernity and self-identity: Self and society in the late modern age*. Stanford university press.
- Giles, K., 2016. *The Next Phase of Russian Information Warfare* (Vol. 20). NATO Strategic Communications Centre of Excellence.
- Giles, K., 2019. *Moscow rules: what drives russia to confront the west*. Brookings Institution Press.
- Goede, M., 2019. E-Estonia: The e-government cases of Estonia, Singapore, and Curaçao. *Archives of Business Research*, 7(2).
- Gold, J. 2019 (online) *How Estonia uses cyber security to strengthen its position in NATO*, <Available at: <https://icds.ee/how-estonia-uses-cybersecurity-to-strengthen-its-position-in-nato/>> [Last accessed 01/09/2019]
- Golovchenko, Y., Hartmann, M. and Adler-Nissen, R., 2018. State, media and civil society in the information warfare over Ukraine: citizen curators of digital disinformation. *International Affairs*, 94(5), pp.975-994.
- Graham, M., 2020. Regulate, replicate, and resist—the conjunctural geographies of platform urbanism. *Urban geography*, 41(3), pp.453-457.
- Graham, M., Zook, M. and Boulton, A., 2013. Augmented reality in urban places: contested content and the duplicity of code. *Transactions of the Institute of British Geographers*, 38(3), pp.464-479.
- Grigas, A., 2012. *Legacies, coercion and soft power: Russian influence in the Baltic States*. London: Chatham House.

- Guardian (No author), 2017. British Troops land in Estonia for NATO mission to deter Russia, Guardian, 18 March 2017, Accessed 24 April 2017, [Available at: <https://www.theguardian.com/uk-news/2017/mar/18/british-troops-land-in-estonia-for-nato-mission-to-deter-russia>]
- Guetterman, T., Creswell, J.W. and Kuckartz, U., 2015. Using joint displays and MAXQDA software to represent the results of mixed methods research. *Use of visual displays in research and testing: Coding, interpreting, and reporting data*, pp.145-175.
- Guitton, C., 2013. Cyber insecurity as a national threat: overreaction from Germany, France and the UK?. *European Security*, 22(1), pp.21-35.
- Haddad, C. and Binder, C., 2019. Governing through cyber security: national policy strategies, globalized (in-) security and sociotechnical visions of the digital society. *Österreichische Zeitschrift Für Soziologie*, 44(1), pp.115-134.
- Hall, P., Heath, C. and Coles-Kemp, L., 2015. Critical visualization: a case for rethinking how we visualize risk and security. *Journal of cyber security*, 1(1), pp.93-108.
- Hansen, L., 2013. Security as practice: discourse analysis and the Bosnian war. Routledge.
- Hansen, L. and Nissenbaum, H., 2009. Digital disaster, cyber security, and the Copenhagen School. *International studies quarterly*, 53(4), pp.1155-1175.
- Hardy, A. 2020, *Estonia's Soft Power Through Technology*, e-IR, viewed 21 November 2020, <<https://www.e-ir.info/2020/02/14/opinion-estonias-soft-power-through-technology/>>
- Hardy, A. 2020a, *Russia Scales e-voting key referendum but misses security issues*, Open Democracy, viewed 21 November 2020, <<https://www.opendemocracy.net/en/odr/russia-scales-e-voting-key-referendum-misses-security-issues/>>
- Hartleb, F., 2020. E-Estonia—"Europe's Silicon Valley" or a New "1984"? In *Redesigning Organizations* (pp. 215-228). Springer, Cham.
- Harvey, F., 2015. "What If" History Matters? Comparative Counterfactual Analysis and Policy Relevance. *Security Studies*, 24(3), pp.413-424.
- Hay, I. 2010. *Qualitative Research Methods in Human Geography*, Oxford, Oxford University Press
- Helemäe, J. and Saar, E., 2012. Estonia—Highly Unequal but Classless?. *Studies of Transition States and Societies*, 4(2).
- Heller, N. 2017. Available at: <https://www.newyorker.com/magazine/2017/12/18/estonia-the-digital-republic> *New Yorker* (online) [Accessed 01.10.18]
- Henshel, D., Cains, M.G., Hoffman, B. and Kelley, T., 2015. Trust as a human factor in holistic cyber security risk assessment. *Procedia Manufacturing*, 3, pp.1117-1124.
- Herzog, S., 2011. Revisiting the Estonian cyber attacks: Digital threats and multinational responses. *Journal of Strategic Security*, 4(2), pp.49-60.
- Herzog, S., 2017. Ten years after the Estonian cyberattacks: Defense and adaptation in the age of digital insecurity. *Geo. J. Int'l Aff.*, 18, p.67.
- Hey, J.A., 2003. Introducing small state foreign policy. *Small states in world politics: Explaining foreign policy behavior*, 1(1).

- Hodgson, C. 2017. The 8 Major Economies with the most inequality, Business Insider, Available at: <https://www.businessinsider.com/the-8-major-economies-with-most-inequality-2017-8?r=US&IR=T#5-israel-037-4> [Last accessed 01.04.2020]
- Hoffmann, T. and Makarychev, A., 2017. Russian speakers in Estonia: Legal,(bio) political and security insights. In *Borders in the Baltic Sea Region* (pp. 147-173). Palgrave, London.
- Horner, J.S., 1998. Research, ethics and privacy: the limits of knowledge. *Public Health*, 112(4), pp.217-220.
- Hossain, K., 2016. Securitizing the Arctic indigenous peoples: A community security perspective with special reference to the Sámi of the European high north. *Polar Science*, 10(3), pp.415-424.
- <https://www.err.ee/934992/gemalto-laks-id-kaardi-hanke-voitja-asjas-riigikohtusse> [Last accessed 14.05.2019]
- Hudson, H. 2005. 'Doing' Security As Though Humans Matter: A Feminist Perspective on Gender and the Politics of Human Security, *Security Dialogue*, 36 (2), 155 - 174
- Hufkin, B (2017) Available at: <http://www.bbc.com/future/story/20171019-could-estonia-be-the-first-digital-country> *BBC News* [Accessed 01.10.18]
- Huysmans, J. 2002. 'Defining Social Constructivism in Security Studies: The Normative Dilemma of Writing Security', *Alternatives*, 27, Special Issue
- Hyndman, J., 2008. Conflict, citizenship and human security: geographies of protection. *War, citizenship, territory*, pp.241-257.
- Høybraten, D. 2018. Trust Behind Nordic Success, *Huffington Post*. Available online; https://www.huffingtonpost.com/dagfinn-hoybraten/trust-behind-nordic-succes_b_6170250.html?guccounter=1 <last accessed 01.04.2018>
- Icelandic Cyber security, 2013. Available at: <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/cyber-security-strategy> [Accessed 12.12.2018]
- Ilves, L. 2019. The case for investment in (cyber) security: Lessons from Estonia. 29 June 2019, Taltech University, Tallinn. 3
- Ilves, T.H. 2017. What is e-identity and why do you need one for the 21st century?. [Online]. 16 March, Stanford University, California. [Accessed 21 April 2017]. Available from: <https://www.youtube.com/watch?v=yP9A4v1mzrY>
- Iso-Markku, T., Innola, E. and Tiilikainen, T., 2018. A stronger North? Nordic cooperation in foreign and security policy in a new security environment.
- Jackson, L & Valentine, G. 2014. Emotion and politics in a mediated public sphere: Questioning democracy, responsibility and ethics in a computer mediated world, *Geoforum* (52) Pp. 193-202
- Jæger, Ø., 2000. Securitizing Russia: Discursive practices of the Baltic states. *Peace and Conflict Studies*, 7(2), pp.18-36.
- Jašina-Schäfer & Cheskin, 2020. Horizontal citizenship in Estonia: Russian speakers in the borderland city of Narva, *Citizenship studies*, 21 (1), 93-110
- Jeanne Hey, (ed.), *Small States in World Politics: Explaining Foreign Policy Behavior* (London: Lynne Rienner 2003) p.1.

- Jensen, B., Valeriano, B. and Maness, R., 2019. Fancy bears and digital trolls: Cyber strategy with a Russian twist. *Journal of Strategic Studies*, pp.1-23.
- Jones, M.O., 2019. The gulf information war | propaganda, fake news, and fake trends: The weaponization of twitter bots in the gulf crisis. *International journal of communication*, 13, p.27.
- Jun, K.N., Wang, F. and Wang, D., 2014. E-government use and perceived government transparency and service capacity: Evidence from a Chinese local government. *Public Performance & Management Review*, 38(1), pp.125-151.
- Kaiser, R., 2015. The birth of cyberwar. *Political Geography*, 46, pp.11-20.
- Kalja, A., 2002. The X-road project. A Project to Modernize Estonia's National Databases. *Baltic IT&T review*, 24, pp.47-48.
- Kalvet, T., 2012. Innovation: a factor explaining e-government success in Estonia. *Electronic Government, an International Journal*, 9(2), pp.142-157.
- Kamais, C.E., 2019. Emerging Security Risks of E-hail Transport Services: Focus on Uber Taxi in Nairobi, Kenya. *International Journal of Security, Privacy and Trust Management (IJSPTM) Vol. 8*.
- Kasekamp, A., 2016. Why Narva is not next. Anne-Sophie Dahl (Ed.). *Baltic Sea Security* (30– 33).
- Kasekamp, A., 2017. A history of the Baltic states. Macmillan International Higher Education.
- Kattel, R. and Mergel, I., 2019. Estonia's digital transformation: Mission mystique and the hiding hand (pp. 143-160).
- Kearns, G., 2009. *Geopolitics and Empire: The Legacy of Halford Mackinder*. Oxford University Press
- Kello, L., 2013. The meaning of the cyber revolution: Perils to theory and statecraft. *International Security*, 38(2), pp.7-40
- Kello, L., 2017. *The Virtual Weapon and International Order*. Yale University Press.
- Kerikmäe, T., Troitiño, D.R. and Shumilo, O., 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), pp.71-80.
- Khan, I & Shahaab, A. 2020. Estonia is a Digital Republic: What that means and why it may be everyones future, *The Conversation* [online], Available at: <<https://theconversation.com/estonia-is-a-digital-republic-what-that-means-and-why-it-may-be-everyones-future-145485>> [Accessed 01.06.2021]
- Kimmo, M.; Pappel, I. & Draheim, D. 2018. 'E-residency as a nation branding case,' in Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance, New York: ACM, pp. 419–428. <https://doi.org/10.1145/3209415.3209447>
- King, G., Keohane, R.O. and Verba, S., 1994. *Designing social inquiry: Scientific inference in qualitative research*. Princeton university press.
- Kinsley, S., 2014. The matter of 'virtual' geographies. *Progress in Human Geography*, 38(3), pp.364-384.
- Kitchin, R., 2013. Big data and human geography Opportunities, challenges and risks. *Dialogues in human geography*, 3(3), pp.262-267.
- Kitchin, R. and Dodge, M., 2011. *Code/space: Software and everyday life*. Mit Press.

- Kitsing, M., 2011. Success Without Strategy: E-Government Development in Estonia. *Policy & Internet*, 3(1), pp.1-21.
- Kitsing, M. 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, New York: ACM, pp. 59–68. <https://doi.org/10.1145/3209415.3209453>
- Klein, N., 2014. *Capitalism vs. the Climate*. Alternative Radio.
- Kolsaker, A. and Lee-Kelley, L., 2008. Citizens' attitudes towards e-government and e-governance: a UK study. *International Journal of Public Sector Management*.
- Kompella, L., 2020. Socio-Technical Transitions and Organizational Responses: Insights from E-governance Case Studies. *Journal of Global Information Technology Management*, 23(2), pp.89-111.
- Koopman S. 2011. Alter-geopolitics: Other securities are happening. *Geoforum* 42(3): 274–284.
- Korjus, K. 2018. [online] We told you about our potential security vulnerability, here is an update <Available at: <https://medium.com/e-residency-blog/we-told-you-about-a-potential-security-vulnerability-heres-our-update-86e04119b734>> Last accessed 23.07.2019
- Kosenkov, A., Pappel, I. and Draheim, D., 2019, April. On Existing Trends towards Creation of a Holistic Socio-technical Approach to e-governance. In *Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance* (pp. 492-493).
- Kotka, T., Vargas, C. and Korjus, K., 2015a. Estonian e-Residency: Redefining the nation-state in the digital era. *University of Oxford Cyber Studies Programme working paper*, 3.
- Kremlin.ru. 2005. [online] Available at: http://kremlin.ru/events/president/news/eng/speeches/2005/04/25/2031_type70029type82912_87086.shtml Last accessed 03/02/2019
- Kristoffersen, B., 2014. 'Securing' geography: Framings, logics and strategies in the Norwegian High North. *Polar geopolitics*, pp.131-148.
- Krivý, M., 2021. "Post-Apocalyptic Wasteland" or "Digital Ecosystem"? Postsocialist Ecological Imaginaries in Tallinn, Estonia. *Geoforum*, 126, pp.233-243.
- Kurtz, G. and Meyer, C.O., 2019. Is conflict prevention a science, craft, or art? Moving beyond technocracy and wishful thinking. *Global Affairs*, 5(1), pp.23-39.
- Kuus, M., 2002a. Toward cooperative security? International integration and the construction of security in Estonia. *Millennium*, 31(2), pp.297-317.
- Kuus, M., 2018. The terroir of bureaucratic practice: Everyday life and scholarly method in the study of policy. *Environment and Planning C: Politics and Space*, p.0263774X18802954.
- Kuus, M. 2002. European Integration in Identity Narratives in Estonia: A Quest for Security, *Journal of Peace Research*, 39 (1), 91-108
- Kuznetsova, A., 2020. Finno-Ugric World (s) and "Language Brotherhood". In *Baltic-Black Sea Regionalisms* (pp. 117-129). Springer, Cham.

- Kuzio, T., 2019. Russian stereotypes and myths of Ukraine and Ukrainians and why Novorossiia failed. *Communist and Post-Communist Studies*, 52(4), pp.297-309.
- Kyiv Post, 2019. Zelenskiy expresses interest in cooperation in IT and cyber security with Estonia, *Kyiv Post* [online] Available at: <https://www.kyivpost.com/ukraine-politics/zelenskiy-expresses-interest-in-cooperation-in-it-and-cybersecurity-with-estonia.html> [Last accessed 09/10/2019]
- Lacy, M. and Prince, D., 2018. Securitization and the global politics of cyber security. *Global Discourse*, 8(1), pp.100-115.
- Lanoszka, A., 2016. Russian hybrid warfare and extended deterrence in eastern Europe. *International Affairs*, 92(1), pp.175-195.
- Lauristin, M. and Vihalemm, P., 2009. The political agenda during different periods of Estonian transformation: External and internal factors. *Journal of Baltic Studies*, 40(1), pp.1-28.
- Lee-Geiller, S. and Lee, T.D., 2019. Using government websites to enhance democratic E-governance: A conceptual model for evaluation. *Government Information Quarterly*, 36(2), pp.208-225.
- Lee-Geiller, S. and Lee, T.D., 2019. Using government websites to enhance democratic E-governance: A conceptual model for evaluation. *Government Information Quarterly*, 36(2), pp.208-225.
- Lefebvre, H., 1991. *Critique of everyday life* (Vol. 2). Verso.
- Lefebvre, H. and Levich, C., 1987. The everyday and everydayness. *Yale French Studies*, pp.7-11.
- Lehtola, V.P. 2015. in Spangen, M., Salmi, A.K., Äikäs, T. and Lehtola, V.P., 2015. Sámi histories, colonialism, and Finland. *Arctic Anthropology*, 52(2), pp.22-36.
- Leichtova, M., 2016. *Misunderstanding Russia: Russian Foreign Policy and the West*. Routledge.
- Leszczynski, A., 2015. Spatial big data and anxieties of control. *Environment and Planning D: Society and Space*, 33(6), pp.965-984.
- Liik, K. 2020. Why the Baltic States behave as they do towards Russia, Carnegie Moscow [online] Available at <<https://carnegiemoscow.org/commentary/83540>> [Accessed 02.01.2021]
- Mac Ginty, R., 2019. Circuits, the everyday and international relations: Connecting the home to the international and transnational. *Cooperation and Conflict*, p.0010836719832343.
- Mäe, R., 2017. The Story of e-Estonia: A discourse-theoretical approach. *Baltic Worlds*. URL: <http://balticworlds.com/the-story-of-e-estonia>.
- Makarychev, A. and Yatsyk, A., 2016. Celebrating borderlands in a wider Europe: Nations and identities in Ukraine, Georgia and Estonia. Nomos Verlag.
- Malatji, M., Von Solms, S. and Marnewick, A., 2019. Socio-technical systems cyber security framework. *Information & Computer Security*.
- Mälksoo, M., 2015. 'Memory must be defended': Beyond the politics of mnemonical security. *Security Dialogue*, 46(3), pp.221-237.
- Mälksoo, M., 2018. Countering hybrid warfare as ontological security management: the emerging practices of the EU and NATO. *European security*, 27(3), pp.374-392.

- Mäliksoo, M. 2012. Hard Memory, Soft Security: Competing Securitization of the Legacy of Communism in Eastern Europe. *East European Memory Studies* [Online] 9:17-20.
- Mäliksoo, M., 2021. A ritual approach to deterrence: I am, therefore I deter. *European Journal of International Relations*, 27(1), pp.53-78.
- Männiste, M. and Masso, A., 2018. The role of institutional trust in Estonians' privacy concerns. *Studies of Transition States and Societies*, 10(2).
- Manor, I., 2019. *The digitalization of public diplomacy*. Cham: Palgrave Macmillan.
- Manor, I., 2020. The Russians are Laughing! The Russians are Laughing! How Russian Diplomats Employ Humour in Online Public Diplomacy. *Global Society*, pp.1-23.
- Marcus, G & Saka, E. 2006. *Assemblage, Theory, Culture and Society*, 23, 101-106
- Margetts, H. and Naumann, A., 2017. Government as a platform: What can Estonia show the world. *Research paper, University of Oxford*.
- Martin, K.M., 2016. *Everyday Cryptography: Fundamental Principles and Applications*, Oxford University Press
- McBrien, N. 2020. Defending the vote: Estonia Creates a Network to Combat Disinformation, Innovations for Successful Societies, Princeton University [online] Available at <<https://successfulsocieties.princeton.edu/>> [Accessed 01/05/2021]
- McFarlane, T. and Hay, I., 2003. The battle for Seattle: protest and popular geopolitics in The Australian newspaper. *Political Geography*, 22(2), pp.211-232.
- McGlynn, C. and Rackley, E., 2017. Why 'upskirting' needs to be made a sex crime. *The conversation*.
- McGraw, G., 2013. Cyber war is inevitable (unless we build security in). *Journal of Strategic Studies*, 36(1), pp.109-119.
- McLean, I. and McMillan, A., 2009. *The concise Oxford dictionary of politics*. OUP Oxford.
- McNab, A. 2000. *Firewall*, Welbeck Publishing, London
- McNamara, E.M., 2017. Between Trump's America and Putin's Russia: Nordic-Baltic security relations amid transatlantic drift. *Irish Studies in International Affairs*, 28, pp.73-98.
- McNamara, E. 2021. Estonia's Outgoing Government Leaves Damaged Security Legacy, *Foreign Policy Research Institute*, viewed 01 April 2021 <<https://www.fpri.org/article/2021/02/estonias-outgoing-government-leaves-damaged-security-legacy/>>
- McNamara, E.M. and Sulg, M.L., 2020. The Baltic states in NATO: An evolving transatlantic bargain from newcomers to President Trump. In *NATO and Transatlantic Relations in the 21st Century* (pp. 142-166). Routledge.
- McSweeney, B., 1999. *Security, identity and interests: a sociology of international relations* (Vol. 69). Cambridge University Press.
- Mearsheimer, J.J., 2014. Why the Ukraine crisis is the West's fault: the liberal delusions that provoked Putin. *Foreign Aff.*, 93, p.77.

- Medaglia, C.M. and Serbanati, A., 2010. An overview of privacy and security issues in the internet of things. In *The Internet of Things* (pp. 389-395). Springer New York.
- Meehan, K., Shaw, I.G.R. and Marston, S.A., 2013. Political geographies of the object. *Political Geography*, 33, pp.1-10.
- Meehan, K et al. 2013. Political Geographies of the Object, *Political Geography*, 33, 1-10
- Meijer, Albert. 2015. "E-governance Innovation: Barriers and Strategies." *Government Information Quarterly* 32 (2): 198–206. Accessed September 6, 2016. doi:10.1016/j.giq.2015.01.001.
- Mejias, U.A. and Vokuev, N.E., 2017. Disinformation and the media: the case of Russia and Ukraine. *Media, Culture & Society*, 39(7), pp.1027-1042.
- Ministry of Foreign Affairs for the Russian Federation, 2016. Doctrine of Information Security for the Russian Federation [online] available at: http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/Cpt-ICk6BZ29/content/id/2563163 [accessed 01/02/2019]
- Mitzen, J., 2006. Ontological security in world politics: State identity and the security dilemma. *European Journal of international relations*, 12(3), pp.341-370.
- Morozov, V., 2009. Obsessed with identity: the IR in Post-Soviet Russia. *Journal of International Relations and Development*, 12(2), pp.200-205.
- Morozov, V., 2015. *Russia's postcolonial identity: A subaltern empire in a Eurocentric world*. Springer.
- Morozov, V. and Fofanova, E., 2016. Imperial Legacy and the Russian-Baltic Relations: From Conflicting Historical Narratives to a Foreign Policy Confrontation?. In *Identity and Foreign Policy* (pp. 15-32). Routledge.
- Morrissey, J., 2011. Closing the neoliberal gap: risk and regulation in the long war of securitization. *Antipode*, 43(3), pp.874-900.
- Mudde, C., 2014. A New (Order) Ukraine? Assessing the Relevance of Ukraine's Far-right in an EU Perspective. *Open Democracy*, 28.
- Mudde, C., 2019. *The far-right today*. John Wiley & Sons.
- Mueller, R.S., 2019. The Mueller report: Report on the investigation into Russian interference in the 2016 presidential election. WSBLD.
- Müller, M. 2008. 'Reconsidering the concept of discourse for the field of critical geopolitics: Towards discourse as language and practice', *Political Geography* 27 (3):322-338.
- Müller, M. 2010. 'Doing discourse analysis in Critical Geopolitics', *Online Journal of Political Geography and Geopolitics*, 12 [Online] Available at: <<http://espacepolitique.revues.org/1743>> [Accessed 16/08/2013]
- Mutlu, Can E. 2013b. "The Material Turn." In: *Research Methods in Critical Security Studies. An Introduction*. Ed. Mark. B. Salter and Can E. Mutlu. London and New York: Routledge, 173-179.
- National Security Concept of Estonia, 2010 [online] Available at: http://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_security_concept_of_estonia.pdf [Accessed 02/02/2019]
- NATO CCDCOE, 2018. Available at: <https://ccdcoe.org/cyber-security-strategy-documents.html> NATO *CCD-COE* [Accessed 09.10.18]

- Neocleous, M., 2008. *Critique of security*. Edinburgh University Press.
- Neocleous, M., 2016. *The Universal Adversary: Security, Capital and 'the Enemies of All Mankind'*. Routledge.
- Nunes, J. 2012. Reclaiming the Political: Emancipation and critique in Security Studies, *Security Dialogue*, 43 (4), 345-361
- Nye Jr, J.S., 2009. Get smart: Combining hard and soft power. *Foreign affairs*, pp.160-163.
- Nye Jr, J.S., 2013. From bombs to bytes: Can our nuclear history inform our cyber future?. *Bulletin of the Atomic Scientists*, 69(5), pp.8-14.
- Nyman, J., 2016. What is the value of security? Contextualising the negative/positive debate. *Review of International Studies*, 42(5), pp.821-839.
- Nyman-Metcalf, K. and Repytskyi, T., 2016. Exporting good governance via e-governance: Estonian e-governance support to Eastern partnership countries. In *Political and Legal Perspectives of the EU Eastern Partnership Policy* (pp. 81-100). Springer, Cham.
- OECD, 2019 (online) *Economic Survey of Estonia - Overview*. Available at: <https://www.oecd.org/economy/estonia-economic-snapshot/> [Last accessed 21/03/2021]
- O'Flaherty, K. 2019. [online] *Huawei Security Scandal - Everything you need to know*, Available at: <https://www.forbes.com/sites/kateoflahertyuk/2019/02/26/huawei-security-scandal-everything-you-need-to-know/#3a41d83c73a5> [Last accessed 14.05.2019]
- O'Neill, M., 2016. Insecurity by design: Today's IoT device security problem. *Engineering*, 2(1), pp.48-49.
- Paasi, A., 2003. Region and place: regional identity in question. *Progress in human geography*, 27(4), pp.475-485.
- Paasi, A. 2006. Texts and contexts in the globalising academic marketplace: comments on the , debate on geopolitical remote sensing. *Eurasian Geography and Economics*, 216-220
- Pain, R. and Smith, S. eds., 2008. *Fear: Critical geopolitics and everyday life*. Ashgate Publishing, Ltd..
- Pain R. 2009. Globalized fear: Towards an emotional geopolitics. *Progress in Human Geography* 33(4): 466-486.
- Panke, D. and Gurol, J., 2018. Small states as agenda-setters? The Council Presidencies of Malta and Estonia. *Journal of Common Market Studies*, 56(S1), pp.142-151.
- Pappel, I., Pappel, I. and Saarmann, M., 2012. Digital records keeping to information governance in Estonian local governments. *i-Society*, pp.25-28.
- Pappel, I. and Pappel, I., 2011, January. Implementation of service-based e-government and establishment of state IT components interoperability at local authorities. In *Advanced Computer Control (ICACC), 2011 3rd International Conference on* (pp. 371-377). IEEE.
- Papp-Váry, Á. 2018. A Successful Example of Complex Country Branding: The e-Estonia Positioning Concept and Its Relation to the Presidency of the Council of the EU. *Acta Universitatis Sapientiae, European and Regional Studies*, (14), 87-115.
- Parsovs, A., 2020. Estonian electronic identity card: security flaws in key management. In *29th {USENIX} Security Symposium ({USENIX} Security 20)* (pp. 1785-1802).
- Patton, M.Q., 2002. *Qualitative evaluation methods*. Sage. London

- Paul, C. 2016. Confessions of a Hybrid Warfare Skeptic. *Small Wars Journal* [online] Available at: <<https://smallwarsjournal.com/jrnl/art/confessions-of-a-hybrid-warfareskeptic>> [Accessed 10/02/2021]
- Peoples, C. and Vaughan-Williams, N., 2014. *Critical security studies: An introduction*. Routledge.
- Petsinis, V., 2019. Ethnopolitics in Central and Eastern Europe in a State of Flux. *Ethnopolitics*, 18(4), pp.379-382.
- Petsinis, V. 2019. 'Hijacking the Left? The Populist and Radical Right in Two Post-Communist Polities', in Left Radicalism and Populism in Europe (chapter 8, p.p. 156-180), Routledge Studies in Radical History and Politics.
- Philo, C., 2012. Security of geography/geography of security. *Transactions of the Institute of British Geographers*, 37(1), pp.1-7.
- Pieper, M., 2018. Russkiy mir: the geopolitics of Russian compatriots abroad. *Geopolitics*, pp.1-24.
- Pigman, L., 2018. Russia's vision of cyberspace: a danger to regime security, public safety, and societal norms and cohesion. *Journal of Cyber Policy*, pp.1-13.
- Poller, A., Waldmann, U., Vowé, S. and Türpe, S., 2012. Electronic identity cards for user authentication-promise and practice. *IEEE Security & Privacy*, 10(1), pp.46-54.
- President.ee [online] 2018. *With Iceland we will digitally transform the nordic circle*, Available at: <https://www.president.ee/en/media/press-releases/14408-president-kaljulaid-with-iceland-we-will-digitally-transform-the-nordic-circle/index.html> [Accessed 10.12.18]
- Priisalu, J. and Ottis, R., 2017. Personal control of privacy and data: Estonian experience. *Health and technology*, 7(4), pp.441-451.
- Putin, V. 2021. On the historical unity of Russians and Ukrainians, *kremlin.ru* [online] Available at: <<http://en.kremlin.ru/misc/66182>> [Last accessed 01.08.2021]
- Rabinow, P., 2003. *Anthropos Today*. Princeton, NJ: Princeton University Press.
- Raento, P. 2011. Introducing Popular Icons of Political Identity, *The Geographical Review*, 101 (1), iii-vi
- Raik, K., Aaltola, M., Pynnöniemi, K. and Saloniemi-Pasternak, C., 2015. Pushed together by external forces? The foreign and security policies of Estonia and Finland in the context of the Ukraine crisis. *FIIA Briefing Paper*, 167.
- Ranganathan, M. 2015. Storm Drains as Assemblages: The Political Ecology of Flood Risk in Post-Colonial Bangalore. *Antipode*, 47: 1300-1320
- Raun, T.U., 2002. *Estonia and the Estonians (Second Edition)*. Hoover Inst Press.
- Reisinger, H. and Golts, A., 2014. Russia's Hybrid Warfare. *Research Paper, NATO Defense College*, (105).
- Renz, B., 2016. Russia and 'hybrid warfare'. *Contemporary Politics*, 22(3), pp.283-300.
- Reynolds, M. 2016. Digital Estonia, *Wired* (online), 20 October 2016, Accessed 28 April 2017 [Available at: <http://www.wired.co.uk/article/digital-estonia>]
- Rid, T., 2012. Cyber war will not take place. *Journal of strategic studies*, 35(1), pp.5-32.
- Rid, T., 2013. *Cyber war will not take place*. Oxford University Press, USA.

- Rid, T. and Buchanan, B., 2015. Attributing cyber attacks. *Journal of Strategic Studies*, 38(1-2), pp.4-37.
- Rid, T., 2016. *Rise of the Machines: the lost history of cybernetics*, Scribe, Melbourne & London
- Rislakki, J., 2014. The Case for Latvia. *Disinformation Campaigns Against a Small Nation: Fourteen Hard Questions and Straight Answers about a Baltic Country* (Vol. 15). Rodopi.
- Robinson, N. and Hardy, A., 2020. From the “Bronze Night” to cyber security pioneers. *Routledge Companion to Global Cyber-Security Strategy*.
- Robinson, N., Hardy, A. & Ertan, A., 2022. Estonia: A Curious and Considered Approach to Artificial Intelligence and National Security. *Routledge Companion to Global AI Strategy*.
- Robinson, N. and Martin, K., 2017. Distributed Denial Of Government: The Estonian Data Embassy Initiative. *Network Security*, 2017(9), pp.13-16.
- Roe, P., 2008. The ‘value’ of positive security. *Review of International Studies*, 34(4), pp.777-794.
- Rose, G., 2015. Rethinking the geographies of cultural ‘objects’ through digital technologies Interface, network and friction. *Progress in Human Geography*, p.0309132515580493.
- Rose, G., 2016. *Visual methodologies: An introduction to researching with visual materials*. Sage.
- Rumer, E.B., 2017. *Russian foreign policy beyond Putin*. Routledge.
- Runnel, P., Pruulmann-Vengerfeldt, P. and Reinsalu, K., 2009. The Estonian Tiger leap from post-communism to the information society: from policy to practice. *Journal of Baltic Studies*, 40(1), pp.29-51.
- Sakwa, R., 2017. *Russia against the rest: The post-cold war crisis of world order*. Cambridge University Press.
- Sakwa, R., 2020. Greater Russia: Is Moscow out to subvert the West?. *International Politics*, pp.1-29.
- Salminen, M., Zojer, G. and Hossain, K., 2020. Comprehensive cyber security and human rights in the digitalising European High North. In *Digitalisation and Human Security* (pp. 21-55). Palgrave Macmillan, Cham.
- Salminen, M. and Hossain, K., 2018. Digitalisation and human security dimensions in cyber security: an appraisal for the European High North. *Polar Record*, 54(2), pp.108-118.
- Salonius-Pasternak, C., 2018. 6 Finland’s ambiguous deterrence. *Deterring Russia in Europe: Defence Strategies for Neighbouring States*.
- Salter, M.B., 2015. *Making Things International 1: Circuits and Motion*. University of Minnesota Press.
- Salter, M.B. and Mutlu, C.E. eds., 2013. *Research methods in critical security studies: An introduction*. Routledge.
- Särav, S. and Kerikmäe, T., 2016. E-residency: a cyberdream embodied in a digital identity card?. In *The Future of Law and eTechnologies* (pp. 57-79). Springer, Cham.
- Schmidt, E. and Cohen, J., 2013. *The new digital age: Reshaping the future of people, nations and business*. Hachette UK.
- Schryen, G. and Rich, E., 2009. Security in large-scale internet elections: a retrospective analysis of elections in Estonia, the Netherlands, and Switzerland. *IEEE Transactions on Information Forensics and Security*, 4(4), pp.729-744.

- Schulze, E. 2019: online. *How Estonia became a digital society* <Available at: <https://www.cnn.com/2019/02/08/how-estonia-became-a-digital-society.html>> [Last accessed 20.7.19]
- Scott, T. 2014 [online] *Estonians embrace life in a digital world* <Available at: <https://www.nytimes.com/2014/10/09/business/international/estonians-embrace-life-in-a-digital-world.html>> [Last accessed 14.09.2019]
- Sear, T. 2017. Cyber Attacks Ten Years On, *The Conversation* (online). <Available at; <https://theconversation.com/cyber-attacks-ten-years-on-from-disruption-to-disinformation-75773>> [Last accessed 01/06/2018]
- Sharp, J.P., 1993. Publishing American identity: popular geopolitics, myth and The Reader's Digest. *Political geography*, 12(6), pp.491-503.
- Sheldon, J.B., 2014. Geopolitics and cyber power: Why geography still matters. *American Foreign Policy Interests*, 36(5), pp.286-293.
- Shires, J. 2020. Cyber-Noir: Cybersecurity and Popular Culture, *Contemporary Security Policy*, 41 (1), pp. 82-107
- Sicari, S., Rizzardi, A., Grieco, L.A. and Coen-Porisini, A., 2015. Security, privacy and trust in Internet of Things: The road ahead. *Computer networks*, 76, pp.146-164.
- Sidaway, J.D. and Power, M., 2005. 'The tears of Portugal': empire, identity, 'race', and destiny in Portuguese geopolitical narratives. *Environment and Planning D: Society and Space*, 23(4), pp.527-554.
- Snyder, A.A., 1997. *Warriors of disinformation: American propaganda, Soviet lies, and the winning of the Cold War: an insider's account*. Arcade Publishing.
- Snyder, T., 2011. *Bloodlands: Europe between Hitler and Stalin*. Random House.
- Soll M, Salvet S and Masso A, 2015. Changes in language policy in Estonia: Self-descriptions of Russian-speaking students. *Trames: Journal of the Humanities and Social Sciences* 19(3): 221-247.
- Solvak, M., Unt, T., Rozgonjuk, D., Võrk, A., Veskimäe, M. and Vassil, K., 2018. E-governance diffusion: Population level e-service adoption rates and usage patterns. *Telematics and Informatics*.
- Solvak, M. and Vassil, K., 2018. Could Internet Voting Halt Declining Electoral Turnout? New Evidence That E-Voting Is Habit Forming. *Policy & Internet*, 10(1), pp.4-21.
- Sparke, M.B., 2006. A neoliberal nexus: Economy, security and the biopolitics of citizenship on the border. *Political geography*, 25(2), pp.151-180.
- Springall, D., Finkenauer, T., Durumeric, Z., Kitcat, J., Hursti, H., MacAlpine, M. and Halderman, J.A., 2014, November. Security analysis of the Estonian internet voting system. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (pp. 703-715). ACM.
- Springer, S., Chi, H., Crampton, J., McConnell, F., Cupples, J., Glynn, K., Warf, B. and Attewell, W., 2012. Leaky geopolitics: The ruptures and transgressions of WikiLeaks. *Geopolitics*, 17(3),
- Steinsson, S. and Thorhallsson, B., 2019. *Small State Foreign Policy*.
- Sterling, B (2017) Available at: <https://www.wired.com/beyond-the-beyond/2017/08/meanwhile-estonian-e-identity/> *Wired* [Accessed 04.10.18]
- Stevens, D. and Vaughan-Williams, N., 2016a. Everyday security threats: Perceptions, experiences, and consequences.

Stevens, T., 2018. Global Cyber security: New Directions in Theory and Methods. *Politics and Governance*, 6(2), pp.1-4.

Stevens, T., 2020. Knowledge in the grey zone: AI and cyber security. *Digital War*, pp.1-7.

Stevens, T. 2018. The Internet of Things; When objects threaten national security. *The Conversation* (online) <Available at: <https://theconversation.com/internet-of-things-when-objects-threaten-national-security-96962>> [Last accessed 01/06/2018]

Suslov, M., 2018. Russian World” concept: Post-Soviet geopolitical ideology and the logic of “spheres of influence. *Geopolitics*, 23(2), pp.330-353.

Talant, B. 2019. Estonia has shown the path to successful e-Government (online) <Available at: <https://www.kyivpost.com/ukraine-politics/president-kaljulaid-estonia-has-shown-the-path-to-successful-e-government.html?cn-reloaded=1>> [Last accessed 14.09.2017]

Talving, L. 2020. Freedom House. Estonian Election - An Executive Summary Available at: <https://www.ecoi.net/en/document/2035820.html>

Tamppuu, P. and Masso, A., 2018. ‘Welcome to the virtual state’: Estonian e-residency and the digitalised state as a commodity. *European Journal of Cultural Studies*, p.1367549417751148.

Thompson, T. 2019 [online] *Countering Russian disinformation the Baltic nations’ way*, The Conversation, <Available at: <https://theconversation.com/countering-russian-disinformation-the-baltic-nations-way-109366>> [Last accessed 20.08.2019]

Thomson, M. 2019 [online] Scotland should look to Estonia for the digital future, The Scotsman. <Available at: <https://www.scotsman.com/business/comment-scotland-should-look-to-estonia-for-the-digital-future-1-4947321>> [Last accessed 02/09/2019]

Thorhallsson, B., 2006. The size of states in the European Union: Theoretical and conceptual perspectives. *European Integration*, 28(1), pp.7-31.

Thorhallsson, B., 2012. Small states in the UN Security Council: means of influence?. *The Hague Journal of Diplomacy*, 7(2), pp.135-160.

Thorhallsson, B., 2017. *The role of small states in the European Union*. Routledge.

Thorhallsson, B. ed., 2018. *Small states and shelter theory: Iceland’s external affairs*. Routledge.

Thorhallsson, B., 2018a. Nordicness as a shelter: the case of Iceland. *Global Affairs*, 4(4-5), pp.377-390.

Tlostanova, M., 2012. Postsocialist≠ postcolonial? On Post-Soviet imaginary and global coloniality. *Journal of Post-colonial Writing*, 48(2), pp.130-142.

Toal, G., 2017. *Near abroad: Putin, the West and the contest over Ukraine and the Caucasus*. Oxford University Press.

Trenin, D., 2011. Russian Policies toward the Nordic-Baltic Region. *Nordic-Baltic Security in the 21st Century. The Regional Agenda and the Global Role*, Atlantic Council.

Trenin, D., 2016. *Should we fear Russia?*. John Wiley & Sons.

Trenin, D. 2020. Respect thy neighbour: Russia and the Baltic Region, Carnegie Moscow [online], Available at: <<https://carnegiemoscow.org/commentary/83539>> [Accessed 02.01.2021]

- Trimbach, D.J. and O'Lear, S., 2015. Russians in Estonia: Is Narva the next Crimea?. *Eurasian Geography and Economics*, 56(5), pp.493-504.
- Tyler, I., 2010. Designed to fail: a biopolitics of British citizenship. *Citizenship studies*, 14(1), pp.61-74. University Press, Oxford, UK.
- UN Development Report. 1994 [online] Available :<http://hdr.undp.org/en/content/human-development-report-1994> [Accessed 29.12.18]
- Vaarik, D. 2015. Where Stuff Happens First: White Paper on Estonia's Digital Ideology. Retrieved from https://www.mkm.ee/sites/default/files/digitalideology_final.pdf [accessed 18 Mar 2019]
- Valeriano, B. and Maness, R.C., 2015. *Cyber war versus cyber realities: Cyber conflict in the international system*. Oxford University Press, USA.
- VanderStoep, S.W. and Johnson, D.D., 2008. *Research methods for everyday life: Blending qualitative and quantitative approaches* (Vol. 32). John Wiley & Sons.
- van Wijk, S., Lemke, F. and Draheim, D., 2020, November. On the Narratives of e-Government: A Comparison of the Democratic and Technocratic Approach in Post-Soviet States. In *International Conference on Electronic Governance and Open Society: Challenges in Eurasia* (pp. 3-16). Springer, Cham.
- Vassil, K., 2016. Estonian e-Government ecosystem: Foundation, applications, outcomes. *Background paper for World Development Report*.
- Vassil, K. 2015. Estonian e-Government Ecosystem. Foundation, Applications, Outcomes, World Bank. Retrieved from <http://pubdocs.worldbank.org/en/165711456838073531/WDR16-BP-Estonian-eGov-ecosystem-Vassil.pdf> [accessed 18 Mar 2019] <https://doi.org/10.1017/S0265052503202132>
- Vassil, K. and Weber, T., 2011. A bottleneck model of e-voting: Why technology fails to boost turnout. *New media & society*, 13(8), pp.1336-1354.
- Vaughan-Williams, N. and Stevens, D., 2016. Vernacular theories of everyday (in) security: The disruptive potential of non-elite knowledge. *Security Dialogue*, 47(1), pp.40-58.
- Vilson, M., 2020. Framing the EU and the Green Deal in Estonia: A reluctant balancing act.
- Vinkel, P. and Krimmer, R., 2016, October. The how and why to internet voting an attempt to explain E-Stonia. In *International joint conference on electronic voting* (pp. 178-191). Springer, Cham.
- VM.fi Finnish Ministry of Finance, 2018. Available at: <https://vm.fi/en/public-services-will-be-digitalised> *VM Ministry of Finance* [Accessed 09.10.18]
- Vojinović, Zoran; Abbott, Michael B. 2012. *Flood risk and social justice: from quantitative to qualitative flood risk assessment and mitigation*. London: IWA Publishing
- Volkamer, M., Renaud, K., Kulyk, O. and Emeröz, S., 2015, September. A socio-technical investigation into smartphone security. In *International Workshop on Security and Trust Management* (pp. 265-273). Springer, Cham.
- Von Solms, R. and Van Niekerk, J., 2013. From information security to cyber security. *computers & security*, 38, pp.97-102.
- Wæver, O., 1993. *Securitization and desecuritization* (p. 48). Copenhagen: Centre for Peace and Conflict Research.

- Warf, B., 2015. Cyberwar: A new frontier for political geography. *Political Geography*, (46), pp.89-90.
- Whitman, M.E. and Mattord, H.J., 2011. *Principles of information security*. Cengage Learning.
- Williams, J. and Boyce, G.A., 2013. Fear, loathing and the everyday geopolitics of encounter in the Arizona borderlands. *Geopolitics*, 18(4), pp.895-916.
- Wilson III, E.J., 2008. Hard power, soft power, smart power. *The Annals of the American Academy of Political and Social Science*, 616(1), pp.110-124.
- Wodak, R. and Meyer, M. eds., 2009. *Methods for critical discourse analysis*. Sage.
- Wood, E. and Latham, K.F., 2009. Object knowledge: Researching objects in the museum experience. *Reconstruction*, 9(1).
- Work in Estonia, 2021. The Ukrainian Community in Estonia, *Work in Estonia* [online] Available at <<https://www.workinestonia.com/living-in-estonia/ukrainian-community-in-estonia/>> Last accessed 06.04.2021
- Wrange, J. and Bengtsson, R., 2019. Internal and external perceptions of small state security: the case of Estonia. *European Security*, 28(4), pp.449-472.
- Yang, L., Elisa, N. and Eliot, N., 2019. Privacy and security aspects of E-government in smart cities. In *Smart cities cyber security and privacy* (pp. 89-102). Elsevier.
- Yatsyk, A., 2018. A popular geopolitics of the refugee crisis in Europe: The re-actualization of identity-driven geopolitical narratives in Estonia. *Geopolitics*, 23(4), pp.803-822.
- YLE, 2017. Ministry Working Group Says 'Not Yet' to Online Voting, *YLE* [online] Available at: <https://yle.fi/uutiset/osasto/news/ministry_working_group_says_not_yet_to_online_voting_in_finland/9984736> [Accessed 09.10.18]
- Zayani, M., 2015. *Networked Publics and Digital Contention: the politics of everyday life in Tunisia*. Oxford University Press.
- Zetter, K. 2018. Inside the cunning, unprecedented hack of Ukraine's power grid, *Wired* [online] Available at: <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/> [Last accessed 02/04/2019]
- Zissis, D. and Lekkas, D., 2011. Securing e-Government and e-Voting with an open cloud computing architecture. *Government Information Quarterly*, 28(2), pp.239-251.
- Zojer G. . (Forthcoming 2019). The Interconnectedness of Digitalisation and Human Security in the European High North: Cyber security Conceptualised through the Human Security Lens. *The Yearbook of Polar Law*, 9.
- Zook, M. and Graham, M., 2007. From cyberspace to DigiPlace: Visibility in an age of information and mobility. *Societies and cities in the age of instant access*, pp.241-254.