Distributed Denial-of-Government:

The Data Embassy and the geopolitical, diplomatic and legal implications of extraterritorial data storage

Nicholas David Robinson

Thesis submitted to the University of London for the degree of Doctor of Philosophy

September 2020
Declaration of Authorship

I, Nicholas David Robinson, hereby declare that this thesis and the work presented in it is entirely my own. Where I have consulted the work of others, this is always clearly stated.

Signed:

Date: 20/09/2020
Abstract

In 2018, the Estonian government opened the world’s first Data Embassy in Betzdorf, Luxembourg. Aimed at ensuring the ‘digital continuity’ of the Republic of Estonia, the Data Embassy will backup critical components of the state (such as key information systems, databases and registries) to the cloud, ensuring the state can endure in the event of an emergency or national crisis. Operated from a government-controlled data centre outside of its own borders, the Data Embassy will have functions akin to those of a traditional embassy, guaranteeing similar diplomatic immunities to Estonian data and information systems held on its server racks. For a country that has a high dependency on its digital infrastructure, and a history of facing up to threats to its continuity and political independence, the Data Embassy has emerged as a radical and profound attempt at tackling the many ontological insecurities Estonia faces today. Indeed, for other states around the world - particularly those facing limited political recognition, existential threats to their independence, or threats from natural hazards and climate change – the premise of extraterritorial data storage and ‘hibernating’ the state may be an appealing anticipatory logic in an increasingly uncertain world, with the Data Embassy’s arrival pointing to a radical shift in how states may look to function and endure in the future.

In this thesis, I explore the geopolitical, diplomatic and legal implications of extraterritorial data storage, specifically, in the context of a state-level emergency or crisis. With a focus on the novel Estonian Data Embassy - and what many might consider an attempt at ‘backing up’ the state to the cloud - I examine how this potentially transformative e-government/national security innovation calls into question many long-held assumptions around conventional forms of geopolitics, diplomacy and international law. Drawing on nearly three years of ethnographic engagements with Estonian policymakers, cybersecurity professionals, academic experts and those working close to the Data Embassy project itself, I contextualise the initiative alongside Estonia’s own unsettled past and uncertain future, arguing that its emergence is intertwined in a much deeper state continuity project that is rooted in the ontological insecurities and collective memory of the state today.

Fundamentally, this is a thesis about the changing nature of statehood and diplomacy in a digital age. Through a critical examination of the Estonian Data Embassy and the environment it necessitates, it questions what the Data Embassy reveals (or, conversely, ‘masks’) about the everyday practice and performance of the state – from revelatory extraterritorial archival practices that predate the Data Embassy itself, to the ontological insecurities facing the state today that point to a deep-seated anxiety at its centre. It also considers what the Data Embassy’s emergence may mean for the future practice of diplomacy, critiquing whether new diplomatic relations will begin to form in and around the ‘digital embassy’ and the extraterritorial space of the data centre.

Providing one of the first in-depth, critical studies into the Data Embassy, this thesis draws together a number of emerging interdisciplinary debates from across areas of geopolitics, cybersecurity and diplomatic studies. In doing so, it makes a number of significant contributions to these fields of research, developing new insights into anticipatory logics of statehood in a digital age; state-level anxieties (and their distinct temporalities) and how other emotions/affects may be identified at a collective level in world politics; and the emergence of a novel form of digital diplomacy that is sited within the extraterritorial data centre, and how this may herald changes to outmoded international agreements such as the Vienna Convention. With the potential advent of more Data Embassies in the future, such debates will undoubtedly intensify and converge as other states (and non-state actors) are allured by the promise of extraterritorial data storage. As such, this thesis should be of interest to a wide-range of stakeholders, from scholars working on issues of statehood/political legitimacy and with interests in data extraterritoriality and diplomatic law, to policymakers working in areas of cyber resilience and national security, and IT professionals with interests in cloud computing and disaster recovery management.
Contents

ABSTRACT .......................................................................................................................... I

CONTENTS .......................................................................................................................... II

LIST OF FIGURES AND TABLES ........................................................................................ IV

LIST OF ABBREVIATIONS ................................................................................................. VI

LIST OF PUBLICATIONS .................................................................................................... VII

ACKNOWLEDGEMENTS ..................................................................................................... IX

CHAPTER 1 - INTRODUCTION ........................................................................................... 1

  1.1 KEEPING THE REPUBLIC ALIVE: ESTONIAN CONTINUITY PAST AND PRESENT ............ 3
  1.2 BACK TO THE FUTURE? RUSSIA, PUTIN AND THE SPECTRAL GEOGRAPHIES/GEOPOLITICS OF THE NEAR ABROAD .............................................................. 8
  1.3 BACKING UP THE STATE: THESIS OUTLINE AND EARLY PROVOCATIONS ................ 10

CHAPTER 2 – DIPLOMACY, INFRASTRUCTURES AND AFFECTIVE GEOPOLITICS ............ 20

  2.1 GEOPOLITICAL INFRASTRUCTURES ........................................................................... 21
  2.2 THE IMPROVISED STATE ........................................................................................... 30
  2.3 NEW DIPLOMATIC STUDIES ....................................................................................... 33
  2.4 AFFECTIVE GEOPOLITICS ......................................................................................... 40
  2.5 CONCLUSION .............................................................................................................. 45

CHAPTER 3 – RESEARCHING THE DATA EMBASSY ......................................................... 49

  3.1 RESEARCHING EMOTION, AFFECT AND THE ANXIOUS STATE ................................... 51
  3.2 EMBODIED ESTONIAN ENCOUNTERS: ELITES, EXPERTS, NETWORKS .......................... 55
      3.2.1 Studying up: ethnography and the state ................................................................. 56
      3.2.2 Elite today, gone tomorrow .................................................................................. 59
      3.2.3 Interviewing reflexively ........................................................................................ 62
  3.3 DATA EMBASSY DISCOURSE: REPORTS, BILATERAL AGREEMENTS AND PROPAGANDA 65
  3.3.1 Letting your (geopolitical) imagination run free ..................................................... 67
  3.3.2 Terminology matters ............................................................................................... 69
  3.3.3 Where lies the scrutiny? ........................................................................................... 70
  3.4 FAILURE IN THE FIELD: THE PRECARITY OF RESEARCH/ THE DATA EMBASSY ........ 72
      3.4.1 Researching a 'government as a startup' ............................................................... 73
      3.4.2 No confidence, no Data Embassy? ....................................................................... 74
  3.5 CONCLUSION .............................................................................................................. 75

CHAPTER 4 – A CATALYST FOR THE CLOUD ................................................................. 79

  4.1 TIGERS AND UNICORNS: ESTONIA’S RISE TO DIGITAL POWERHOUSE .................. 80
      4.1.2 Estonia’s pivot to the West: a story of resilience, alliances and strategies (2001-2008) .......... 84
      4.1.3 The ‘Skype effect’: framing creativity, trust and diplomatic cooperation (2008-present) ....... 91
  4.2 FRAMING THE DATA EMBASSY ................................................................................. 97
      4.2.1 Government cloud ............................................................................................... 99
      4.2.2 From embassy to data centre ................................................................................ 104
      4.2.3 Brexit, Betzdorf and bilateral agreements ............................................................. 106
  4.3 CONCLUSION .............................................................................................................. 115
List of Figures and Tables

**Figure 1.1** - The EBRC European Reliance Centre East, located in Betzdorf, Luxembourg
(source: www.datacenters-in-europe.com; copyright: EBRC – WIDE David Laurent)

**Figure 1.2** - August Torma (*left*) and Ernst Jaakson (*right*) - ambassadors without a country?
(sources: blog.vm.ee and commons.wikimedia.org)

**Figure 1.3** - Unmarked counterinsurgency fighters that arrived in Crimea shortly after the 2014
annexation – Russian military or (as Putin described) local ‘self-defence groups’?
(source: www.bbc.co.uk)

**Figure 1.1** - A typical media depiction of a data centre, often used when reporting on the Data Embassy
(source: www.securitytoday.com)

**Figure 2.1** - A 2015 map depicting global undersea cable infrastructure in the style of a Victorian-era
map of the world (source: www.blog.teleography.com)

**Figure 2.3** - A common depiction of ‘the cloud’ found across industry and media
(source: www.innovationatwork.ieee.org)

**Figure 2.4** - One of Europe’s largest data centres, Next Generation Data, based on an industrial park on
the outskirts of Newport, Wales (source: www.nextgenerationdata.co.uk)

**Figure 2.5** - Images taken from a visit to Hack Green, a former government-owned nuclear bunker in
Cheshire, UK. Now the site of a museum, an area of the site has also been retrofitted into a
modern data centre (author’s own images)

**Figure 2.6** - A recent screenshot of the U.S. ‘Virtual Embassy’ in Iran, a government website that was
first launched in 2011 by then Secretary of State Hillary Clinton (source: ir.usembassy.gov)

**Figure 3.1** - The Office of the President of the Republic of Estonia, located in Kadriorg park on the
outskirts of Tallinn (author’s own image)

**Figure 3.2** - Bar charts representing interviewee demographics in terms of gender, nationality, workplace
sector, and affiliation/knowledge of the Data Embassy project.

**Figure 3.3** - A map indicating what a network of Estonian ‘Data Embassies’ may look like in the future
when in full operation (author’s own image)

**Figure 4.1** - My view sat behind the Estonian Prime Minister Jüri Ratas and his National Digital Advisor
Marten Kaevats during a roundtable discussion at the Tallinn Digital Summit
(October 2018) (author’s own image)

**Figure 4.2** - Restoration diplomacy: (i) Estonian President Lennart Meri (*left*) with Russian President
Boris Yeltsin (*right*) during the signing of the July Treaties (26 July 1994) which negotiated
the withdrawal of Soviet troops from Estonia later that year; (ii) Estonian Prime Minister
Mart Laar (*right*) meets with President of the European Commission Jacques Delors (*left*)
shortly before signing an agreement with the European Economic Community (EEC) (19

**Figure 4.3** - A popularised overview of Estonia’s X-Road architecture (source: www.ria.ee)

**Figure 4.4** - A visual representation of how the Estonian Data Embassy could be situated (and
demarcated) within a government-operated data centre, including the use of key-card access
(NB: this is the author’s own depiction and does not claim to accurately represent the data
centre design – nor is it to any scale)

**Figure 4.5** - Screenshot of Twitter conversation between Taavi Kotka and Gilles Feith on the morning
after the Brexit vote (source: www.twitter.com)

**Figure 4.6** - Estonian Prime Minister Jüri Ratas tweeting after the signing of the bilateral agreement
between Estonia and Luxembourg (source: www.twitter.com)
Figure 5.1 - A pivot from East to West? An image from ‘downtown’ Tallinn where the modern business district stands in sharp contrast to the city’s existing material Soviet architecture (author’s own image)

Figure 5.2 - The Estonian Embassy in Kensington, London. An example of an embassy location where key databases may have been stored (source: www.globalestonian.com)

Figure 5.3 - A tweet from former Estonian President Toomas Hendrik Ilves, outlining why the 2007 cyberattacks were a positive for the country (source: www.twitter.com)

Figure 5.4 - Recent branding used by the Estonian government for its e-Residency programme (source: www.brand.estonia.ee)

Figure 5.5 - The ‘Welcome to Estonia’ logo, developed by Interbrand in 2002 (source: www.worldvectorlogo.com)

Figure 6.1 – A collection of images taken during a visit to the Estonian city of Narva in August 2017, located on the border with Russia (author’s own images)

Figure 6.2 - An image of Kaleva, the civilian passenger and transport plane that was shot down while en route from Tallinn to Helsinki on 14 June 1940 (source: Helsingin Sanomat Oy/HS Arkisto)

Figure 6.3 - Estonian President Toomas Hendrik Ilves delivering a speech on Victory Day in Valga, 23 June 2014 – the first major public speech following the annexation of Crimea (source: www.president.ee)

Figure 7.1 - The Tallinn TV tower - located just outside of capital. Built in time for the 1980 Moscow Olympics, the tower is a symbolic, material reminder of Estonia’s Soviet past (author’s own image)

Figure 7.2 - A visual metaphor depicting the cloud-based backup for ISIS, taken from Carl Miller’s (2020) article on the topic (source: www.wired.co.uk)

Figure 7.3 - Jüri Ratas (left) and Xavier Bettel (right), Prime Ministers of Estonia and Luxembourg respectively, after signing the bilateral agreement regarding the establishment of the world’s first Data Embassy (source: www.estonianworld.com)

Figure 7.4 - Luxembourg Prime Minister Xavier Bettel tweeting following a visit from Estonian President Kersti Kaljulaid – a sign of greater diplomatic cooperation between the two countries? (source: www.twitter.com)

Figure 7.5 - Estonia’s ‘virtual embassy’ in the internet-based virtual world of Second Life (source: MoFA, 2017)

Figure 8.1 – An image of Tallinn’s Old Town skyline (author’s own image)

Table 1 - An overview of a number of state-led technological advancements in Estonia since 2000

Table 2 - An overview of different public-sector approaches to cloud computing

Table 3 - A timeline of key events in the development of the Data Embassy

Table 4 - A comparison of startup and Data Embassy characteristics
List of Abbreviations

APRA – The Peruvian Aprista Party

AWS – Amazon Web Services

BCE – Before the Common Era

CCDCOE – The NATO Cooperative Cyber Defence Centre of Excellence

CIO – Chief Information Officer

CTO – Chief Technology Officer

DDoS – Distributed Denial-of-Service attack

EU – The European Union

FCO – The British Foreign and Commonwealth Office

FSB – Federal Security Service of the Russian Federation

GDP – Gross Domestic Product

HM – His/Her Majesty’s

ICDS – International Centre for Defence and Security

ICT – Information and Communications Technology

MoEAC – Estonian Ministry of Economic Affairs and Communications

MFAs – Ministry of Foreign Affairs | MoFA – Estonian Ministry of Foreign Affairs

MoU – Memorandum of Understanding

NASA – The National Aeronautics and Space Administration

NATO – North Atlantic Treaty Organization

NGO – Non-Governmental Organisation

NIST – National Institute of Standards and Technology

OECD – The Organisation for Economic Co-operation and Development

ROCA – Return of Coppersmiths Attack (a cryptographic vulnerability)

R&D – Research and Development

VCCR – Vienna Convention on Consular Relations (1963)

VCDR – Vienna Convention on Diplomatic Relations (1961)
List of Publications

Listed below are the four publications that were completed during the course of this research, elements of which have been replicated in thesis (as stated below):


My first publication was an opportunity to write publicly about the Data Embassy for the first time, and to sketch out a number of ideas for this thesis. It was published in a Special Issue in Network Security on the theme of nation-state cyberattacks. My co-author and supervisor Professor Keith Martin initially brought the Special Issue to my attention and made the initial pitch to the editor. I then worked on a number of initial drafts and Keith then offered comments and edits at various stages before submitting. The article’s content can be regarded as ‘early thoughts’ on my research and the Data Embassy (there are even a few inaccuracies as the project and Data Embassy have evolved so much during this time), so there isn’t much content replicated throughout this thesis – there is, however, the odd paragraph or sentence included throughout the thesis (e.g. the introduction to Chapter 4).

My second publication was a bi-product of my three-month stint as a visiting PhD researcher in the Ragnar Nurkse Department of Innovation and Governance at Tallinn University of Technology (TTÜ – now TalTech). During that time, I coordinated a small research project with colleagues from TTÜ and the University of Tartu on the Data Embassy and its impact upon international law. Working alongside Professor Robert Krimmer and PhD researcher Laura Kask, we produced an exploratory research paper for ICEGOV’19 in Melbourne, Australia (3-5 April, 2019). Robert and I spent a great deal of time discussing ideas initially, before we joined up with Laura and gained a great deal from her legal experience and time working on the Data Embassy project1. I completed the initial drafts on this paper, with additional contributions from Laura on legal semantics and argument. Robert assisted with final comments. This paper

---

1 Laura Kask was the legal officer in the Ministry of Economic Affairs and Communications and had sole responsibility for legal aspects of the Data Embassy initiative. Laura helped draft the bilateral agreement that was signed between Estonia and Luxembourg (see Chapter 4) and worked closely on the project in its early stages before moving into the private sector.
shaped lots of my thinking in the latter stages of writing this thesis and sections of text are thus replicated in a number of sections – in particular, Section 4.2 where an overview of the Data Embassy is provided¹.

In my third publication, I worked with fellow postgraduate colleague Angharad Butler-Rees on a short intervention piece for a Special Issue in the journal *Emotion, Space and Society*. This opportunity arose from a session we organised as part of the RGS-IBG Annual International Conference in Cardiff, UK (August 2018). The session was entitled “Emerging voices in political geography: navigating challenges, barriers and failures in the field”, and was in part motivated by Harrowell et al.’s (2018) work on ‘Making Space for Failure in Geographic Research’, and spurred on by our own personal experiences of encountering various challenges in the field (and beyond) as postgraduate research students. Angharad and myself contributed an equal amount to the paper, and divided our own experiences into individual sections – and both equally contributed to an introduction, conclusion and epilogue. My section focussed on my personal experience researching the Data Embassy and the contingent nature of research in the face of many setbacks and complications. My edited contribution to this paper is replicated in Chapter 3 (see Section 3.4).

In my final publication, I worked with fellow postgraduate colleague Alex Hardy on a book chapter for an edited collection on global cybersecurity policy and national strategies. Focussing on the Estonian approach, we detailed Estonia’s recent cyber history and its introduction of a national cybersecurity strategy (one of the first of its kind). Providing an overview of three iterations of Estonia’s Cyber Security Strategy (2008-2013, 2014-2017, 2019-2022), we chart the many organisational, legislative and diplomatic changes implemented by the Estonian government in this period, also highlighting some of challenges faced. Alex and myself contributed equal amounts to the chapter, with my own contributions to the chapter being shaped by the research conducted in this thesis. There are no specific sections of text replicated between both chapter and this thesis.

¹ I would also like to express my gratitude to my funders for the opportunity to spend time researching this paper and wider thesis research in Tallinn, Estonia. I was in large part supported as part of the EPSRC Centre for Doctoral Training in Cyber Security at Royal Holloway, University of London (EP/K035584/1), and partially from the Dora Plus program funded by the European Regional Development Fund.
Acknowledgements
Writing this thesis has been one hell of a journey – from London to Tallinn, and Egham, Northampton, Huddersfield and everywhere else in between. There are a number of people I would like to thank, without whom this research would not have been possible.

Firstly, I would like to thank my two supervisors, Klaus Dodds and Keith Martin, for their constant support, advice and encouragement throughout the duration of this project. Klaus, from inspiring me throughout my Masters, to the support you showed in the last few days before submitting this thesis, I will always remember the care, kindness and faith you have shown in me over the past 6-7 years. In the beginning, you reassured me that I could approach this journey differently, and that I could gain just as much from stepping outside the confines of a traditional PhD, and for that advice, I am forever grateful. Keith, thank you for always supporting me as a researcher and for pushing me throughout my time in the CDT – whether this was through tackling my writing insecurities or for encouraging me to do so much more beyond this project. I’m not quite sure what you saw in me on that short trip to Oxford in 2015, but I am so glad I attended and, as they say, the rest is history. As supervisory duos go, I have been incredibly fortunate and I am incredibly indebted to you both.

To Al Pinkerton, Anna Jackman, Lizzie Coles-Kemp, Pete Adey and Rikke Bjerg Jensen, thank you for the support and guidance you have provided as advisors over the years - both in official and unofficial capacities. To Jen Turner, Kevin Grove and Kim Peters, thank you for the belief you showed in me back in Aberystwyth – I never thought I could tackle a Masters, let alone a PhD, so I know that this journey wouldn’t have started without the three of you.

I would like to acknowledge the financial support provided by EPSRC and Royal Holloway’s Centre for Doctoral Training (CDT) in Cyber Security, without which the countless research visits, conferences and incredible experiences over the years would not have happened. From presenting my research in Boston, New Orleans and Melbourne, to my many fieldwork visits to Estonia, this research simply would not have been possible without their support – nor would I have been fortunate enough to visit and experience parts of the world I had only dreamed of venturing to. To Claire Hudson, thank you for the many hours spent replying to emails, trawling through poorly referenced receipts and reimbursements, and for being the true hero of the CDT. To Jen Thornton, thank you for being the equivalent hero in the Geography department and for all the help and support you provided with various map and diagram designs over the years.

A significant period of this research took place in Tallinn, Estonia - a place that now holds a special place in my heart. After first visiting in 2015, I instantly fell in love with the country, its people and its culture. So often portrayed as cold and reserved, I’ve experienced nothing but warmth and generosity, and there are a number of people I would like to thank for making my time in Estonia so impactful and special. First, I would like to thank Robert Krimmer and everyone at Ragnar Nurkse (TTÜ) for the hospitality and kindness you showed during my time in Tallinn in 2018. To Robert in particular, I want to thank you for the mentorship, guidance, and indeed patience you showed towards my work, and for the opportunity to collaborate and step across into an entirely new discipline. Our work – and your perspective on the Data Embassy and Estonian e-governance - gave new impetus to my research and overall direction of my PhD, so danke. Thanks to Ott Vatter, for opening so many
doors (and for opening that first email) and for making my initial trip to Tallinn a reality. Thank you also to Laura Kask, without which large parts of this project would not have been possible. Your knowledge of the Data Embassy, international law, and good Tallinn eateries was an inspiration - as was our trip along the Great Ocean Road, after which you will remain a good friend for life. To Marianne, I am so thankful to have met you on that busy flight to Tallinn – you remained a constant throughout my time in Estonia, and will remain one of my closest friends. Thank you also to Agnė, Hanna, Kaire, Kadi-Ell, Kieren, Martin and many others for making my time in Tallinn so special. Finally, I would like to thank all of the participants who took part in this research – the majority of whom were based in Tallinn. Your time was invaluable and I thank every single one of you for your contribution to this work - aitäh.

I would also like to thank all of my incredible friends who have supported me over the years. To those in the CDT - Amit Deo, Amy Ertan, Angela Heeler, Georgia Crossland, Greg Fenn, Jodie Knapp, Laura Shipp, Liam Medley, Lydia Garms, Rob Markiewicz, Rory Hopcraft, Steve Hersee and Taryn Padmore - thank you for being the most incredible of colleagues, for the many pints and coffee breaks, and for pushing me towards the finish line. To Andreas Haggman, Ben Curtis and Pip Thornton, thank you for everything over the years – you have helped in more ways than you could imagine. To those in Royal Holloway’s geography department – Adam Badger, Alex Hardy, Ed Brookes, Elly Cotterill, Emily Hopkins, Hannah Dickinson, Helen Turner, Nicola Wendt and Nina Willment – thank you for being my academic confidants and supporting me from the start. To everyone I met through the many conferences, summer schools and events over the years – Alice Brown, Angharad Butler-Rees, Andrew Dwyer, Kate Miltner, Nat O’Grady, Niko Hatakka, Shyam Krishna, Tim Highfield and Tommo Sear – thanks for playing a huge part in this journey, I’m incredibly lucky to have met you all. To all of my close friends outside of academia, thank you for everything, and for often reminding me that there was a life outside of this PhD. Bean, Charly, Emily, Euan, Frances, Fred, Han, Harry, my two Jade’s, James, Jess, Laura, Niall, Robbie, Sammy, Shauna and Voycey – I love you all. Harry, Mitch, Sam and Twister, thanks for always being there and for entertaining my incessant chat. To Adam, Angus, Stroud, Loz and Sparky, thanks for getting me through lockdown.

Finally, I would like to say thank you to my family. Your unwavering love and support throughout my time at University has meant the world to me. To Mum, Dad and my sister Rachel, thank you for always being there and for looking after me during some of the toughest periods of this PhD journey. To Grandad, Laura, Jane and Bob, and Ian and Elizabeth, thank you for the continued love and support over the years. Ruby, thank you for always being there for me, for distracting me from PhD life, and for reminding me to be the best possible person I can be – I love you. Mum, Rachel, Ruby and Jack – thank you for proofreading this thesis. Any remaining errors are, of course, my own.

And finally, Mum, I wanted to dedicate these final words to you. Writing the final parts of this thesis during the pandemic was one of the hardest things I’ve had to do, but I will never forget the patience and selflessness you showed by providing a roof for me to live under, supporting me every single day (even when you didn’t feel yourself), and for putting up with my sh*t when I felt most up against it. Thank you.
This one is for Frances.
Figure 1.1 – The EBRC European Reliance Centre East, located in Betzdorf, Luxembourg
(source: www.datacenters-in-europe.com; copyright: EBRC – WIDE David Laurent)
Chapter 1 - Introduction

In 2018, the Estonian government announced that it had opened the world’s first Data Embassy in Luxembourg. Aimed at ensuring the ‘digital continuity’ of the Republic of Estonia, the Data Embassy will ‘backup’ critical components of the state (information systems, databases, registries) to the cloud, ensuring the state can continue to endure in the event of an emergency. Operated outside of its borders from a government-controlled data centre on the outskirts of the tiny Luxembourgian town of Betzdorf (see Fig. 1.1), the Data Embassy will have functions akin to those of a traditional embassy, guaranteeing similar diplomatic immunities to Estonian data and information systems held on its server racks.

In an age of increasing global insecurity - from climate change to geopolitical instability - evolving cyberattack sophistication and threats to critical national infrastructure and vital organs of the state are both genuine and effective. The *NotPetya* and *WannaCry* ransomware cyberattacks that targeted a global network of computers in 2017, proved devastating in scale and disruption; the former targeting power grids and critical national infrastructure in Ukraine (Greenberg, 2019), the latter disrupting the UK’s National Health Service, costing its government approximately £92m (Field, 2018).

Estonia, with its own visceral history of dealing with such threats, has cause for concern. In 2007, the country was victim to what is widely believed to be the first instance of a state-sponsored cyberattack (see, Ehala, 2009; Hansen and Nissenbaum, 2009; Kaiser, 2015). Over a number of weeks, vast swathes of the state’s infrastructure were targeted by a number of sustained distributed denial-of-service (DDoS) attacks1, leading to many government websites, banks and public services being driven offline. Fingers immediately pointed to Russia (though never officially attributed), following the breakdown of diplomatic relations between the two countries over the movement of a Soviet World War II memorial. Soon after, critical questions were also being levelled at the Estonian government. What would happen if government services and IT infrastructure suddenly became unavailable again – this time for even longer? What would happen if the nation’s digital archives and databases were to be corrupted, possibly held to ransom? Widely viewed as the “most advanced digital society in the world” (Hammersley, 2015), and highly dependent on its thriving digital ecosystem, the attack served as a potent wakeup call, stressing the importance of cyber defence in the twenty-first century.

---

1 A DDoS cyberattack is a “malicious attempt to disrupt normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic” (Cloudflare, 2019). Frequent targets are large organisations and businesses that are reliant on the availability of their services (e.g. financial services and e-commerce), and are now considered one of the most disruptive (and relatively cheap) tools in a cyber-attackers arsenal. The title of this thesis – *Distributed Denial-of-Government* – is a deliberate play on the notion of a DDoS attack, denoting the Data Embassy’s role in potentially limiting the threat of future DDoS attacks for the Estonian government. It can also refer to the role of a future distributed network of Estonian Data Embassies, as a form of deterrence against an attack (both cyber or physical) against the country. This will become more apparent as the design and function of the Data Embassy is explained in greater detail later in this thesis (see Chapter 4).
Today, tensions between Estonia and neighbouring Russia continue to play out on the ground. The regular build up and stationing of NATO troops in Estonia, alongside performative military exercises along its borders, continues to aggravate Putin’s Russia, whilst Russian military interventions throughout its ‘near abroad’ continue to put Estonia and the wider Baltic sea region on a heightened sense of alert. For a country that spent more than half of the twentieth century under occupation, the notion that ‘it might happen again’ still rings true for many Estonians. In many ways, the Data Embassy may not only serve as a necessity for any government in a digital age, but, for Estonia, as a vital deterrence against a potentially hostile and aggressive neighbour.

In this thesis I explore the geopolitical, diplomatic and legal implications of extraterritorial data storage, specifically, in the context of a state-level emergency or crisis. Taking the novel Estonian Data Embassy as the central focus and case study of this research, I critically examine how this potentially transformative e-government/national security innovation calls into question many long-held assumptions around conventional forms of geopolitics, diplomacy and international law. Drawing on nearly three years of ethnographic engagements with Estonian policymakers, cybersecurity professionals, academic experts and those working close to the Data Embassy project itself, I contextualise the initiative alongside Estonia’s own unsettled past and uncertain future, arguing that its emergence is intertwined in a much deeper state continuity project that is rooted in the ontological insecurities and collective memory of the state today.

Fundamentally, this is a thesis about the changing nature of statehood and diplomacy in a digital age. Through a critical examination of the Estonian Data Embassy and the environment it necessitates, it questions what the Data Embassy reveals (or, conversely, ‘masks’) about the everyday practice and performance of the state – from revelatory extraterritorial archival practices that predate the Data Embassy itself, to the ontological insecurities facing the state today that point to a deep-seated anxiety at its centre. It also considers what the Data Embassy’s emergence may mean for the future practice of diplomacy, critiquing whether new diplomatic relations will begin to form in and around the ‘digital embassy’ and the extraterritorial space of the data centre.

Providing one of the first in-depth, critical studies into the Data Embassy, this thesis draws together a number of emerging interdisciplinary debates from across areas of geopolitics, cybersecurity and diplomatic studies. Making a number of significant contributions to these areas, this research develops new insights

---

2 The term ‘near abroad’ is used to denote the fourteen former Soviet Republics (including Estonia) that are now independent but still remain within Russia’s supposed ‘sphere of influence’. Despite disputes over its genealogy, awkward translation and geographical extent, the term has been ever-present within Russian political discourse and continues to unsettle the former republics, as many of them believe they signify renewed attempts at expansion and/or unsettling ethnic Russians within their countries (see, Cameron and Orenstein, 2012; Toal, 2017).
into anticipatory logics of statehood in a digital age; state-level anxieties (and their distinct temporalities) and how other emotions/affects may be identified at a collective level in world politics; and the emergence of a novel form of digital diplomacy that is sited within the extraterritorial data centre, and how this may herald changes to outmoded international agreements such as the Vienna Convention. With the potential advent of more Data Embassies in the future, such debates will undoubtedly intensify and converge as other states (and non-state actors) are allured by the promise of extraterritorial data storage. As such, this thesis should be of interest to a wide-range of stakeholders, from scholars working on issues of statehood/political legitimacy and with interests in data extraterritoriality and diplomatic law, to policymakers working in areas of cyber resilience and national security, and IT professionals with interests in cloud computing and disaster recovery management.

In the remainder of this chapter, we take one step backwards into the past, and then forwards into the present, as we consider the Data Embassy and the different temporalities of Estonian continuity, before then going on to introduce the main themes, aims and research questions of this thesis.

1.1 Keeping the Republic alive: Estonian continuity past and present
On 17 June 1940, the Republic of Estonia was forcibly annexed and incorporated into the Soviet Union under the auspices of the Molotov-Ribbentrop Pact (1939). Alongside neighbouring Latvia and Lithuania, the annexation and unremitting occupation of all three Baltic states by foreign powers would last for 51 years - first, by the Soviet Union (1940-1941), then by Nazi Germany (1941-1944), and again by the Soviet Union (1944-1991) - until independence was restored in 1991.

In the year preceding the annexation (1939), following a period of military presence and ultimatums from the Soviet Union, the Estonian government was pressured into accepting and signing a treaty of mutual assistance. The treaty called for mutual cooperation and respect of one another’s sovereignty, but crucially led to the installation of a pro-Soviet ‘puppet’ government and allowed the Soviet Union to establish military and naval bases on Estonian territory (Taylor, 2018; Van Elsuwege, 2003).

This, as many scholars have since argued, constituted a violation of international law under the principle of *ex injuria jus non oritur jus* - meaning no legal benefit can be derived from an illegal act. Accordingly, the seizure and subsequent occupation of Estonia and all three Baltic states were judged to be illegal (Mälksoo, 2000; Van Elsuwege, 2003). As Peter Van Elsuwege explains, despite occupying the Baltic states, legally speaking, the Soviet Union had “no sovereign rights” over their territory, thus Estonia, Latvia and

---

3 Signed in Moscow on 23 August 1939, the Molotov-Ribbentrop Pact was effectively a non-aggression treaty between Nazi Germany and the Soviet Union. After the Nuremberg trials at the end of the Second World War, it was revealed that Germany and the Soviet Union had inserted a ‘secret protocol’ into the Pact that meant that Estonia (along with Latvia, Finland, East Poland – and later, Lithuania) had been divided into the Soviet’s ‘sphere of influence’ (Kasekamp, 2018: 113).

4 Pro-Soviet governments were also installed in Latvia and Lithuania following the signing of similar treaties on 5 October and 10 October 1939 respectively.
Lithuania “continued to exist as subjects of international law” (2003: 377-378). They were, in fact, *de jure* independent states under illegal occupation.

At the time, this was reflected across the international community as a growing number of states, whilst having no choice but to accept Soviet occupation of the Baltic states *de facto*, refused to do so *de jure*. This stemmed largely from the Wells Declaration, issued on 23 July 1940 by acting U.S. secretary of state Sumner Wells, that condemned the occupation and set U.S. policy of refusing to accept their newly installed pro-Soviet governments. Enacting the 1932 Stimson Doctrine of non-recognition of “any situation (including the establishment of a new State), treaty or other agreement procured by illegal means” (Turns, 2003: 107), the U.S.’ stance would remain a key, symbolic policy over the next 51 years of occupation, and would soon be joined by a number of key allies, including the UK and Canada.

The anomalous circumstances and legal ambiguity that characterised this period would also impact upon traditional diplomatic norms and procedures. No more so than the fact that many Baltic embassies and consular representations continued to function in some form between 1940 and 1991. Despite Soviet attempts to limit, close or incorporate many existing Baltic embassies and legations – as well as attempts at seizing archives and gold reserves, and ordering exiled diplomats to return ‘home’ (Taylor, 2018) – there were many in the Baltic diasporic community who were likely heartened by the non-recognition stance that the U.S. and other countries took on the Soviet occupation. This had two significant implications. First, as mentioned, that many Western governments would continue to recognise the independence and continuity of the Baltic states, whilst deeming the occupation as fundamentally illegitimate under international law. Second, it meant that Baltic embassies could remain “in situ” and retain certain diplomatic privileges (Taylor, 2018: 88), something that Estonians August Torma and Ernst Jaakson took significant advantage of.

Throughout this period, in London and New York respectively, Torma and Jaakson (see Fig. 1.2) continued to operate as diplomatic envoys from their respective embassies. In an effort to draw the world’s attention to the continued illegitimacy of the Soviet Union’s occupation of the Baltic states, both tirelessly pursued the case of Estonia’s legal existence and the restoration of sovereignty to the wider world, whilst often revered as ambassadors without a country (McHugh and Pacy, 2001; Radcliffe, 1988; Stewart, 1998).

---

5 As historian Neil Taylor points out, around fifty other countries would soon take the same line as the U.S. – some more publicly than others (2018: 81). The Swedish government, however, became one of the first governments to formally recognise the Soviet occupation of the Baltic states, and did not allow for any pre-war Baltic embassies to function in Stockholm (2018: 113). Taylor goes on to point out that the Wells Declaration is still commemorated in the Baltics and their Washington embassies today, “such is the effect that it had and maintained.” (2018: 82)
In Tina Tamman’s biographical account of his life – *The Last Ambassador* (2011) – August Torma is seen as the “embodiment” of a free Estonia, playing both a major role in Estonia’s initial “birth pangs” after declaring independence in 1918 following the collapse of the Russian Empire, but also in keeping the doctrine of legal continuity alive after Soviet occupation in 1940. Having just lost his government – and resisting orders by the new pro-Soviet ‘puppet’ government to return to Tallinn – Torma had no direct role, official contact nor directive from his homeland (Tamman, 2011: 102). In London, his position was no clearer as the British Foreign Office initially ceased to recognise the Estonian embassy and downgraded Torma’s status to that of “a person who enjoyed individual diplomatic privileges but was not recognised as a diplomatic representative of a foreign country” (Made, 2008: 137). As Tamman writes, Torma would have cut a forlorn figure during this period, yet remained resolute in exerting his (weakened) diplomatic agency and pressured the British government to not recognise the “forcible usurpation” of his homeland (2011: 103). In a plea to the British Foreign Secretary Lord Halifax, Torma went on to write:

“I venture to express the hope that HM Government, in conformity with their frequently reiterated determination not to approve of situations engendered by

---

6 This reflects the somewhat cautious and ambiguous approach by the UK to the Soviet occupation during this period. There was an initial reluctance from the British government to come out in defence of the Baltic states during the inter-war period, as Churchill almost conceded Soviet claims to *de jure* status. The UK’s stance towards the Soviet Union (and, indeed, Joseph Stalin) would ebb and flow, namely for geostrategic reasons, but were soon persuaded by the U.S. to think otherwise and come out in support of the Baltic states’ plight (Kirkby, 1996: 81).

7 Neil Taylor notes how Torma was still able to fly the Estonian flag outside his office, “which was a source of considerable comfort to the exile community and to the few Estonians allowed to travel in Soviet times who happened to see it” (2018: 88).
force as against law, will refuse to recognise the incorporation of Estonia into the Soviet Union, since it is only too apparent that this situation has been brought about under duress.”

(Tamman, 2011: 106)

Meanwhile, in New York, Ernst Jaakson served as Consul General of Estonia from 1965 – after the death of his predecessor Johannes Kaiv – until the regaining of independence in 1991. Working from the 14th floor of the Rockefeller Center, Jaakson would boldly defend and promote the interests of the Estonian people, often airing messages of hope and solidarity via the Voice of America broadcasting service (Stewart, 1998). Jaakson was ideally located in close proximity to the United Nations Headquarters, the principle organs of international diplomacy and law, whilst also serving as the “unofficial” Dean of the Diplomatic Corps during the Cold War (Kuus, 1998). It is well documented that he continued to issue Estonian passports – or Jaakson passports – during this period (Kempster, 1988). Still honoured by many Western governments (in line with the U.S.’ Stimson Doctrine), the passports were more than simply symbolic gestures to a displaced Estonian diaspora: their political agency would continue to defy the Soviet Union’s enduring illegal occupation during this period. As another act of resistance, in 1969, Jaakson (on behalf of the Estonian nation) joined 72 other leaders and dignitaries from around the globe in signing the Apollo 11 Goodwill Messages – short statements left on a small silicon disc and placed in the Sea of Tranquillity on the moon by astronauts Neil Armstrong and Buzz Aldrin (Liu, 2019). His message to the world was short and poignant:

"The people of Estonia join those who hope and work for freedom and a better world."

(NASA, 1969)

Only Jaakson would live to see a free and independent Estonia (with Torma passing away in 1971)⁸, but the indefatigable and selfless work of both would serve as a powerful and symbolic testament to Estonia’s continuity (both legally and figuratively) between 1940 and 1991 (Mälksoo, 2000; Tamman, 2011). Such practice and performance of what McConnell et al. (2012) term “unofficial” forms of diplomacy and statecraft has remained relatively understated until now, but their struggle and diplomatic service throughout the Cold War arguably played a crucial role in keeping Estonia’s cause for independence, legitimacy and sovereignty alive. They were, as McHugh and Pacy acknowledge, a “small and largely

---

symbolic part of a larger process, but (in terms of foreign support for that process) a catalyst for it, nonetheless” (2001: 159).

Alongside these symbolic forms of political rebellion, however, the doctrine of legal continuity would prove more pertinent and powerful, not only serving to undermine the legality and legitimacy of Soviet rule throughout this period, but also posturing as a ‘political fighting program’ throughout the Cold War and into the early years of re-independence (Aalto, 2000; Mäkssoo, 2000). For Van Elsuwege, the principle of legal or state continuity not only denounced the forcible annexation of the Baltic states, but also held a vital “symbolic” and “moral” dimension that would later prove crucial in driving forward accession into both NATO and the EU (2003: 388). Also central to this Baltic thesis, as Lauri Mäkssoo (2000) has explored, was that after decades of non-recognition from much of the Western world, the Baltic states must not be characterised as ‘successor states’ of the Soviet Union, but identical as their independent statehood in the interwar period of 1918-1940 (see also, Aalto, 2000; Berg and Oras, 2000). This would then be key to Estonia’s “restoration doctrine” that later characterised its domestic and foreign policies throughout the 1990s (Aalto, 2000; Kaljund, 2018).

Mäkssoo’s (2000) significant legal analysis on this topic also brings into focus the role of the Estonian Government-in-Exile during this period, assessing its contribution towards the preservation of Estonia’s continuity. Following Nazi Germany occupation, and before the country was occupied for a second time by the Soviet Union in 1944, acting Prime Minister Otto Tief attempted (and failed) to restore the legitimate independence of Estonia and de facto control of its territory9. With Soviet forces advancing on the capital once again, Tief and his government were forced to flee to Western Estonia in an attempt to escape to Sweden, before many officials (including Tief) were captured and either executed or deported to Siberia. Of the four ministers who were able to escape to Stockholm, it fell to the most senior surviving member, Minister of Foreign Affairs August Rei, to assume the role as acting head of state. It would not be until 12 January 1953, however, that Rei would officially declare the Estonian Government-in-Exile – one that would last until after Estonia restored its independence in 199110.

Mäkssoo concludes that the Estonian Government-in-Exile, with its activities and influence severely limited (as they were for Torma and Jaakson), may have served a largely “passive” and “symbolic” role (2000: 299). But, as McConnell et al. argue, turning to the costly and time-consuming diplomatic practice of an exiled government (similarly, serving as a diplomat ‘without a country’) tries, if nothing else, to constitute a “form of recognition” (2012: 808). During a historic ceremony at Kadriorg Palace in Tallinn on 8 October 1992,

---

9 Mäkssoo writes emotively of this period, describing the events in Tallinn whereby the Nazi German flag was finally symbolically replaced by the Estonian tricolour on top of the Pikk Hermann flag tower – only, days later, for the Soviet forces to take it back down once again (2000: 295-296).

10 According to Mäkssoo, despite all members of the government living in Stockholm, the proclamation actually had to be made in Oslo, Norway, due to Swedish restrictions on the “political activities of refugees” (2000: 298). There were five governments-in-exile formed during this period (1953-1992).
newly elected Estonian President Lennart Meri expressed “deep gratitude” to departing president-in-exile, Heinrich Mark, and all other members of the government-in-exile “for preserving the continuity of the Republic of Estonia” during 51 years of occupation (Meri, quoted in Mälksoo, 2000: 300).

As this section has shown, and serving as a central theme in the remainder of this thesis, notions of ‘recognition’, ‘legitimacy’ and ‘continuity’ appear rooted into Estonia’s complex political history and collective memory. Keeping the Republic alive was as much political as it was legal, but has come to represent and embody something much deeper in the spirit of the Estonian nation – and, as this thesis aims to show, this is still very much something that exudes affective power in a free and self-determining Estonia today.

1.2 Back to the future? Russia, Putin and the spectral geographies/geopolitics of the Near Abroad

Over twenty-five years later, and with Estonia’s independence fully restored and a greater degree of prosperity found within the European Union (EU) and North Atlantic Treaty Organisation (NATO) alliances, it is not unreasonable to deduce that the issue of continuity should be consigned to the history books. Yet, amidst the backdrop of increasing geopolitical and security tensions, both globally and across the Baltics, the spectre of territorial uncertainty and political independence has reared its head once again.

This was illustrated no more strikingly than in February and March of 2014, as Russia unlawfully annexed the Crimean Peninsula, leading to further military intervention, instability and conflict in the Donbass region of Ukraine later that year. Capitalising on the Ukrainian political crisis at the time, Russia and Vladimir Putin’s purported expansionist agenda across its ‘near abroad’ (Toal, 2017) - in the face of NATO and EU ‘enlargement’ from the West - has led some commentators to speculate over Russia and Putin’s next move (Carpenter, 2014; Friedman, 2016; Lucas, 2015; Naylor, 2020; Rubin, 2019; Wood, 2016).

Such events should not be taken in isolation however. The Kremlin, particularly under Putin’s autocratic leadership, has not defected too far from a common long-term strategy and goal of unsettling its so-called ‘near abroad’. The events in Ukraine also mirror those of 2008, when Russia invaded the South Ossetia and Abkhazia regions of Georgia under similar pretences. Putin has remained indifferent to those in the West who are critical of his actions, vehemently defending the conduct (and sometimes even the existence) of Russian forces in both regions. Instead, Putin has asseverated the self-determination of Georgia and Ukraine’s large Russian-speaking populations, and pledged to “protect” the rights of other Russians living abroad (The Washington Post, 2014). With comparably large and geographically concentrated
Russian-speaking populations of their own\textsuperscript{11}, it is of no surprise that some commentators have postulated on the future of the Baltics and where Putin may “try his luck” next (Stuttaford, 2015).

\textbf{[IMAGE REMOVED DUE TO COPYRIGHT]}

Figure 1.3 – Unmarked counterinsurgency fighters that arrived in Crimea shortly after the 2014 annexation – Russian military or (as Putin described) local ‘self-defence groups’? (source: www.bbc.co.uk)

The destabilisation of eastern Ukraine and self-determination rhetoric has unquestionably put Estonia and the Baltic states on a higher state of alert. Talk of ‘Little Green Men’ (like the unmarked counterinsurgency fighters observed across eastern Ukraine in 2014 – see Fig. 1.3) and tanks rolling across the Estonian eastern border may simply serve as hearsay, but this hasn’t stopped those in prominent positions from postulating on future doomsday scenarios. Former NATO secretary-general Anders Fogh Rasmussen has stated that Putin may wish to intervene in the Baltics (Evans-Pritchard, 2015), whilst a recent RAND study wargamed Baltic defence and concluded that a Russian invasion of both Estonia and Latvia would take as little as 36 hours and required an urgent collective response (Shlapak and Johnson, 2016). As Chapter 3 of this thesis explores in more detail, this has been compounded by a raft of hyperbolic international news coverage:

\textbf{“‘They Will Die in Tallinn’: Estonia Girds for War With Russia”}

(McKew, 2018)

But to what extent are such eventualities exaggerated? Former Estonian President Toomas Hendrik Ilves (2006-2016), who has been more outspoken than most on Russia, has been resentful of the largely hysterical “journalistic trope” that Narva – Estonia’s third largest city along its Eastern border, with a sizable Russian population – would be next in Putin’s sights (Servettaz, 2014). Ilves expressed his frustration on this topic during his final Victory Day speech as president in June 2016, stating: “For two years we have read hundreds of naïve articles about possible "little green men" in Estonia and Latvia, and the ill-informed questions of armchair analysts: ‘Is Narva next?’ – ‘Kas Narva on järgmine?’” (President.ee, 2016). Indeed, Estonia-Russia relations may have ‘waxed and waned’ over the years (Trimbach and O’Lear, 2015), but the immediacy or likelihood of any kind of threat to Estonia may be overstated given, amongst other factors, Estonia’s strong position within NATO and the treaty obligation of Article 5 (Coffey, 2015; Kasekamp, 2019).

\textsuperscript{11} Ethnic Russians make up approximately 25% of the populations of Estonia and Latvia, and 5% of Lithuania’s. The number of Russian-speakers across the Baltic states is much higher. Discussed further in Chapter 5, the number of those obtaining citizenship within their respective countries is much lower, however, which has many socio-political implications.
Nevertheless, throughout the development of this thesis, the world and Estonian politics have seldom stood still. The election of Donald Trump as U.S. president and Brexit have shaken the Western political consensus to their foundations (both, interestingly, also tainted by claims of Russian interference)\(^{12}\). Meanwhile, there have been two national Estonian elections - the most recent of which in March 2019 was dominated by a populist revolt and lurch to the far-right as the populist Conservative People’s Party of Estonia (EKRE) gained 17.8% of the vote and forced their way into coalition with Jüri Ratas’ Centre Party (Eesti Keskerakond) and Pro Patria (Isamaa). Furthermore, the ongoing Ukrainian crisis has also spilled into the Baltic Sea region with both Russia and NATO deploying troops and running exercises close to the Estonia-Russia border (Kasekamp, 2019).

Estonia, often patronisingly referred to as the “tiny” Russian neighbour (Miller, 2018), and in need of constant reassurance and protection, seems tainted by paradoxical circumstances. On the one hand, key public figures and politicians are keen to profess that there is no physical threat to Estonia’s territorial borders and its people. Yet, on the other, determent by way of military exercises, a new 110km border fence along its eastern border (Whyte, 2018) and a diplomatic doggedness, appear the most preferential strategy for both Estonia and wider NATO alliance\(^{13}\). The legitimate anxieties and concerns that do exist, therefore, appear grounded in a collective memory politics (Tamm, 2013) and everyday affective geopolitics (Toal, 2017) that this thesis contends shape elements of Estonian policymaking and (inter)national discourse. Nevertheless, as former President Ilves recently ruminated:

“One term I didn’t like is ‘reassurance’. We’re not patients on a psychologist’s couch…We’re not worried. What we need to work on is deterrence.”

(Kim, 2015)

1.3 Backing up the state: thesis outline and early provocations

“Before Crimea, nobody saw a need.”

(Taavi Kotka interview 15/07/19)

\(^{12}\) The rhetoric of Donald Trump in particular has had numerous implications for the security of the Baltic states. In January 2017, Trump described NATO as ‘obsolete’ in comments to two major European news publications, The Times and Bild. Trump had made similar comments during his election campaign in 2016 – a reaction to what he felt was unfair contributions by other alliance members’ defence spending budgets - but the timing of such criticism just days before assuming presidency alarmed a number of diplomats across the alliance (Gordon and Chokshi, 2017). Trump’s comments and inherent scepticism towards NATO was felt no more so than in the Baltics, and Estonia in particular, where uncertainty over alliance members’ commitment to collective defence is a continuous source of anxiety for those most exposed along NATO’s eastern frontier (ironically, Estonia meets its fair share of NATO defence spending, contributing 2.1% of its GDP compared to major allies such as Germany and France). Trump has since reaffirmed U.S. support and his personal commitment to NATO, but as former Estonian ambassador to the U.S., Kalev Stoicescu, recently suggested, Trump still “worries everyone” in Estonia (Rubin, 2019).

\(^{13}\) Many commentators have argued this strategy appears increasingly necessary as Russia continues to disrupt through novel forms of hybrid warfare and “reflexive control” (Giles et al., 2018) that seem to be “sowing seeds of discontent in Eastern Europe” (Marten, 2017) (see Chapter 5).
When he announced, in 2013, that the Estonian government was going to build a Data Embassy outside of the country’s borders, Taavi Kotka knew he faced an uphill battle. Ministers were rightly sceptical (maybe some a little confused) and not immediately sold on this ‘moonshot’ proposal. Where was the value for the country and its citizens? Was this – both domestically and internationally – even legal? Heeding to the advice of its current president (see above), perhaps the Data Embassy could serve as a vital deterrence against an increasingly antagonistic Russia. Yet, how would this be perceived by the media (or even Estonia’s closest allies), if it were believed that the government was seemingly “prepping” (Garrett, 2020) for a future geopolitical catastrophe?

Then Crimea happened. According to Kotka, the events that unfolded over the course of 2014 were the catalyst for those in government who were perhaps yet to see the significance of storing Estonia’s critical databases and information systems outside of its territory:

“The Crimea thing was the warning bell, because then the fact that the Russians can do something outrageous, conquer land and the world says we’re okay with that.

That rang a bell. So, yes, we are part of NATO. But, come on, nobody starts World War III because of 1.3m people.”

(Taavi Kotka interview 15/07/19)

As this chapter has so far outlined, Estonia is no stranger to threats to its ontological security. From the initial ‘birth pangs’ of the Estonian state in 1918, to an occupation that lasted fifty-one years, it is not surprising that notions of sovereignty and independence are still important questions within Estonian security discourse today. Such existential logics – and a belief, regarding occupation, that ‘it might happen again’ (see Chapter 5) – are not only embedded within a troubled collective memory but are somewhat intensified by the contemporary geopolitical insecurities Estonia faces today. As Riina Kaljurand, a researcher at an Estonian-based security think-tank (ICDS), recently commented:

14 In 2013, Taavi Kotka was the Estonian government’s Chief Information Officer, tasked with overseeing Estonia’s ICT infrastructure and the implementation of its digital strategy. Kotka can be seen as the driving figure behind the Data Embassy concept, and thus plays a central role in this research (please see Appendix A for more information on Kotka, his role, and other key protagonists mentioned throughout this thesis). As I discuss in Chapter 3, Kotka insisted he was attributed in this thesis, whereas (for consistency and anonymity purposes) I have anonymised all other quotes throughout.

15 A ‘moonshot’ is technology-speak for an ambitious or exploratory project that is undertaken without the expectation of success/profit – and perhaps sometimes without an overview of the potential risks and benefits (Rouse, 2014). The term holds some relevance in an Estonian context with many people that I spoke to often using the term (perhaps sometimes flippantly) to refer to many of Estonia’s recent technological innovations – one of them being the Data Embassy.
“For us this is existential. Either you have Estonia on the map or you do not. It’s in our psyche. You cannot get it away. You can laugh about it, but this is the way it is with Russia.”

(O’Leary, 2017)

Kotka, writing for the government the year following his announcement, explicated how “geopolitical events in 2014” had brought the “question of continuity” to the forefront of Estonia’s national conversation (MoEAC, 2015: 1). In an early research paper on the subject, he and academic researcher Innar Liiv went on to highlight some of the idiosyncrasies facing a modern-day digital Estonia, and how the country’s biggest challenge was to “develop a solution whereby the Estonian state would endure despite an occupation of its territory” (Kotka and Liiv, 2015: 152). Similar to discourse explicated during Soviet occupation (see Section 1.1), it is clear that a discourse of continuity was once again being driven from within, with the Data Embassy being presented as a novel solution to such existential logics in order to avoid such a catastrophe ever happening again.

Since the birth of the modern state in a Westphalian system, states have often had to face up to legitimate (as well as imagined) threats to their existence. During the Cold War, this was manifest in the proliferation of nuclear weapons, specifically the atomic bomb and the threat of all-out nuclear war. For the United States and the Soviet Union, a doctrine of mutually assured destruction (MAD) meant that the threat of nuclear annihilation was largely curtailed; but a subsequent fallout of this was a proxy nuclear arms race that was psychologically played out by other states across the world. During apartheid in the 1960s, facing what it perceived as encirclement and potential onslaught from so-called Frontline States (FLS), South Africa developed its own secret nuclear weapons programme. Similarly, the Israeli government and its first Prime Minister David Ben-Gurion, “haunted” by the Holocaust and subject to incessant hostility from its larger Arab neighbours, believed nuclear weapons were a “last resort” in ensuring the survivability of the Jewish state (Keck, 2019).

States have also faced up to deep anxieties from within. In The Encrypted State (2019), David Nugent illustrates the paranoia and consternation that gradually overcame the Peruvian government during the 1930s in the face of (what it believed to be) an insurgent and subversive political party (APRA) in the northern Chachapoyas region of the country. What followed was an almost self-destruction of the state from within, with delusional practices and a deep-seated collective anxiety at the heart of the state’s
apparatus\textsuperscript{16}. In this thesis, and under a slightly different context, I argue that a collective anxiety may be present at the heart of the Estonian state, as it contends with its own existential concerns over territory and sovereignty. As I go on to explore, this not only stems from fears over Estonia’s territorial integrity and political independence, but equally around the preservation of the state’s digital ecosystem and its archives (see Chapters 5 and 6). Now highly dependent on the state’s information systems as part of a wider ‘e-state’\textsuperscript{17}, there are many in Estonia who fear an eventuality whereby the state is somehow incapacitated or critical components/data are ‘lost’ – with some civil servants ruing the prospect of having to ‘return to paper’ in the event of a crisis. Such beliefs are exacerbated by Estonia’s own recent history, where 2007’s targeted cyberattack against the state’s critical infrastructure still rings true for many Estonians today\textsuperscript{18}.

It would be remiss, therefore, to think of the Data Embassy simply in terms of the state’s physical, ontological security, nor simply as a knee-jerk reaction to Crimea and the proximate unease felt close to its eastern border. As stipulated by Kotka and the Estonian government, the Data Embassy’s main aim is to ensure the digital continuity of the state (MoEAC, 2015; 2016). A term that has existed in the parlance of archivists and the security architects of large organisations since the late 1990s to tackle emerging concerns over the preservation and legacy of digital information (MacLean and Davis, 1999), the Estonian government has since appropriated the term to specify its goal of preserving the most critical functions of the state:

“Digital continuity means the capacity of a state to maintain its services and digital data relevant for the functioning of the state, regardless of any adverse changes or interruptions”

(MoEAC, 2016: 7)

The logic dictates that, given Estonia’s dependency on its information systems and services, preserving the core functions of its digital society would ensure that the state could endure and continue to function in the event of a crisis or contemporary emergency. For anthropological scholar Lorraine Kaljund, whether it is ensuring the availability of government services or the preservation of state data, digital continuity “involves laying the technological groundwork necessary to ensure that, if need be, state infrastructure—

\textsuperscript{16} Nugent writes of how key government officials of that period felt incredibly threatened by APRA and that the ‘Aprista movement’ “appeared to be everywhere” and “closing in around them” (2019: 4). To assuage these inherent anxieties, a select group of high-ranking government officials took the unprecedented step of ‘encrypting the state’, and began communicating with one another in coded messages, attempting to create a “new inner frontier between state and subversive” (2019: 5). Despite these efforts, this boundary would soon dissolve as officials even began to distrust one another – including their own police force and other forms of authority – with the state seemingly descending into a state of disorder and delusion.

\textsuperscript{17} Highlighted at the beginning of this chapter, Estonia is today widely considered a “digital power” (Areng, 2014) and innovative leader in e-government solutions and its approach to cybersecurity. This is unpacked further in Chapter 4, with the myriad of technological innovations (such as eID, i-voting and e-Residency) discussed, as well as the state’s growing dependency on its digital infrastructure, the implications of which are scrutinised further in Chapters 5, 6 and 7.

\textsuperscript{18} A recent survey conducted in 2017 suggests that 67\% of Estonians believe that a targeted cyberattack is the most likely threat facing the country today (MoEAC, 2018).
the access to and control of which is often a key component in the enactment of de facto sovereignty — can be easily delaminated from the historical territory of the nation-state.” (2018: 9). Drawing parallels to the efforts made to keep the Estonian state alive throughout the twentieth century, might the Data Embassy be seen as its twenty-first century digital equivalent?

In many ways, the advent of the world’s first Data Embassy in Luxembourg may represent a radical shift in our thinking with regards to how the state can endure in testing or unusual circumstances. Faced with the hypothetical scenario whereby a state’s territorial control is somehow inhibited or lost, could the state still effectively function from the cloud or even exist entirely virtually? In reality, such a scenario would appear unlikely under the Montevideo Convention’s (1933) criterion for statehood19, yet the Data Embassy may still recalibrate many of our long-held assumptions over statehood and the function of a state in the twenty-first century (see Chapter 7). In 2015, WIRED journalist and futurist Ben Hammersley (2015) pondered over what this could mean in the future, suggesting that the state could go into “hibernation”:

“It could be backed up and turned off, reduced to a suitcase full of hard drives, only to boot back up again when the time is right.”

(Hammersley, 2015)

The practice of ‘hibernating’ the state is somewhat radical and profound. Serving as a disaster recovery mechanism for states threatened by devastating earthquakes, or as a deterrence against threatening state or non-state actors, the ability to ‘backup’ critical components of the state (e.g. population/land registers or vital information systems) and to ‘restore’ them once the dust has settled, may prove an attractive proposition for those smaller states facing existential concerns of their own. It may, as shown in Estonia, also form part of a state’s wider national security strategy.

With new debates beginning to open up with regards to the agency and survivability of the state, the Data Embassy may also recalibrate many traditions and norms found at the intersection of diplomacy and international law. Located in a government-operated data centre in Luxembourg, the Data Embassy is not an embassy per se, yet (through a bilateral agreement) the Estonian government hopes this novel, exceptional space will function like one (see Chapter 4). The true ramifications of this are yet to be fully realised, but it is not unreasonable to suggest that conventional understandings of diplomacy may be under increasing tension. Can diplomatic immunity be applied to information systems and data residing outside of a traditional embassy? How should states respect the integrity and sovereignty of other states’ data in the

---

19 Signed in the Uruguayan capital, Montevideo, on 26 December 1933, the Montevideo Convention on the Rights and Duties of States effectively established the standard definition of statehood under international law. Under the convention, it stipulates that a state, recognised as a person of international law, should possess the following criteria: i) a defined territory; ii) a permanent population; iii) a government; and iv) a capacity to enter into relations with other states.
cloud? Can the notion of an embassy be extended to that of a space outside of the traditional confines of a diplomatic mission? If we begin to see more states following Estonia’s lead, then the advent of more Data Embassies may lead to radical changes in diplomatic protocol and laws, with pressure being applied to somewhat outdated conventions (such as the Vienna Convention on Diplomatic Relations\(^\text{20}\)) which are arguably increasingly not fit for purpose within a digital age.

It is important to reiterate that, at the time of writing this thesis, the Data Embassy is still within its formative, ‘beta phase’. In truth, it may be decades until we begin to see the full impact of a growing network of Data Embassies around the world, and what this may mean for future statecraft, diplomacy and international legal norms. However, the number of pertinent themes outlined in this introduction point to the transformative potential of the Data Embassy — but also what such developments may mean for our understanding of geopolitics, diplomacy and cybersecurity in the future. My aim in this thesis is to contribute to these contemporary debates, whilst also setting the foundations from which this novel (and indeed exceptional) concept can be studied through more of an interdisciplinary lens.

In order to address the conceptual phenomena that surround the Data Embassy, and in an effort to consolidate some of the wider themes and provocations highlighted so far, this thesis tackles three core research questions:

1) **What motivations are behind the Estonian government’s decision to start ‘backing up the state’ outside of its own borders?**

2) **Is Estonia experiencing a collective, state-level anxiety?**

3) **To what extent will the Data Embassy reconfigure our traditional conceptualisations of geopolitics and diplomacy in the future?**

The first research question aims to uncover what motivations are behind the establishment of the world’s first Data Embassy. Put simply, under what circumstances (or indeed pressures) do the Estonian government believe that ‘backing up’ vast quantities of the state’s critical data is necessitated? Is it simply, as the Estonian government stipulates, to ensure the digital continuity of Estonia? Or does the role of Russia and its actions in its ‘near abroad’ play a significant part in Estonia’s everyday security discourse and thus the establishment of the Data Embassy? Here, I draw empirically on nearly three years’ worth of ethnographic encounters with Estonian policymakers, academics and cybersecurity experts in order to build a more complete picture of the Data Embassy, its key motivators and, in doing so, informing what the

---

\(^{20}\) Signed on 18 April 1961, the Vienna Convention on Diplomatic Relations (VCDR) established a crucial framework through which states were able to establish and maintain diplomatic relations with one another. Coupled with the Vienna Convention on Consular Relations (1963), both are often thought of as cornerstones of modern diplomacy (see Chapters 2, 4 and 7 for more on the VCDR and its relationship to the Data Embassy).
Estonian Data Embassy project may reveal about the everyday practice and performance of the state (Mountz, 2007).

The second research question builds on the first and tackles an early hypothesis regarding the Data Embassy, and whether its establishment points to a deep-seated collective anxiety at the heart of the Estonian state. From everyday concerns over the fragility of its digital ecosystem and the preservation of critical databases and archives, to more existential concerns over territorial integrity and political independence, I claim that such an anxiety is not just present in the psyche of many Estonians, but also the apparatus of the state as a discourse of continuity is framed through both a historical and contemporary lens. Recognising the challenge of researching and identifying where this anxiety is located, I build on a growing body of research that attends to emotion and affect at a state-level in world politics (Billé, 2014; Hutchinson and Bleiker, 2014; Mercer, 2014; Toal, 2017). My aim is to: i) identify Estonia’s anxiety and to differentiate it from an everyday geopolitical ‘fear’ (Pain and Smith, 2008); ii) analyse its affective implications and how it manifests itself (e.g. through collective memory, public discourse, social and political practices, law, diplomacy); iii) examine how such an anxiety is administered by the state in order to manage many of its everyday insecurities.

Building on some of the provocations outlined during this introductory chapter, the final research question will broadly consider how the Data Embassy reconfigures our senses of geography and politics. Situating the Data Embassy within broader debates around state improvisation, political legitimacy and new forms of diplomatic practice (Jeffrey, 2013; McConnell, 2016), I examine to what extent our traditional understandings of the state and diplomacy are under increasing tension due to the emergence of the Data Embassy. In particular, I explore the potential impact and efficacy of a ‘virtual state’ that can operate from the cloud, whilst also drawing upon how the Data Embassy is already being reimagined and repurposed in an array of different contexts. I also examine what impact the Data Embassy may have on the practice of diplomacy – first, through its potential to forge new diplomatic relations and norms between states, and second, questioning whether the embassy and the Vienna Convention may be outdated in a digital age. Whilst it may be a little too soon to gauge the full impact and transformative effects of the Data Embassy, my aim is to situate the initiative within wider debates within geopolitics, diplomacy, cybersecurity and international law.

The remainder of this thesis is divided into seven main chapters.
that necessitates its arrival, and consider possible shifts in statecraft and diplomacy in the future, I suggest that the Data Embassy can be better understood as a form of geopolitical assemblage. Unpacking this assemblage further, I reflect upon how the Data Embassy touches upon and draws together a number of interdisciplinary debates from across the fields of political geography, cybersecurity and diplomatic studies, and point to where such debates inform key arguments made throughout this thesis.

In Chapter 3 – *Researching the Data Embassy* – I outline the design and methodological approach adopted for this research. Attending to one of the central research questions in this thesis, I begin by exploring how I intend to identify and theorise a collective entity, such as the state, as being anxious. I then go on to reflect on the embodied encounters and various political discourses experienced whilst researching the Data Embassy, unpacking what these reveal (or ‘mask’) about the everyday practice and performance of the Estonian state. The chapter concludes with some thoughts on the precarity of research, as I engage with the prospect of the Data Embassy ‘failing’ and what other roadblocks and uncertainties a researcher can face during the process of completing doctoral research.

In Chapter 4 – *A catalyst for the cloud* – I contextualise the Data Embassy as part of Estonia’s much broader geopolitical culture, and how the country sees and positions itself in the world today. Detailing Estonia’s journey (and relative success) since regaining independence – often framed through a lens of *restoration* and *transformation* – I examine the country’s rise to becoming today’s digital powerhouse, and what this story can tell us about the emergence of the Data Embassy from 2013 onwards. In the second half of the chapter, I unpack the Data Embassy itself in more detail, sketching out its key features and functions, and the initiative’s journey from mere conceptual blueprint to a fully operational project in Luxembourg. In doing so, I also uncover what the Data Embassy is not, providing conceptual clarity around the scope and aim of the initiative which help to clarify key arguments made throughout the remainder of the thesis.

In Chapter 5 – *Cloudy Geopolitics* – I explore the somewhat clouded message surrounding the Estonian government’s decision to begin extraterritorially storing its information systems and data outside of its own borders. Is the Data Embassy, as many in the media jumped to conclude, simply a mechanism to deter Russian aggression both on the ground and in cyberspace? Or can it be considered the next vital cog in Estonia’s powerful nation branding strategy and role as digital pioneer? Drawing on key ethnographic encounters in the field and analysis of government discourse since the Data Embassy was first announced, this empirical chapter paints a more complex picture in which a pragmatic, logical business case has since been projected by the state and its elite, contrasting to its own previous rhetoric and political realities regarding the Russian threat. In unpacking the Estonian government’s inconsistent motivations, I conclude that the Data Embassy is, in fact, intertwined as part of Estonia’s overarching continuity efforts that are rooted in the collective memory and wider practice and performance of the state.
Building on this analysis, Chapter 6 – *Estonia’s Anxiety* – addresses my second research question and examines whether Estonia is experiencing a collective, state-level anxiety. From everyday concerns over the fragility of its digital ecosystem and preservation of critical databases and archives, to more existential concerns over territorial integrity and political independence, I argue that the decision to establish a Data Embassy is rooted in an anxiety that is pervasive, undulatory and paradoxical for the Estonian state. Drawing on a growing body of work that considers different emotions/affects at a state level in world politics, this chapter aims to identify Estonia’s anxiety and how it manifests through the archive and an everyday affective geopolitics. Pointing to its distinct temporalities, I explore how such an anxiety congregates and sticks to particular political moments and histories – e.g. periods of occupation, regaining independence, 2007’s cyberattacks and the annexation of Crimea in 2014 – and uncertainties over the state’s ‘unknowable’ future, and how this anxiety is felt and experienced through expressions of Estonia’s collective memory, wider public discourse, various social and political practices, diplomacy and infrastructures. By way of concluding, I consider how this anxiety may also serve a productive function, allowing the state to manage many of the ontological insecurities it faces today.

In Chapter 7 - *The Data Embassy and Geopolitics in a Digital Era* – I examine what role the Data Embassy plays in reconfiguring traditional conceptualisations of geopolitics, diplomacy and international law. Drawing together some of the key themes touched upon throughout the thesis – from notions of state hibernation and anticipatory exile, to novel forms of diplomacy conducted through the extraterritorial data centre – this chapter considers the ways in which the Data Embassy will challenge and potentially alter conventional forms of statehood and diplomacy in the future. First, I explore the utility and function of the Data Embassy in the event of an emergency, before highlighting how the concept has been reimagined in a number of different contexts and futures. Second, I point to the ways in which the Data Embassy may alter diplomatic relations between states and whether, with the potential advent of more Data Embassies in the future, international agreements such as the Vienna Convention are fit for purpose in a digital age. As well as sketching out new directions of research in this area, I also outline a policy recommendation for the international community as the Data Embassy will continue to elicit interest from other state (and non-state) actors in the future.

To conclude, Chapter 8 brings together the key themes and findings from this research project, highlighting the interdisciplinary appeal of the Data Embassy and why it should form a crucial site of inquiry for scholars, practitioners and policymakers moving forward. In doing so, this chapter highlights the key contributions and limitations of this study, whilst reflecting on possible future avenues of research and practice in relation to the Data Embassy.
“The participant chuckled and told me there was absolutely no way I would be able to access the area within the data centre – ‘I’m not even sure I will be allowed access’. Access, they told me, will only be granted to Estonian nationals – and even then, only to key diplomatic staff and technical personnel.

This didn’t surprise me. Earlier attempts at visiting UK-based data centre hadn’t proved fruitful. In many ways, the data centre remains this mysterious, elusive infrastructure – often out of sight, out of mind.”

(September 2017)

Figure 2.1 – A typical media depiction of a data centre, often used when reporting on the Data Embassy
(source: www.securitytoday.com)
Chapter 2 – Diplomacy, Infrastructures and Affective Geopolitics

A term coined by the Estonian government to describe what is effectively a mechanism for ‘backing up’ the state to the cloud, the notion of a ‘Data Embassy’ may be a little deceptive or ambiguous to some. For geopolitical scholarship, a Data Embassy might immediately raise questions around territory, sovereignty and diplomacy – or even geopolitical logics of anticipation and survivability – as might any traditional spatialisation of the term ‘embassy’. Yet, with the term becoming something of a misnomer itself (the Data Embassy is not technically an embassy - merely functioning like one – see Chapter 4), how should such a term be conceptualised in the context of this research?

When considering a Data Embassy at a more practical level, novel questions also emerge around the (im)material infrastructures it capacitates - from the cables that connect the data centre to host state via the ethereal cloud, to data traversing national jurisdictions and borders. As we begin to consider how states may function with and operate from the cloud in the future, the Data Embassy also raises new theoretical challenges around the future of statehood and diplomacy. Whilst the emergence of the Data Embassy may also spark novel debates around notions of data sovereignty and extraterritoriality, with the potential to influence new directions within current disciplinary debates at the intersection of law, political geography and critical data and media/communication studies.

As we unpack the Data Embassy, then, beyond its early geopolitical discourses and imaginaries (see Chapters 1 and 3), a more complex picture begins to emerge. From the multitude of (im)material infrastructures and processes enacting upon one another at any given time (data centre, cloud, data), or possible shifts in statecraft and diplomacy, to a unique security context or affective geopolitics that necessitate its emergence, in this chapter I suggest that the Data Embassy can be better understood as a form of geopolitical assemblage. In his book Diplomatic Material (2017), political geographer Jason Dittmer applies assemblage theory through more of a geopolitical/IR lens in order to examine the “material circulations – of media, of objects, of bodies and their practices – that produce elite political subjectivities within the varying assemblages of the ‘international community’” (2017: 3). Building on Jane Bennett’s (2010) influential intervention on vibrancy, agency and materialism (i.e. ‘the force of things’), Dittmer’s notion of a geopolitical assemblage posits a “more-than-rational, more-than-human” (2017: 3) approach to understanding foreign policy, diplomacy and international relations, that moves beyond a certain fixation with the primacy of the human in political discourse (for other contributions on assemblage thought in geopolitics, see, Dittmer, 2014; Mostafanezhad and Promburom, 2018; Weir, 2020).

In this chapter and in the context of this research, I adopt the notion of a geopolitical assemblage in order to identify and conceptualise the various components and ‘material circulations’ that make up the Data Embassy. The following thematic discussion is divided into four sections: Geopolitical Infrastructures, The
Improvised State, New Diplomatic Studies and Affective Geopolitics. Although these themes are quite distinctive and disparate in scope, they do not claim to be exhaustive. Rather, this chapter is, first and foremost, intended to represent my initial reflections on the most prevalent conceptual challenges and debates posed by the Data Embassy and the environment it necessitates.

First, I focus on the geopolitical infrastructures that help shape and facilitate the Data Embassy (Section 2.1). In doing so I draw on a growing body of research that is becoming increasingly attentive to the material politics of the Internet and the global infrastructures that sustain and govern the spaces of everyday life. In particular, I focus on work that has drawn attention to the largely ‘invisible’ infrastructures that enable our increasingly digitalised world to function, from the colonial histories of subterranean fibre-optic cabling routes to the data centres where the cloud is understood to materialise.

Second, I shift my attention to the state as I consider how the Data Embassy may recalibrate many long-held assumptions regarding statehood in the future (Section 2.2). To do so, I examine the Data Embassy in the context of wider contemporary debates around the role and function of the state, drawing on Jeffrey et al.’s (2015) notion of anomalous geopolitical spaces and entities where “international norms and ideals of statehood […] are called into question” (2015: 180).

Third, I examine the changing nature of diplomacy and situate the Data Embassy within a growing scholarly interest in forms of ‘alternative’ and ‘unofficial’ diplomacies that are exercised and performed at the margins of political life (Section 2.3). In particular, I focus on the embassy as a fairly neglected site of diplomatic inquiry, whilst also examining the Data Embassy’s relationship to other forms of public diplomacy, such as the growing utilisation of virtual embassies and nation branding.

Finally, to begin unpacking the question of whether or not Estonia is experiencing a form of state-level anxiety (see Chapter 6), I draw on a growing body of work that engages with affect, anxiety and other emotions in world politics (Section 2.4). In particular, I focus on Gerard Toal’s work on affective geopolitics in the context of Russia’s near abroad, and aim to conceptualise Estonia’s anxiety within a wider history and geopolitical context, and how this potentially shapes our reading of the Data Embassy and post-Soviet space.

2.1 Geopolitical Infrastructures

When considering the Data Embassy in more practical terms, one might start to think about its inner mechanics and wider functionality. How do Data Embassies connect to their host state? How are data backed up to the cloud (wherever that may be…)? What happens if state data are intercepted in transit by an adversary? From the intense whirls of server racks inside a data centre, to the encrypted packets of data zipping across vast
interconnected networks of fibre-optic subterranean cabling at imperceptible speeds, the Data Embassy assemblage should first and foremost be understood by the amalgamation of (im)material infrastructures it facilitates. For the average person, these ‘global’ infrastructures are largely invisible – often concealed, secretive and underground – as they form the ‘taken-for-granted’ background of our everyday lives (Graham and McFarlane, 2015). Yet, despite their near ubiquity for many, seldom are the power and agency of such infrastructures considered as they form the crucial cogs in today’s networked digital world. With many of these infrastructures exhibiting their own complex colonial/Cold War histories and geographies, might we also, as Louise Amoore (2018) warns, be turning a blind eye to their inherent ‘geopoliticalness’?

In this section, I turn our attention to the geopolitical infrastructures that help shape and facilitate the Data Embassy. In doing so, I draw on a growing body of research that is becoming increasingly attentive to the material politics of the internet and the global infrastructures that sustain and govern the spaces of everyday life. The term infrastructure has been used since the nineteenth century – initially, as a French term used to describe the construction of France’s railroads during the Industrial Revolution, before becoming synonymous with NATO jargon and military planning during the Cold War (Parks, 2015; Lewis, 2008). Since then, infrastructure has increasingly become a ‘catch-all’ term, denoting all manner of mundane systems and services that underpin much of modern life and society today – such as power grids, bridges, motorways, subways, dams, satellites, and sewer systems. As John Durham Peters writes, infrastructures invite us to explore “the basic, the boring, the mundane, and all the mischievous work done behind the scenes” (2015: 33), and they have since become the focus of scrupulous academic inquiry across fields such as urban studies, geography, digital humanities and science and technology studies (STS) (see, for example, Balbi et al., 2016; Barry, 2013; Carse, 2014; Cowen, 2017; Easterling, 2014; Furlong, 2011; Graham, 2010; Graham and McFarlane, 2015; Guldi, 2012; Larkin, 2013; Star, 1999).

However, in keeping pace with general advancements in technology and communications, the last decade or so has also seen a growing interest in the social, political, cultural and material dimensions of the infrastructures that “undergird and sustain communication networks and media cultures across the world” (Plantain and Punathambekar, 2019: 165). This ‘infrastructural turn’ has largely been driven by scholars within media and communication studies (see, Larkin, 2008; Mattern, 2017; Parks and Starosielski, 2015; Peters, 2015), where the term ‘media infrastructures’ has been coined to signify the “material sites and objects involved in the local, national, and/or global distribution of audiovisual signals and data”, and which include specific sites/objects such as “broadcast transmitters, transoceanic cables, satellite earth stations, mobile telephone towers, and Internet data centers” (Parks, 2015: 356). Lisa Parks and Nicole Starosielski’s edited collection Signals Traffic (2015) offers us one of the earliest (and most joined up) explorations in this area, with scholars conceptualising sites/objects such as undersea cables, data centres and mobile telephone
systems, highlighting their complex material formations and the affective relations they generate as they operate at various scales and across numerous geographies.\(^1\)

One of the most significant developments from this body of work (and of relevance to this thesis) has been the increasing attention paid to the materiality and politics of the Internet – specifically, the cables or ‘tubes’ that form key data routes between large, strategically interconnected computer networks and exchange points, and make up the arterial backbone of the Internet’s infrastructure (see, Blum, 2012; Burrington, 2016a; Fish, 2018; Starosielski, 2012; 2015). In her book, *The Undersea Network* (2015), Starosielski goes in search of the ‘visual traces’ left behind by the Internet in a journey that explores the vast interconnected networks of transoceanic cabling that now zigzag across the globe (see Fig. 2.2), taking us from cable landing points in Hawaii (U.S.) and Muriwai (New Zealand) to colonial cable stations in Guam and Fiji in the Pacific. Her “archaeology of undersea networks” (2015: 227) is an important contribution to the literature, for it not only seeks to make the material systems that underpin the ‘immaterial’ Internet visible, but also crucially reveals the complex histories and geopolitics that lie alongside these infrastructures.\(^2\) Arguing that cable routes have been “critically shaped by territorial politics” and “continue to be constructed in a dense web of existing territorial affiliations” (2015: 12), Starosielski’s work speaks to the growing recognition of the undersea cable’s deeper colonial/imperial legacies, as well as its importance to national security today.\(^3\) (see, Mainwaring and Aldrich, 2019; Smithies, 2008; Thorat, 2019).

---

1 For other work that seeks to explore the relationship between infrastructure and affect, Ryan Ellis (2020) examines how key national infrastructure in the U.S., such as the postal system, freight rail network and electric power grid, were remade and reordered post-9/11 (see Section 2.4 for more detailed discussion on affect in the context of this research).

2 Such work also builds on a growing body of research that focusses on subterranean geopolitics and the material, political and elemental politics of underground spaces (see, for example, Billé, 2020; Elden, 2013; Graham, 2016; Klinke, 2019; Squire, 2016; Squire and Dodds, 2020).

3 It is well known that lots of undersea cable routes follow the path of pre-existing telegraph/telecommunication cable networks – such as the transatlantic telegraph cable first built in the 1850s. Writing about the Trans-Tasman Cable between Australia and New Zealand, James Smithies (2008) notes how the cable served as a symbol of British imperial power and expansion. Scholars have also discussed the cable’s inherent insecurities and its role within wider intelligence gathering, highlighting longer histories of cable ‘tapping’ and cable ‘cutting’ from intelligence agencies (Aldrich and Karatzogianni, 2020; Khazan, 2013).
Beyond the cable, another vital component of the Data Embassy’s infrastructure and assemblage is the cloud – the technology enabling the Estonian government to ‘backup’ critical components of the state (information systems, databases, registries) outside of its own borders. If the Internet can be understood as a global network of computers all linked together through fibre-optic data cables and exchanges, then ‘the cloud’ describes the unique way of using that network – in short, the pooling of computing power and resources onto servers that are accessed over the Internet (and the use of software and databases that run on those servers). Over the last two decades we have seen an explosion of interest in cloud computing, as businesses and governments increasingly turn to cloud-based services in order to improve service continuity and reduce IT costs, as well as improved efficiency, flexibility and scalability of their day-to-day operations.

Despite all of this attention, it would be fair to say that wider discourse around the cloud is somewhat murky and misunderstood. Such is the technology’s ubiquity today, many people are probably unaware that they use the cloud on a daily basis – for example, to store personal photos and data (e.g. iCloud/Dropbox), share and collaborate on projects and everyday tasks (e.g. Google Docs/Office 365), or even to access their favourite entertainment services (e.g. Netflix/Spotify). Similar to other media infrastructures highlighted so far in this section, the cloud appears to have slipped into the taken-for-granted background of modern life, with little public consideration as to what the cloud even is, how it works, or where it is located. Conceptually, the cloud is often envisaged as being virtual, ethereal, mute, or even stateless (see, Hu, 2015; Irion, 2012; Jaeger et al., 2009; Taylor, 2018). Complemented (or perhaps complicated) by a host of other metaphorical jargon – the data centre, server farm, or data lake – it can be argued that the cloud is at times nothing more than a “moving target of misunderstood buzz words” (Chee and Franklin, 2014). In artist and journalist Ingrid Burrington’s timely and insightful series of depictions of the cloud’s infrastructure across North America (2014; 2015a; 2015b; 2016b), what we see is a highly marketed metaphor that rarely sheds light on where our data actually resides:

“One imagines metadata floating, like a thought bubble in a comic strip, away from a personal computer to some impossible destination that is at once everywhere and nowhere in particular.”

Figure 2.3 – A common depiction of ‘the cloud’ found across industry and media (source: www.innovationatwork.ieee.org)

Nevertheless, Burrington’s work has coincided with a recent scholarly turn that aims to contest such metaphor usage – along with the assertion that the cloud is somewhat virtual, nebulous and imperceptible to us as humans - and to instead engage with the cloud’s physical manifestations where it is understood to
materialise (see, Amoore, 2018; Bratton, 2015; Bridle, 2018; Hu, 2015; Jaeger et al., 2009; Neilson et al., 2016; Parker, 2020). Chiming with Sam Kinsley’s (2014) call for greater engagement with the materiality of virtual geographies and the digital, such work aims to recognise the cloud’s various material forms and spatial configurations, whilst also highlighting its significance to wider infrastructural debates (Furlong, 2020). Beyond the “fluffy ethereality the cloud metaphor conjures”, notes social anthropologist Alexander Taylor (2018), “the creeping ubiquity of cloud computing is underpinned by an expansive digital-industrial infrastructure that is aggressively expanding across the surface of the planet”. Indeed, as Louise Amoore suggests – and as Burrington discovered on her ethnographic ventures in search of the cloud across northern Virginia and Arizona – “the whereabouts of ‘unseen computers’ is not unknown at all, but rather the cloud is actualized in data centres” (2018: 8).

In the context of this research, the data centre functions as one of the most crucial components of the Data Embassy’s infrastructure. Not only is it the site upon which the Estonian government is entrusting critical components of the state’s infrastructure and archives, but it also operates as an exceptional geopolitical space whereby diplomatic privileges are afforded to Estonian data and information systems. In short, data centres are the physical facilities that house the network and computing infrastructure necessary for the cloud to operate and function. Consisting of various servers, storage systems, routers, switches and firewalls, their primary purpose is to collect, store, process and distribute vast amounts of data within a secure, controlled, resilient environment. Due to unprecedented global demands in data usage and storage, the last decade or so has seen a rapid growth in data centre infrastructure, as large corporations such as Google, Amazon and Facebook seek to expand their enterprises across the globe (Hogan, 2015a). As the data centre industry has continued to expand, so too has its ‘visibility’ and significance in society, as a growing number of journalists and academics have been drawn to trying to uncover and better understand what lies behind its (often) large, faceless, heavily securitised exteriors (see Fig. 2.4). As such, the data centre has become a crucial site of inquiry for scholars to not only “counter widespread myths about the immateriality of ‘the digital’ and cloud computing” (Hogan, 2018: 3), but also to explore the role the data centre plays within wider social, political and environmental debates – with a growing number of studies in fields such as media and communication studies, sociology, anthropology and geography (see, Furlong, 2020; Hogan and Vonderau, 2019; Holt and Vonderau, 2015; Johnson, 2019a; Taylor, 2019; Vonderau, 2019).
As Taylor (2017) notes, in recent years the data centre has risen from a fairly nondescript and unremarkable element or ‘node’ of the Internet’s infrastructure (often the scope and interest of the IT and network security technician), to the focal point of a number of key sociopolitical/geopolitical debates: from recent hacking scandals that have drawn attention to the “ethics and (in)security of practices and processes of data storage”\(^4\), to the rise and implementation of various data localisation/sovereignty laws across the world (see below) and the impact this has had on data centre construction in ‘information friendly’ countries such as Sweden, Iceland and Luxembourg (see Section 4.2). Furthermore, amidst the impending global climate crisis, the data centre has also become a site of environmental contestation due to its resource-intensive processes and high energy consumption - and how this has pushed the data centre industry to more peripheral locales (see, Burrington, 2015c; Hogan, 2015b). Indeed, the siting or stationing of a data centre can be deemed geopolitical in and of itself, with its location highly dependent on access to large amounts of cheap land (that is also free from political opposition); favourable cooler climates and access to natural resources; favourable tax rates; physical security and proximity to both the backbone of the Internet and transportation networks (Amoore, 2018; Blum, 2012; Burrington, 2014; Hogan, 2015b; Hu, 2015). As Andrew Blum notes:

“Siting a data center is like the acupuncture of the physical Internet, with places carefully chosen with pinpoint precision to exploit one characteristic or another. As competitive companies thrust and parry for advantage, it becomes clear that some places are better than others, and the result is geographic clusters.”

(Blum, 2012: 232)

Due to their required proximity to the backbone of the Internet, scholars have also recognised that many of these ‘geographic clusters’ are built on the “material legacies of pre-existing infrastructures” (Furlong, 2020: 3) and are thus entangled in much deeper imperial/Cold War histories (see, Hu, 2015; Johnson, 2019b). This has also led to an interest in the growing industry trend of

\(^4\) For example, the hacking of Sony Pictures in 2014, or notable examples of data breaches in companies such as TalkTalk (2015), Equifax (2017) or EasyJet (2020), with the exposure of millions of customers’ personal data.
‘repurposing’ and ‘retrofitting’ former industrial buildings and underground bunkers into data centres (see, Fish and Garrett, 2019; Hu, 2015; Jacobson and Hogan, 2019). In *A Prehistory of the Cloud* (2015), Tung-Hui Hu refers to the role that the ‘data bunker’ plays as a secure fortification across an “unsafe Internet” (2015: 81). Taking the form of a purpose-built server-farm nestled beneath bustling mega-cities (Garrett et. al, 2016) or a retrofitted former nuclear bunker in the English countryside (see Fig. 2.5), the bunker’s fortified subterranean structure is now being heavily marketised by many in the data centre industry as the optimal location for secure and reliable data storage. As spaces that were originally associated with survivability in the aftermath of a disaster/apocalypse, Hu notes how the data bunker plays powerfully on Cold War imaginaries and security/sovereignty discourses today: “the sovereign’s rationale for a bunker or a keep, to defend an area of territory, has now become transported to the realm of data” (2015: xxviii). Paul Virilio (1994) and others have written about how the bunker invokes the spectre of future disaster, and, in the context of this research, the data bunker serves as a useful imaginary as I consider how the Data Embassy functions as a form of extraterritorial bunker for the Estonian state with the promise of greater security and sovereignty in the event of an emergency.

So far, this section has considered what kind of media infrastructures and technologies play vital roles in the function of the Data Embassy (both as an individual entity and as part of a potentially much wider network of ‘Data Embassies’ in the future). To conclude, however, I turn my attention to another crucial facet of the Data Embassy’s geopolitical infrastructure and assemblage: data. Whilst data may have been the focus and attention of a number of burgeoning debates across fields such as critical data studies, digital humanities and geography of late (see, Ash et al., 2018; boyd and Crawford, 2012; Dalton et al., 2016; Hintz et al., 2019; Iliadis and Russo, 2016; Thatcher et al., 2018), there has arguably been little work

Figure 2.5 – Images taken from a visit to Hack Green, a former government-owned nuclear bunker in Cheshire, UK. Now the site of a museum, an area of the site has also been retrofitted into a modern data centre (author’s own images)

---

5 Inspired by the ethnographic ventures of the likes of Burrington (2015a) and Taylor (2017), I visited a ‘data bunker’ site in North West England in 2018 as part of a small academic side-project. The former Cold War nuclear bunker is now a museum, but also home to a small data centre company (see Fig. 2.5).

6 For other notable studies on the bunker, see: Beck, 2011; Bennett, 2017; Garrett, 2020; Klinke, 2018.
undertaken that considers data as a form of infrastructure itself, and how other infrastructures bring data into being, circulation and action”.

Data play an integral role in the context of this research – first, as something of enormous value and importance to the Estonian state, and second, as part of the Data Embassy assemblage’s wider political, legal and ‘material circulations’ (Dittmer, 2017) – and as such raises a number of critical questions as we consider data and its relationship to other geopolitical infrastructures that facilitate the Data Embassy. For instance, how do data interact with infrastructures as they travel along undersea cabling, through Internet exchanges and beyond the data centre? What happens when data moves beyond certain territories and borders, and is subject to certain national laws? Or what happens when data stop moving altogether – and are considered at ‘rest’? Although these questions are beyond the scope of this thesis, they highlight the Data Embassy’s relevance to a number of emerging debates and potential new directions of research that consider the agency, mobility and circulation of data. As another point of motivation, such questions also help to counter the perceived immateriality of data in relation to other infrastructures. Paul Dourish expands on this point by stating:

“The digital material that concerns me is not the materiality of the infrastructure and wires but the materiality of the digital signals that cross them. I argue that data and their protocols are also material, both in their consequences for the organization of infrastructures and in their specific manifestations as flows of electrons and signals that spread out over the wires and channels.”

(Dourish, 2015: 184)

Concerning mobility, over the last few years a number of scholars have attempted to theorise the movement, circulation and flow of data, and what material/political affects this can have. Nat O’Grady (2017) and Andreas Baur-Ahrens’ (2017) work in the recently edited collection Security/Mobility (Lees and Wittendorp, 2017) offer two timely contributions to this topic. O’Grady, writing in the context of UK emergency response and governance, examines how data moves and ‘circulates’ through the UK Fire and Rescue Service and wider digital infrastructures, and how this data is then transformed into information relevant for the governing of fire risk (for other relevant studies that focus on data and their circulatory effects: see, Balbi et al., 2016 and Beer, 2013). Baur-Ahrens, on the other hand, analyses the impact of ‘data territorialisation’ on the mobility of data traffic routed through the Internet, as an increasing number of states seek to control the flow of national data over domestic infrastructure and within their

---

7 It could also be argued that geopolitics has yet to fully engage with geography’s so-called recent ‘digital turn’ (Ash et al., 2018) and thus there is a lack of detailed discussion around the geopolitics of the digital and data – although notable exceptions do exist (see, Amoore, 2013; Crampton, 2018; Robin and Acuto, 2018).
own territorial borders. Such a trend speaks to a number of ongoing debates at the intersection of technology, law and society at present, as scholars grapple with (frequently interchangeable) notions of data localisation, data nationalism and data sovereignty (see, Komaitis, 2017; Kuner, 2015; Polatin-Reuben and Wright, 2014).

In what many see as a direct response to Edward Snowden’s intelligence leaks in 2013 (revelations that detailed U.S. and other states’ surveillance activities across the world), a number of states are now taking steps to limit the storage, movement and processing of data within certain geographies and jurisdictions. Some of the most stringent data localisation laws have been implemented in China, Russia, Indonesia and Vietnam, and, as Jonah Hill notes, are viewed as “an effective means to control information and to monitor the activities of their citizens” (2014: 4). But, in a post-Snowden world, we are also seeing democratic countries such as Brazil, India, Australia, France and Germany take steps to ensure that citizens’ data are stored on physical servers within the country’s own borders (see, Chander and Lê, 2015; Nugraha et al., 2015). Despite there being purported benefits for states regarding data privacy and security, scholars have expressed concerns that data localisation will backfire (Chander and Lê, 2015) and could lead to what some scholars are terming as the ‘balkanisation’ of the Internet (or Cyberbalkanisation), where various competing technological, political, religious and commercial factors cause the Internet to fragment and splinter in a number of factional national Internets that are aligned by geographical boundaries (see, Fraser, 2016; Polatin-Reubien and Wright, 2014).

Nevertheless, it is important to recognise that data and the specific technologies and infrastructure of the Internet do not correspond or map onto national borders, jurisdictions and laws, and as such travel around the world with “little relationship to physical territory” (Berman, 2018). For legal scholars in particular, this has meant that issues around the use, control and flow of data are of increasing importance and debate (see, Daksal, 2015; 2018; Eichensehr, 2017; Woods, 2016). This is particularly relevant in an era of cloud computing, where states have overlapping, yet legitimate interests in accessing and protecting data that is stored ‘in the cloud’ (Shurson, forthcoming). Jennifer Daksal notes how this is problematic as data is increasingly “moved around for technical processing” and “copied or divided into component parts and

---

8 In his work, Baur-Ahrens conceptualises data territorialisation into two distinct areas: 1) the routing of data, in an effort to control data flows through national servers, and 2) the location of data storage, so that data are stored on “servers that are physically located in their national territories” (2017: 44).

9 In China, its strict data localisation laws can be seen in conjunction with its government’s strict system of legal and technological Internet controls, often referred to as the Great Firewall of China. In Russia, for example, their recently passed data localisation laws prohibit the storage of Russians’ personal data outside of the country’s borders, whilst operators must disclose the physical locations of data centres (Chander and Lê, 2015). Some commentators have noted how Russia’s localisation laws are also implemented in response to domestic and regional concerns, and as a means of censoring information and controlling dissidents (Newton and Summers, 2018; Walker, 2015). For Indonesia and Vietnam, both now considered emerging cyber powers across the region of ASEAN states, such laws have sought to protect themselves from the economic interests of big global corporations by mandating those who provide ‘public services’ to establish a local data centre within their borders. Indonesia have had strict data localisation laws since 2012, with Vietnam following with its own “Law on Cybersecurity” in 2019, although both now appear to be reneging slightly after strong lobbying from Big Tech companies (Basu, 2020).
stored in multiple places—some territorially and some extraterritorially” (Daksal, 2015: 366). As Kristen Eichensehr goes on to argue, this poses significant difficulties for determining where data are located:

“The problem is not that data is located nowhere, but that it may be located anywhere, and at least parts of it may be located nearly everywhere. And access to data does not depend on physical proximity.”

(Eichensehr, 2017: 145)

Such work is of relevance to this research for two reasons. The first is that there is a clear conceptual overlap between geography and international law in this area, as scholars attend to notions of territoriality, sovereignty, borders and mobility in the context of cybersecurity, Internet infrastructures and data flows (I would argue, however, that there is scope for greater interdisciplinary research in this area, as these terms have different interpretations when used in within individual disciplinary silos). The second concerns different states’ approaches to data sovereignty. Whilst data sovereignty refers to the broad spectrum of approaches “adopted by different states to control data generated in or passing through national internet infrastructure” (Polatin-Reuben and Wright, 2014: 1), it is clear that the Data Embassy goes against this principal as the Estonian government is actively seeking to store its data outside of its own borders (albeit extraterritorially in a government-operated data centre). Although beyond the remit of this thesis, I believe the Data Embassy will continue to speak to many of the ongoing debates regarding data sovereignty and data extraterritoriality, and is thus worthy of further interdisciplinary attention moving forward.

2.2 The Improvised State

_Hibernation, Exile and the Virtual State_

In the previous chapter, I outlined the hypothetical scenario whereby the Estonian state could effectively go into ‘hibernation’ in the event of an emergency. An idea first put forward by journalist and author Ben Hammersley, it referred to the process of backing up critical components of the state’s digital infrastructure (such as key information systems and databases) – either physically to hard drives or virtually via the cloud – only to then be able to restore and “boot back up again when the time is right” (Hammersley, 2015). Whilst the idea may seem fairly far-fetched in principle, the practice of hibernating or ‘backing up’ the state in the event of a crisis or emergency may be a particularly alluring prospect for those states facing any number of existential anxieties today. For a state facing the threat of a crippling DDoS...
cyberattack, forced annexation, or destructive natural disaster, a Data Embassy may evoke a number of distinct imaginaries regarding the future survivability of the state.\[11\]

In this thesis, I am interested in exploring what the Data Embassy’s emergence may mean for our understanding of contemporary statehood in the twenty-first century. Indeed, the very idea of the state going into hibernation, or being able to exist or operate entirely virtually from the cloud, raises some very important questions regarding how the state may function in the future. Further, I wish to examine how the Data Embassy may recalibrate many long-held assumptions over statehood and how the state may endure in more testing circumstances, particularly in the context of an emergency (see Chapter 7). In this section I draw on contemporary conceptualisations of the state and examples where ideals of statehood are brought into question.

Today, the state is recognised as more than simply a fixed administrative entity and rigid set of institutions and practices. Building on the influential work of Philip Abrams (1988), over the last few decades scholars have increasingly conceptualised the state as more of a process or ‘idea’ (Jones, 2007; Mitchell, 1991; Nugent, 2019; Trouillot, 2001). In geography in particular, a number of scholars have utilised the state idea as a means to explore its fragmented nature and the way in which ‘stateness’ permeates our everyday life (see, Gill, 2010; Jeffrey, 2013; Neocleous, 2003; Painter, 2006).

In this thesis I am particularly interested in Alex Jeffrey’s (2013) work on the state, an entity he argues is “politically and intellectually seductive” (2013: 4). Jeffrey’s central claim is that states are improvised, in that their legitimacy and capacity to lay claim to rule relies on their ability to perform power: “[A]ll assertions of statehood are improvisations, since statehood is secured through repeated performances of power” (2013: 178). Writing in the context of Bosnian state building since the 1995 Dayton Peace Agreement, Jeffrey’s work explores how the state has enacted particular performances in both an international and national political context – such as implementing new legal frameworks, restructuring state services and the seemingly more banal acts of renaming streets – and how this constitutes the view of a rational and intelligible Bosnian state. Jeffrey’s metaphor of improvisation is useful in the context of this research as I examine the everyday practices of the Estonian state in relation to the Data Embassy (see Chapter 5). In this thesis I view the Data Embassy as a form of state improvisation itself, as Estonia aims to routinely performs its ‘stateness’ and claims to political legitimacy through the extraterritorial space of the data centre (see Chapter 7).

---

11 I was also struck by how the idea of a state going into ‘hibernation’ was evoked during the recent COVID-19 crisis, as governments across the world enacted radical economic policies that effectively put the economy into hibernation for months during the pandemic (Dombey, 2020; Norman, 2020).

12 This institutional view of the state has largely been influenced by Max Weber’s writings on the state, which he defined as a “human community that (successfully) claims the monopoly of legitimate use of physical force within a given territory” (Weber, 1958: 78).
Whilst the state is often viewed as the primary source of political legitimacy, recently we have seen a growing interest in examples whereby legitimacy is projected from outside the traditional statist perspective. In their 2015 Special Issue ‘Understanding Legitimacy’ in the journal *Geoforum*, Alex Jeffrey, Fiona McConnell and Alice Wilson open up a body of work that examines alternative sites of political legitimacy and what they term as ‘anomalous geopolitical spaces’. These are sites that embody “unrecognised, contested or alternative forms of geopolitics from that of a sovereign state” (Jeffrey et al., 2015: 177) and where “international norms or ideals of statehood, that is a neat coincidence of statehood, territory and sovereignty, are called into question” (2015: 180). Drawing greater attention to the role and function of entities such as de facto states, annexed territories, quasi-(or proto-)states, states-within-states and governments-in-exile, their work is a call to “move away from a state-centric notion of legitimacy to challenge dominant narratives of sovereignty and think instead of situations where the loci of legitimacy is dispersed and situated outside of formal state structures” (Jeffrey et al., 2015: 178 – for other notable studies in this area, see, Caspersen, 2012; Jackson, 1991; Kingston and Spears, 2004; Lynch, 2004; McConnell, 2016). In this thesis I argue that the Data Embassy may be better understood through the lens of anomalous geopolitical spaces, as I contend that ‘international norms and ideals of statehood’ are arguably called into question with regards to the function of the extraterritorial data centre and attempts at enhancing Estonia’s political legitimacy (see Chapter 7). Speaking to Fiona McConnell’s influential work on the Tibetan Government-in-Exile (2009; 2016), I also explore whether the Data Embassy is symbolic of a Government-in-anticipation-of-Exile as the Estonian government aims to manage its own everyday geopolitical anxieties (see Chapter 6).

This section concludes with some brief reflections on how the state could be conceptualised in the future. As highlighted in Chapter 1, the notion of a Data Embassy opens up novel questions around whether a state may function from the cloud, or even exist entirely virtually, in the event of an emergency. Whilst I address these themes later in the thesis (see Chapter 7), it does speak to a number of debates regarding the virtualisation of the state in a digital age. The notion of a virtual state has gained most traction in the fields of information technology, public administration and e-governance, but are largely consigned to processes of digitalisation found across society (Fountain, 2001; 2006; Frissen, 1997; Garson, 2006). For Jane Fountain, a ‘virtual state’ is largely metaphorical, drawing attention to increasing use of ICT and digital technologies across the state’s public sector, and how these are a catalyst for “fundamental changes in the nature and structure of the state in the information age” (2006: 149). It is important to note, however, that studies such as these are predominantly focussed on the virtualisation of public services, not the entire apparatus of the state.

Interestingly, the idea of a ‘virtual’ or ‘digital’ state has perhaps had the most currency in Estonia to-date (see Chapters 4 and 5). Indeed, since the late 2000s, Estonia has adopted the moniker ‘e-Estonia’ – a shorthand label used to highlight the country’s successes in digital transformation, whilst also serving as an
attestation of Estonia’s successful transformation from post-Soviet transition state to today’s advanced digital society (Mäe, 2017). Since then, Estonia has developed (and benefitted heavily from) its powerful narrative as a ‘digital nation’ and ‘pioneer’, whilst scholars have also noted how this has been employed effectively as part of the state’s wider nation branding agenda (Tammpuu and Masso, 2018 – see Section 2.3 and 5.3). Scholars elsewhere have also considered the nature and function of the state in a digital age. For Katharina Pistor, statehood will take on new configurations where new digital states may be “based primarily on data, not territory” (see Section 6.1.1 where one respondent makes a claim remarkably close to this in an Estonian context). Building on work relating to geopolitical infrastructures highlighted in Section 2.1, James Maguire and Brit Ross Winthereik (2019) have considered the impact that data centres are having on the ongoing digitalisation of the state, examining the role that ‘Big Tech’ is playing in territorialising the state and its resources. Meanwhile, Abdel-Bari Atwan (2016) has written about the role technology has played in the function and existence of the Islamic State, highlighting how the “digital caliphate” utilised the Internet and other digital communication tools (such as the dark web) to spread its message, recruit fellow sympathisers, and evade global intelligence agencies (in Chapter 7, I discuss how the Data Embassy concept has been reimagined in the context of ISIS).

2.3 New Diplomatic Studies

Embassies, ‘Twiplomacy’ and Branding the Nation

Diplomacy, broadly understood, is “the practice of conducting negotiations between representatives of distinct communities or causes” (Dittmer and McConnell, 2016: 1). A practice that has existed for millennia, formal traces of diplomacy have been recorded as far back as the fourteenth and eleventh century BCE in ancient Egypt and imperial China (Bjola and Komprobst, 2013). Diplomatic historian Eileen Denza (2009) has written about how diplomatic envoys in ancient Greece were considered sacrosanct and were afforded personal inviolability as they travelled between different cities in order to negotiate war, peace and other commercial endeavours. Diplomacy in its modern form can be dated back to the early Renaissance period in Northern Italy (fourteenth and fifteenth century), where powerful city-states such as Florence, Venice and Milan established permanent diplomatic missions and resident ambassadors as a means of balancing power and resolving disputes between rival rulers (Fletcher, 2015; Mallett, 2001). At the end of the Second World War, diplomacy became increasingly formalised and universal in its practice, with the adoption of the Vienna Convention on Diplomatic Relations (VCDR) in 1961 (VCDR, 1961). Setting the framework from which sovereign states were able to establish, maintain and (if necessary) terminate diplomatic relations with one another, the VCDR established universal diplomatic norms and is widely regarded as the “cornerstone of modern diplomacy” (Bruns, 2014: 16) and a vital tool in maintaining peace and security globally.

Whilst modern forms of diplomacy are generally understood to be the purview of the experienced diplomat or politician – traditionally taking place in the ministerial office, at the negotiation table or at the press conference – there is increasing recognition of the ways in which diplomacy is practiced beyond the
conventional method of negotiation between sovereign states. As such, scholars are becoming increasingly attentive to the 'alternative' sites, actors and practices of diplomacy that “transcend traditional state-centric modalities” (Jackson, 2018: 1), focusing instead on the interplay between state and non-state actors, supra/subnational entities and NGOs, and forms of ‘unofficial diplomacy’ that are exercised and performed at the margins of political life (see, Hocking, 2011; Langhorne, 2005; McConnell et al., 2012). In an increasingly globalised and digital world, diplomacy is also having to adapt and transform, as states seek to find new and inventive ways to connect and communicate with each other, their citizenry, and now even large transnational corporations that are now ‘state-like’ in their power and outreach (see, Klyngé et al., 2020; Muldoon Jr., 2006).

In this thesis, I am interested in understanding what impact the Data Embassy may have on the future practice of diplomacy. For instance, will new diplomatic relations be forged or improved through the creation of new Data Embassies? Can an embassy be conceptualised beyond its traditional confines? Or does the advent of more Data Embassies in the future potentially call pre-existing (and arguably outdated) international laws and conventions into question? Although these questions are addressed later in this thesis (see Chapter 7), this section draws on work that addresses the changing nature of diplomacy, whilst examining how such debates are relevant in the context of the Data Embassy.

Over the last few decades, a number of scholars and practitioners have started to sketch out new directions of research in the study of international diplomacy (see, Bjola and Kornprobst, 2013; Hocking et al., 2012; Melissen, 2005; Rana, 2011; Riordan, 2003). This includes a growing interest in novel forms of public diplomacy, where new theoretical and empirical insights have been developed around notions of soft power (Chitty et al., 2016; Nye, 2004), digital and cyber diplomacy (Bjola and Holmes, 2015; Riordan, 2019), and nation branding as states seek to improve their image and reputation on the global stage (Aronczyk, 2013; Kaneva, 2012). The study of diplomacy has also been enriched by a growing body of work in areas of political geography and critical geopolitics, with scholars attending to the various everyday practices, spaces and cultures of diplomacy13 (see, Dittmer and McConnell, 2016; Khatib and Dodds, 2009; Kuus, 2013; Pinkerton and Benwell, 2014). Furthermore, a number of scholars have also shown an interest in ‘newer’ forms of diplomacy that operate beyond a traditional statist perspective, with studies that focus on non-state actors and groups such as NGOs (Betsill and Corell, 2008; Cooper and Hocking, 2000), businesses and large corporations (Ordeix-Rigo and Duarte, 2009; Strange, 1992), indigenous groups and marginalised communities (Abele and Rodon, 2007; Beier, 2010; Henderson, 2008), and forms of ‘paradiplomacy’ that focus on the international activity and foreign policy capacity of subnational political entities (Jackson, 2018; Jackson and Jeffrey, 2019; Kuznetsov, 2015).

13 Political geographers Fiona McConnell (2020) and Merje Kuus (2013; 2018) have also been at the forefront of developing new methodological insights in the study of diplomacy with their ethnographic work inside large bureaucratic institutions such as the UN in Geneva and EU in Brussels – whilst also addressing recent calls to ‘study up’ in the social sciences (see Chapter 3).
In this thesis I am also interested in work that attends to forms of diplomacy that operate in unusual or unexpected spaces. Fiona McConnell, Terri Moreau and Jason Dittmer’s (2012) work on ‘unofficial diplomacies’ has been influential in this regard, adapting Homi Bhabha’s notion of *mimicry* to diplomatic discourse in order to investigate how non-state diplomacies “mimic and intervene” (2012: 805) within more formal structures of ‘official’ state diplomacy, thus exposing “the contingent practices that underlie political power in so-called ‘conventional’ states” (2012: 812). Drawing on empirical case studies from the Tibetan Government-in-Exile, the International Christian Embassy in Jerusalem, and UK-based micropatrias such as the Democratic Republic of Bobalania, McConnell et al. focus on how these non-state diplomacies perform and mimic aspects of ‘stateness’ in ways “that challenge the composition and status of the interstate system” (2012: 811). Such work is of relevance to my research as I consider how alternative forms of diplomacy are now enacted and performed with regards to the Data Embassy and within the ‘unusual’ space of the extraterritorial data centre – and how these go some way to constituting notions of recognition, sovereignty and legitimacy (see Chapter 7).

As highlighted above, scholars in diplomatic studies have long shown an interest in the many diverse sites and spaces where diplomacy is exercised and performed. Drawing on his experiences working in the Norwegian Ministry of Foreign Affairs, Iver Neumann (2013) for example, demonstrates how diplomacy is now imbricated in a host of other sites and practices, from the dining table during the lavish state banquet to the working breakfast during an international summit. The creation and maintenance of these ‘evented sites’, he argues, is at the heart of modern diplomatic work, and goes on to discuss the role that the planning, food and drink, atmosphere and setting itself plays in the practice of diplomacy (Neumann, 2016: 86). Alternatively, Fiona McConnell’s work investigating the Unrepresented Nations and Peoples Organization (UNPO), notes how diplomatic sites are also quintessentially “liminal spaces” where certain norms and rules of conduct are suspended are instead “associated with highly ritualised behaviour[s]” (2017: 143). In his work exploring Australia’s ‘invisible’ diplomacies, Clinton Fernandes (2020) argues how particular subterranean sites – such as the undersea telecommunications cable and state-led submarine/espionage operations – should be considered diplomatic sites in their own right, demonstrating their role and influence in contemporary Australian statecraft and foreign policy.

One site that still plays an integral role in the practice of modern diplomacy is the diplomatic mission or embassy. Yet, whilst scholars have shown an increasing interest in diplomatic sites such as the dining table or international summit, I argue that the embassy has received little analytical scrutiny or attention itself (for notable exceptions, see Cornut, 2015; Malone, 2012; Moore, 2016; Rana, 2013). Whether it is considering the embassy’s function as an extraterritorial outpost within another sovereign territory; the diplomatic privileges and protections they afford to ambassadors and diplomats; or even the building itself, which is central to many fascinating diplomatic practices, rituals and architectures of (in)securities, the
embassy remains a relatively neglected site of inquiry at present. This is surprising, further still, when you consider the embassy’s crucial function as an exceptional geopolitical space (and a space of contestation) during significant historical periods such as the Cold War (see, for example, Herspring, 1998; Hopkins, 2000; Vogeler, 1995). It is also worth noting how the embassy has functioned as a crucial tool in state legitimation practices – as shown by Estonia during the Soviet occupation (see Section 1.1). As Kishan Rana writes, “[F]or countries that were colonies and struggled long for their independence, the exchange of embassies is proof of sovereignty, i.e. their presence in the international system, and also their equality with other nations” (2016: 149). Furthermore, in a contemporary setting the embassy continues to be a key player in international affairs (Rana, 2013) and since 9/11 has been embroiled in a number of debates regarding location, security and architecture.

Consequently, I believe that a more extensive examination of the embassy would be a welcome and timely addition to the study of diplomacy. Drawing on Sara Fregonese and Adam Ramadan’s (2015) call for the hotel to be considered more than a ‘neutral site’ of leisure and tourism, in this thesis I argue that the embassy should be considered a ‘serious’ geopolitical site of inquiry in its own right, where its exceptional/extraterritorial spaces have the potential to open up new debates in the study of geopolitics, diplomacy and law. Moreover, I also contend that the Data Embassy should be understood as a new form of diplomatic site, where the data centre (or more specifically, a server room inside of the data centre) is now considered an extraterritorial space that is entangled in its own ‘unofficial’ diplomatic practices regarding the protection of Estonian data and information systems (see Chapter 7).

As mentioned at the beginning of this section, recent technological advances have contributed to major shifts in conventional forms of diplomacy, meaning that many diplomatic practices, institutions and norms have had to change and adapt in an increasingly digital age. As a result, the last decade or so has witnessed a growing scholarly interest in the notion of digital diplomacy (see, Bjola and Holmes, 2015; Hocking and Melissen, 2015; Manor, 2019). Broadly defined, digital diplomacy is a form of public diplomacy which concerns the growing utilisation of digital technologies and their transformative impact upon the practice of diplomacy in the twenty-first century. Work in this area has largely centred on the rise in use of social media for diplomatic purposes, as states look to embrace platforms such as Facebook and Twitter to engage with their own citizens and foreign publics in a non-costly manner (see, Bjola and Holmes, 2015; Duncombe, 2019). Reflecting on his time as British ambassador to Lebanon (2011-2015), Tom Fletcher (2016) writes of the power and influence his online Twitter presence heralded, at a time where traditional diplomatic channels were at an impasse due to the ongoing civil war that had spilled over the border from Syria. Indeed, social media (and Twitter in particular) has become an

---

14 For example, President Trump’s decision to move the Israeli embassy to Jerusalem in 2018 prompted public outcry across the world, whilst Julian Assange’s decision to seek asylum inside the Ecuadorian embassy in London in 2012 raised interesting debates around the role of diplomatic immunity and asylum inside an embassy (den Heijer, 2013). The brutal murder of Saudi Arabian journalist and dissident Jamal Khashoggi inside the Saudi consulate in Istanbul in 2018 also raised tensions between diplomatic law and international human rights (Milanovic, 2020).
increasingly popular terrain for politicians, diplomats and diplomatic representations, with ‘Twiplomacy’ being recognised as a crucial new form of diplomatic communication.\footnote{The use of embassy Twitter accounts by MFAs are a particularly growing phenomenon, demonstrating a dramatic shift in the ways in which diplomacy is now performed. On the one hand, they serve as useful sources of information for citizens living abroad - updating diasporic communities, expats and tourists on upcoming events and celebrations, whilst offering advice during periods of political unrest or crises (e.g. war or the recent COVID-19 pandemic). On the other, they have also been shown to have a controversial function too, orchestrating certain strategic state narratives whilst diplomatic communications have been known to breakdown as accounts descend into ‘Twitter wars’ (Robinson and Miltner, 2018).}

Beyond social media, digital diplomacy has also been recognised through various other guises. The U.S. are often regarded as the earliest pioneers of digital diplomacy when they established the US Digital Outreach Team in 2006, which aimed to engage directly with citizens in the Middle East by posting messages about U.S. foreign policy on internet forums (see, Khatib et al., 2012). One direct output of the programme came in 2011, when the Obama administration took the unusual step of opening a ‘virtual embassy’ in Iran (see Fig. 2.6) – a digital equivalent of its U.S. embassy in Tehran which had been closed since the Iranian hostage crisis in 1979. Its aim was simple: to promote U.S. policy to Iranian citizens and provide “another perspective and another source of information, so you can make up your own minds about the U.S., our concerns and about the Iranian government’s activities at home and abroad” (U.S State Department quoted in Erdbrink, 2011). Despite being nothing more than a website, it is important to note the virtual embassy’s crucial public diplomacy function - whilst also highlighting the way in which diplomacy can now be practiced and performed within virtual spaces. Since that time, we have also seen states experiment with other forms of ‘virtual embassies’, as countries such as Sweden, Colombia and Estonia all established digital diplomatic representations in the virtual online world Second Life (Bengtsson, 2011 - see Section 7.2.2 for a more detailed explanation). In truth, it may be difficult to gauge the success of virtual embassies on the practice of diplomacy at present, but as Ilan Manor (2014) has argued, shifts like these suggest that digital diplomacy could well become the norm in the future and “succeed where traditional diplomacy has failed”.\footnote{One other notable recent development in the practice of digital diplomacy has been Denmark’s introduction of the world’s first ‘digital ambassador’, Casper Klynge, in 2017. Klynge’s role, which is based between Copenhagen, Silicon Valley and China, forms part of the Danish government’s wider techplomacy initiative and aims to represent his country’s interests before large tech companies (such as Google, Facebook, Apple and IBM), some of which are so large that their accumulated power, wealth and influence far outweighs that of many countries around the world (see, Klynge et al., 2020).}
In this thesis, I am also interested in other forms of public diplomacy and the ways in which Estonia has sought to utilise its own powerful brand and image as a technological ‘pioneer’ and ‘pathfinder’ post-independence, and what role this may have played in the creation of the Data Embassy (see Section 5.3). Therefore, to conclude this section, I briefly focus on the growing phenomenon that is nation branding and its wider contribution to the study and practice of diplomacy. As Ying Fan posits, “nation branding concerns applying branding and marketing communications techniques to promote a nation’s image” (2006: 6), whilst Nadia Kaneva adds that it involves a “compendium of discourses and practices aimed at reconstituting nationhood through marketing and branding paradigms” (2011: 118). Growing in prominence throughout the 1990s and early 2000s, nation branding started life as a largely commercialised practice, dominated by leading branding consultancy firms such as Interbrand. In an effort to tackle a country’s ailing economy or reputation, branders work with national governments to ‘rebrand’ their image in order to boost tourism and attract more trade and investment. Today, for countries in political transition or perhaps facing something of an ‘identity crisis’, nation branding provides an

---

17 Simon Anholt and Wally Olins, two British branding consultants, are widely regarded as early pioneers of the concept, with both playing a vital role in establishing nation branding in consulting practice with governments and academia (Anholt established the journal Place Branding and Public Diplomacy). Despite claiming to have originally coined the phrase, Anholt (2010) has since distanced himself from the term, arguing that it has been distorted by “naïve governments” and consultancy firms as a way of branding a country into existence.

18 Changes can be predominantly cosmetic (for example, through the use of logos and slogans) but also institutionalised through the creation of “governmental and quasi-governmental bodies that oversee long-term nation branding efforts” (Kaneva, 2011: 118) – as seen in the UK with the establishment of the UK’s Public Diplomacy Board in 2002, or in Estonia with the creation of Enterprise Estonia in 2012 (see Section 5.3).
opportunity to reconstitute a country’s own national identity, whilst instilling a greater sense of civic pride amongst its citizens in the process (Kaneva and Popescu, 2011).

The practice of nation branding has received significant attention over the last decade or so, with a number of studies emerging in fields such as business studies and marketing, media and cultural studies, sociology and international relations (see, for example, Aronczyk, 2013; Dinnie, 2008; Fan, 2010; Kaneva, 2012; Szondi, 2008). As Christopher Browning and Antonio Ferraz de Oliveira (2017) have noted, however, political geography and critical geopolitics has had surprisingly little to say on the phenomenon (although their Special Issue on the topic attempts to tackle this particular gap in the literature – see Browning and de Oliveira, 2017). This could be considered unusual, especially as nation branding touches on other notable themes and debates in geography and world politics, such as city and regional place branding (Braun et al., 2013; Nathan et al., 2019), soft power and the mega event (Leonard, 1997; Szostek, 2017; Werther, 2011), and national identity and nation-building (Bolin and Ståhlberg, 2010; Browning, 2015; Jordan, 2014).

Sue Curry Jansen has observed how many states turned to nation branding at the end of the Cold War as a way to “redefine and reposition themselves within the master narrative of globalization” (Jansen, 2008: 121). As Jansen explains, after the breakup of the Soviet Union in 1991, commercial branders such as Interbrand were well-positioned to take advantage of states that were transitioning and re-emerging from behind the Iron Curtain:

“Nations that had literally disappeared behind the shadow of the USSR for almost a half-century, as well as the new nations that emerged out of former Soviet territories, faced unique challenges in their transition into the neoliberal global market economy. Not only did they require radical reorganization of their political and economic infrastructures, they also needed to be introduced or re-introduced to the world.”

(Jansen, 2012: 81)

As I explore in Chapter 5, Estonia was one such country that felt it needed to be ‘re-introduced’ to the world, becoming one of the first former Soviet states to ‘rebrand’ itself after regaining independence (see, Jansen 2012; Jordan, 2014; Saunders, 2017). Its story has also gone on to inspire many others, and the Estonian experience of ‘branding the nation’ can now be examined alongside many other studies that have examined the practice in a post-Soviet context (see, Fauve, 2015; Kaneva, 2012; Kaneva and Popescu, 2011; Miazhevich, 2012; Saunders, 2017; Ståhlberg and Bolin, 2016; Zeineddine, 2018). To briefly conclude, as a form of public diplomacy, nation branding is an incredibly useful tool for states seeking to enhance their
image and reputation in new and creative ways. Furthermore, functioning as “a form of geopolitical practice in contemporary world politics” (Browning and Ferraz de Oliveira, 2017: 484), nation branding can also be considered a crucial component of this research as I consider the Data Embassy’s role in facilitating Estonia’s reputation as a digital pioneer and pathfinder in the twenty-first century (see Section 5.3).

2.4 Affective Geopolitics

Affect, Anxiety and Russia’s ‘Near Abroad’

We are increasingly told that we are living in an ‘age of anxiety’ (Hsu, 2019; Lavin, 2019; Mahdawi, 2018) - but what does this mean? At an individual level, it could point to job and economic insecurities that are magnified in an age of automation and austerity (Bassett and Roberts, 2019; Hitchens, 2019), or to ‘algorithmic anxieties’ elicited by creeping technological surveillance and control (Crampton, 2017; de Vries and Schinkel, 2019). Conversely, at a macro-level, global shifts caused by climate change and the recent COVID-19 crisis, or geopolitical events such as Brexit and the election of Donald Trump, have triggered anxieties that are currently being felt or experienced collectively across modern society (see, Hinde, 2019; Keccmanovic, 2020; Ratuva, 2017; Taylor and Murray, 2020). But can anxiety – a powerful emotion and affect often ascribed to many intense phenomena and contemporary conditions – also be something that is experienced beyond the individual body or collective conscience? For instance, in the same way states are often characterised as reckless or ‘angry’ (Hall, 2011) during periods of conflict or crisis, can a state be considered anxious?

In this thesis, I unpack this question in the context of the Estonian Data Embassy and ask whether the state is experiencing a form of collective anxiety (see Chapter 6). In doing so, I contribute to a growing body of literature at the intersection of geography, international relations and psychoanalysis that seeks to engage with affect, anxiety and other emotions in world politics. In particular, I am interested in how anxieties become collectivised and transpersonal, and how they are potentially produced, managed and circulated at a state-level. Drawing on Gerard Toal’s (2017) reading of an affective geopolitics, this section aims to conceptualise Estonia’s anxiety within a wider history and geopolitical context, and how this potentially shapes our reading of the Data Embassy and post-Soviet space.

But first, if we are to consider what kind of affective geopolitics shapes/is shaped by the Data Embassy, then it is important to begin with a brief discussion on what many have termed as an ‘affective turn’ within the social sciences over the past few decades (see, O’Grady, 2018b; Pile, 2009). Geographers have played a central role in this turn, with many seeking a greater understanding of affect, its politics and its intrinsic socio-spatial relationship to our everyday lives (see, Anderson, 2014; Thrift, 2008). Often regarded as a conceptual break from the burgeoning field of emotional geographies (see, for example, Anderson and Smith, 2001; Davidson et al., 2005), the study of affect has been an important vehicle for
geographers to explore elements of the inexpressible and non-representational\(^\text{19}\). Affect, as defined by Toal, is a “largely biological phenomenon that concerns how human bodies register sensations in pre-cognitive and semiconscious ways” and encompasses the “vast substratum of thinking that is automatic and unconscious, below or barely at the level of consciousness” (2017: 45). As political geographer Ben Anderson demonstrates, once mobilised, affect can be considered a powerful register for describing a plethora of phenomena and embodied experiences that are considered part of everyday life:

“background moods such as depression, moments of intense and focused involvement such as euphoria, immediate visceral responses of shame or hate, shared atmospheres of hope and panic, eruptions of passion, lifelong dedications of love, fleeting feelings of boredom, societal moods such as anxiety or fear, neurological bodily transitions such as a feeling of aliveness, waves of feeling...amongst much else.”

(Anderson, 2014: 5)

Of relevance to this research, the study of affect has also provided geographers the opportunity to attend to the ‘collective condition’ or shared, collective moods that can ‘envelop’ and ‘press’ upon life itself (Anderson, 2009). In recent years, a growing number of scholars have turned to the notion of affective atmospheres as a way of identifying particular feelings or emotions that are produced and experienced collectively by both human and nonhuman actors across different spaces and contexts. Esther Hitchen (2019), for example, asks us to consider what kind of paranoid and uncanny atmospheres inhabit spaces of austerity (such as the library), whilst Robert Shaw’s (2014) work examines the ‘vibrating, pulsating atmospheres’ at play in Bristol’s night-time city centre (for other examples, see, Adey, 2014; Anderson, 2009; Ash, 2013; Bissell, 2010; McCormack, 2008).

The study of affective atmospheres has also inspired a growing body of work at the intersection of affect, emotion and nationalism theory (Antonsich et al., 2020; Antonsich and Skey, 2017; Closs Stephens, 2016; Merriman and Jones, 2017). Building on Raymond Williams’ (1977) influential ‘structure of feeling’ concept, Angharad Closs Stephens (2016) explores the ‘happy atmospheres’ and collective togetherness that was registered, experienced and circulated during the London 2012 Olympic Games across the UK. Beyond a simple assertion of ‘everyday nationalism’, Closs Stephens highlights the different intensities of national identity that were experienced and how they congeal around particular bodies or objects (such as the relay torch) throughout the games (ibid). Whilst contributions such as these are critical to the study of politics and affect, it must also be recognised that any attempt to articulate the ‘national mood’ – or register the

\(^\text{19}\) For example, geographers have used affect in studies relating to popular geopolitics and film (Carter and McCormack, 2006; Dodds, 2013), war and conflict (Fregonese, 2017; Laketa, 2016; Toal, 2003), and, more broadly, surveillance and technology (Adey et al., 2013; Ash, 2013).
circulatory affects of nationalism - is by no means a simple endeavour. As I explore further in Chapter 3, this speaks to an epistemological problem at the heart of this thesis, namely: how do you identify a nonhuman actor, such as the state, as being anxious?

In order to get closer to answering this question, and to build on some of the key themes already outlined within this section, it is worth turning our attention to the notion of anxiety itself and how anxiety has been understood historically. Like the aforementioned affective/emotional turn, geography has also witnessed a ‘psychoanalytical turn’ over the past two decades (see, Kapoor, 2018; Kinsbury and Pile, 2014; Philo and Parr, 2003). Building on Sigmund Freud’s (1856-1939) influential thinking and system of thought at the start of the twentieth century, psychoanalysis is fundamentally concerned with the existence and intricate complexities of the dynamic unconscious, and has become central to our understanding of human behaviour (Pile, 2012). Indeed, as geographers have become increasingly fascinated by our mind and body’s very own ‘terrae incognitae’ (Pile, 2012: 9), psychoanalytic theory has become a critical tool for reinterpreting and reconfiguring many “different kinds of geographies” (Rose, 2000: 654).

However, although anxiety is often viewed as a fundamental component of psychoanalysis, it could be argued that it has yet to play a prominent role in geography’s purported psychoanalytical turn - whilst attempts to ‘psychoanalyse’ geopolitics also remain few and far between (Klinke, 2016). In an attempt to address this imbalance, and to further our understanding of how Estonia’s anxiety may be identified and better understood, it is worthwhile turning to work from outside of geography and to focus on studies that have attempted to theorise anxiety and traverse certain anxious histories during particular ‘political moments’ or periods of crisis, such as the Second World War and Cold War (Ffytche and Pick, 2016; Orr, 2006; Radin, 2017; Shapira, 2013; Stonebridge, 1998; 2007). For historian Lyndsey Stonebridge, returning to psychoanalytical texts from these periods may also present something of an opportunity, with psychoanalysis becoming a crucial discourse of representation that “allows us to make the unconscious effects of history visible” (1998: 173). Representation is central is Stonebridge’s thinking, theorising anxiety as a ‘signal’ or an affect with representational charge – one that prepares us for imminent danger (such as aerial bombardment) or a recurring event from the past (1998: 174).

---

20 Notably, the completion of this thesis has coincided with two significant ruptures in Western politics – Brexit and the election of Donald Trump as U.S. president. Unsurprisingly, geographers have paid close attention to the affective implications of these (often polemical) contemporary geopolitical events, in an attempt to understand how these emergent forms of populism are formed, shared and lived as part of our daily lives (see, Anderson and Wilson, 2017; Anderson et al., 2019; Callard, 2016; Fortier, 2017; Gökarıksel and Secor, 2018; Ingram, 2008; Jackson, 2010; Pohl, 2020; Salverda and Hay, 2014).

21 Despite this, the last decade or so has seen a growing body of work that broadly considers anxiety across a range of different geographies (see, for example, Billé, 2014; Callard, 2016; Fortier, 2017; Gökarıksel and Secor, 2018; Ingram, 2008; Jackson, 2010; Pohl, 2020; Salverda and Hay, 2014).

22 Building on a Freudian interpretation of anxiety, Stonebridge notes how we are not simply anxious of the things we know and can identify, rather, anxiety has a “quality of indefiniteness and lack of object” and can thus tell us “the affective history of a life that is not consciously known” (1998: 174). This theoretical interpretation of anxiety is built upon further in Chapter 6, as I make a clear distinction between fear (which is object-oriented) and anxiety (which is object-less) and why this is important in the context of the anxiety I propose that Estonia is experiencing.
Turning briefly to contemporary geopolitical scholarship, Banu Gökarıksel and Anna Secor’s (2018) work on the ‘anxious encounters’ between Turkish citizens and Syrian refugees provides timely insights into the levels of angst and apprehension experienced during the Syrian refugee crisis. They remind us that anxiety, when projected politically, is very much an affect of encounter – in their context, an encounter with the ‘Other’. The notion of the ‘Other’ has played a central role in other studies attempting to theorise anxiety geopolitically, such as Ian Klinke’s (2016) work on geopolitical fantasies in the context of Russian ‘Cyber-brides’ and Franck Bilé’s (2014) examination of anti-Chinese sentiments currently experienced across Mongolia.

In an attempt to broaden our understanding of anxiety in relation to this research on the Data Embassy, it is also worth briefly reflecting on current work that has theorised anxiety in relation to technology, data and the algorithm. As Jeremy Crampton has recently argued, the modern-day algorithmic society – one that is dominated by automation, Big Data and various surveillance technologies – is a society that promises “to make our life better whilst simultaneously producing anxieties” (2017: 1). Indeed, as we live in a world that is increasingly dominated by, and reliant upon, data, algorithms and digital technologies, many of us are increasingly anxious around our ‘data futures’ (Pink et al., 2018): how we experience/live with the deluge of data in our everyday lives, but also the uncertainties associated with data usage/loss in the future (see Section 6.1; see also, de Vries and Schinkel, 2019; Jhaver et al., 2018). This work also speaks to a growing number of studies across disciplines such as geography, digital humanities and critical data studies that focus on anxieties in relation to the use/pervasiveness of Big Data and technological surveillance (Belcher, 2016; Crawford, 2014; Kitchin and Lauriault, 2018; Leszczynski, 2015).

In order to draw together some of the key themes addressed so far, this section concludes by turning to work that has engaged with notions of affect and anxiety in a post-Soviet context. Principally, I draw on Gerard Toal’s research that aims to understand the power of emotion and affect in the conceptualisation and practice of geopolitics in Russia’s near abroad (see, O’Loughlin et al., 2016; Toal, 2017; Toal and Merabishvili, 2019). Central to this is an understanding of affective geopolitics, which can be understood as the study of the forcefulness of emotions – for example, the experience of being angry, the need to condemn, or the sense of being fearful or anxious of another state. Toal’s reading of an affective geopolitics is of relevance to this research, not least for its conceptualisation of emotion/affect at a

---

23 In his work, Bilé illustrates how the spectral presence of the Chinese ‘other’ in Mongolian society – a sense that China is ‘everywhere’ and ‘in everyone’ – has led to a deep mistrust and paranoia amongst many Mongolians, which can be dated to the Soviet era. Such anxieties are omnipresent in Mongolia, and Bilé’s study goes some way in highlighting how anxiety can become transpersonal, collectivised and even embedded within certain structures of society and the state (something I draw upon in my own research – see Chapter 6).
state-level in Russian geopolitics, but also for its understanding of the social, economic and political complexities of post-Soviet space.

Toal’s approach and reading of post-Soviet space draws on two specific aspects. The first considers how certain individuals and groups “tacitly understand and acquire deep-seated dispositions about the territory of the state they live in and those that surround it” (2017: 46). Referencing the role Russia’s geographical size and extent plays in its own ontological security and the certain reassurances this offers, Toal compares Russia’s experience of security to Israel, “whose size, and dominant perception of being surrounded by enemies perpetuates an already visceral sense of existential threat” (ibid). As I highlighted in the previous chapter, I draw on a similar Estonian disposition in the context of this research, where Estonia’s ‘smallness’ (Abulof, 2009) and proximity to its much larger neighbour equally plays on the state’s own existential insecurities. The second considers how affective geopolitics “conditions and shapes the leadership styles and foreign policy decisions of key players in post-Soviet space” (2017: 47). In reference to the distinct hegemonic masculinities that are exhibited, performed and perpetuated by leaders such as Putin, George W. Bush and Mikheil Saakashvili, Toal notes the importance that heroic personalities and storylines play in the geopolitics of Russia’s near abroad.

In his work, Toal (2017) develops a distinctive theoretical framework based around three core categories: geopolitical fields, geopolitical cultures and geopolitical conditions. In this thesis I am particularly interested in the notion of ‘geopolitical culture’. According to Toal, a geopolitical culture is:

“[F]irst and foremost about the identity of a territorial entity and the locational narrative it presents to itself and the world. Its specification involves boundaries of identity and difference, the broad civilizational realm within which it positions itself, the states it views as friends, and those it differentiates itself from and defines itself against. A geopolitical culture, in other words, is made up of a series of geographical imaginations about self and other in the world. A geopolitical culture is also about security and defense, about whom the territorial entity holds to be its enemies and the strategies it deems necessary to preserve its existence, identity, and capacity for maneuver.”

(Toal, 2017: 39)

---

24 Toal’s work speaks to other work within political geography and international relations that broadly considers the notion of ‘affective geopolities’, including studies that focus on political instability and conflict (Fregonese, 2017; Gökarıksel and Secor, 2018; Laketa, 2016; 2019; Szkola, 2020) but also work that conceptualises affect through an everyday geopolitics (Bialasiewicz and Sariaslan, 2020; Howell and Sundberg, 2015; Moïsi, 2010; Pain and Smith, 2008).
In this thesis, I’m interested in how the notion of geopolitical culture can be applied in an Estonian context, and as a tool for understanding the state’s relationship to Russia and how, as a small state, Estonia sees and positions itself within a wider international system (see Chapter 4).

In his book *Near Abroad* (2017), Toal bluntly asks the reader: ‘Why Does Russia Invade Its Neighbors?’. Whilst this intentional provocation requires greater unpacking, it is a question that speaks to a growing political discourse and commentary regarding Russia and the complex geopolitics of its near abroad (see, for example, Clowes, 2011; Forsberg and Mäkinen, 2019; Giles, 2019; Grigas, 2016; Naylor, 2020; Sakwa, 2017). Predominantly focussing on the circumstances surrounding Russia’s invasion of Georgia in 2008 or annexation of Ukraine in 2014, much of the analysis is centred on issues around post-Soviet identity and the impact of ‘frozen conflicts’ in regions such as Abkhazia and South Ossetia, as well as the territorial ambitions of a ‘revanchist’ imperial Russia in the midst of a so-called ‘New Cold War’. Toal, however, argues that many accounts of Russia’s behaviour in relation to its near abroad have been insufficient until now, in that they provide ‘thin’ (and often uncritical) geopolitical accounts that simply ‘flatten’ the many spatial complexities and affective relations that characterise Russian/post-Soviet geopolitics. Rejecting the often-superficial regional representations and dichotomies that are embedded in Western geopolitical discourse (e.g. empire vs freedom, democracy vs authoritarianism, Russia vs the West), Toal calls for scholars to draw on a much ‘thicker’ account of geopolitics that instead recognises “the importance of spatial relationships and in-depth knowledge of places and people” and is thus “grounded in the messy heterogeneity of the world” (2017: 279). Such an approach is of relevance in the context of this research, as I aim to develop a greater understanding of the complex networks, actors and affective forces that make up the Data Embassy assemblage. To augment this approach further, in this thesis I also draw extensively from scholars that are writing on issues relating to post-Soviet space, territory/territorial disputes, boundaries/borders, identity and collective memory from an Estonian, Baltic and Nordic perspective (see, for example, Aalto, 2003; Berg, 2000; Kuus, 2002; Mälksoo, 2000; Tamm, 2013). Such an approach, I believe, is crucial in order to engage with those voices and perspectives that have a critical understanding and knowledge of Estonian/post-Soviet space and geopolitics - and of whom often draw on their own personal experiences, emotions and memories in their writings.

### 2.5 Conclusion

This chapter has examined the various (im)material components and complexities that make up the Data Embassy assemblage - from the ethereal cloud that is actualised inside the shadowy, monolithic structure of the data centre, to the everyday anxieties and affective geopolitics that necessitate the Data Embassy’s establishment. In doing so, I have drawn together some of the key themes, questions and bodies of research that speak to the Data Embassy and the overall direction of this thesis. The themes addressed in this chapter
– whilst not claiming to be exhaustive – serve as my own initial reflections on, and exploration into, the Data Embassy itself, drawing together a number of interdisciplinary debates from across areas of political geography, cybersecurity and diplomatic studies. From ongoing challenges around data sovereignty/localisation to the political legitimacy of states (and non-state actors) in an increasingly uncertain world, this chapter has situated the Data Embassy within a number of cross-cutting themes and debates that reflect the potential impact of the initiative upon the changing nature of statehood, statecraft and diplomacy in a digital age.

Turning to a growing body of research that attends to the material politics of the Internet and the global infrastructures that sustain and govern the spaces of everyday life, Section 2.1 focussed on the geopolitical infrastructures that help shape and facilitate the Data Embassy. From the colonial/Cold War histories of subterranean Internet cabling routes to the emerging significance of data centres and the (im)materiality of data as they traverse the globe, I examined how such work has played a critical role in revealing the often ‘invisible’ infrastructures of our increasingly digitalised world, whilst also playing a fundamental role in the operation and function of the Data Embassy itself. Such infrastructures are foregrounded throughout the remainder of this thesis, as the inner mechanics of the Data Embassy are introduced (see Chapter 4), the motivations behind its establishment are critiqued (see Chapter 5), and the legal and diplomatic implications of extraterritorial data storage are further scrutinised (see Chapter 7).

In Section 2.2, I considered the ways in which the Data Embassy may recalibrate many long-held assumptions regarding the future of statehood, examining the initiative in the context of wider debates around the role and function of the state. Situating the Data Embassy alongside work that characterises the state as ‘improvised’ (Jeffrey, 2013), ‘exiled’ (McConnell, 2009) or ‘digitalised’/’virtual’ (Pistor, 2020), I suggest that the initiative can be best understood in the context of an anomalous geopolitical space and entity where “international norms and ideals of statehood” are increasingly being “called into question” (Jeffrey et al., 2015: 180). Such work theoretically underpins many of the arguments made later in this thesis, particularly around the anticipatory logics of the state (see Chapter 6), and whether the practice and performance of ‘hibernating’ the state and establishing a Data Embassy can be regarded as an attempt at conveying political legitimacy in the event of an emergency (see Chapter 7).

Similarly, Section 2.3 considered what impact the Data Embassy may have on the future practice of diplomacy. Situating the initiative within a growing body of work around the changing nature of diplomacy – from research on virtual embassies and digital forms of diplomacy, to alternative/unofficial forms of diplomacy that operate at the margins of political life – I argue that the Data Embassy is now a crucial site

---

25 Indeed, the concept of the Data Embassy touches upon a number of cross-cutting themes and interdisciplinary debates, from theoretical conceptualisations of territory/territoriality and sovereignty in the social sciences (see, for example, Elden, 2006), to notions of disaster recovery planning in IT risk management (Fallara, 2004) and secret sharing mechanisms in information security (Ermakova, 2013).
of inquiry for future diplomatic studies, with the potential diplomatic and legal ramifications of extraterritorial data storage and the Data Embassy discussed later in this thesis (see Chapter 7).

Finally, Section 2.4 engaged with growing scholarly interest in how emotions and affects are identified and understood at a collective and political level, attending to one of the central questions in this thesis (see Chapter 6): is Estonia experiencing a form of collective, state-level anxiety? Following an overview of both the affective and psychoanalytical ‘turns’ experienced in geography and the social sciences more broadly, my focus turned to anxiety itself and how the term has been theorised historically. Building on this, I wanted to see how anxiety and other affects can be contextualised within broader historical and geopolitical contexts. Engaging with Toal’s (2017) reading of an affective geopolitics, I explored how powerful emotions and affects play a critical role in the conceptualisation and practice of geopolitics in Russia’s ‘near abroad’, and how these shape our understanding of the Data Embassy and post-Soviet space today. In order to develop a greater understanding of the complex “material circulations” (Dittmer, 2017) and affective forces that make up the Data Embassy assemblage, I also pointed to critical work in the post-Soviet/Baltic geopolitical space, where ongoing research on territory, national identity and collective memory play a crucial role in the argumentation made throughout the remainder of this thesis.
Figure 3.1 - The Office of the President of the Republic of Estonia, located in Kadriorg park on the outskirts of Tallinn (author’s own image)
Chapter 3 – Researching the Data Embassy
On a cold and brisk October morning in 2018, I found myself in the picturesque grounds of Kadriorg park: home to the office of Estonian President Kersti Kaljulaid (see Fig. 3.1). Although this wouldn’t turn out to be a meeting with the president (instead, I would be meeting with a strategic advisor), it was an opportune moment to take stock and reflect on the journey I had taken so far throughout my doctoral research. I was halfway through my third visit to Tallinn, spending time as a visiting PhD researcher at Tallinn University of Technology (TTÜ). Over the course of conducting this research, a valuable web of contacts gradually formed, providing me with access to a wide range of government officials, gatekeepers and both industry and academic expositors.

My time ‘in the field’ would lead me to international conferences on e-ID and cybersecurity, a solo sojourn to Narva on the Estonian-Russian border (see Fig. 6.1), and more informal conversations in coffee shops, bars and restaurants. I would sit directly behind the Estonian prime minister as he was addressing dignitaries at the Tallinn Digital Summit (see Fig. 4.1), whilst spending an evening drinking and dancing (‘networking’) with those tasked with keeping the ‘e-Estonia’ brand shining even brighter in the future. I would also find myself feeling isolated as the inexperienced PhD researcher amongst a whole host of Estonian tech experts and evangelists, and even more uneasy at the thought of presenting my research to a group of Estonian academics - many of whom had decades of experience across the public sector and beyond.

Perhaps the most unique aspect of researching the Estonian Data Embassy is Estonia itself, where, due to its size, a fluid nexus exists (and arguably flourishes) across the public sector, industry and academia. During the aforementioned meeting at the Office of the President, the advisor took a brief glance at my colour-coded interview and contact list - he knew nearly every name listed and made countless suggestions of others that I should contact during my time in Tallinn. This was by no means a one-off. I would often find myself introduced to former colleagues or ‘old school friends’ without hesitation – many of whom I had already planned to connect with.

As this chapter will explore in greater detail, there are many pros and cons to the unique ecosystem within which I have been conducting this research. The embodied encounters that were experienced as a researcher would prove incredibly rich and beneficial – not simply through the data collected in recorded interviews and conversations, but more often than not through the banal, everyday experiences across numerous research sites and contexts. Equally, navigating such a close-knit environment as a researcher would be fraught with countless setbacks and personal anxieties over relationships, whilst routinely encountering government one-liners from one interviewee to the next.

---

1 After an initial scoping visit in August 2017 (1 week), I spent 3 weeks in Tallinn during May-June 2018. From September to December 2018, I spent 3-4 months as a visiting PhD researcher at the Ragnar Nurkse Department of Innovation and Governance at Tallinn University of Technology (TTÜ). In July 2019, I spent one more week in Tallinn to conduct final interviews relating to this research.
In this thesis, I explore the geopolitical, diplomatic and legal implications of extraterritorial data storage in the context of an emergency. Focussing specifically on the Estonian Data Embassy, I aim to uncover what underpins the Estonian government’s decision to begin extraterritorially backing up its state data and information systems outside of its own borders (see Chapter 5). In doing so, I’m also interested in understanding what such motivations reveal about the Estonian state – from its performative practices, to an everyday security discourse that centres on Russia and other existential threats – and argue that a pervasive anxiety exists at its centre (see Chapter 6). But how, as this chapter attempts to explore, do we research something as novel and complex as the Data Embassy? Equally challenging, how do we identify and register a whole state as being anxious?

In this chapter, I will outline the design and methodological approach adopted for this research. In doing so, and by taking a somewhat reflexive approach in the process, I will also reflect on the numerous successes, barriers and challenges that have come to shape, accompany and sometimes alter the research design employed. Remaining mindful of the many potential pitfalls that can befall a researcher during the process of conducting academic research, I reflect on moments where I was forced to revise my strategy and approach in the field and adapt to any unforeseen circumstances that were met along the way.

In Section 3.1, I return to the epistemological dilemma mentioned above: can we theorise a collective entity, such as the state, as being anxious? Forming an ongoing concern of my own during the course of this research, I build on a growing body of scholarly research that has attended to emotion and affect at a state-level in world politics. Here, I draw upon two methodological approaches that I employ during this thesis that build on encounters with Estonian elites and are attentive to wider discourse around the Data Embassy.

In Section 3.2, I reflect on the numerous embodied encounters that I have experienced during the course of completing this thesis and aim to situate the Data Embassy within the wider practices and performances of the state. Drawing on two key ethnographic studies from Alison Mountz (2007) and Merje Kuus (2014), I outline the benefits of employing ethnographic methods in a state and elite context, whilst making the case for ‘studying up’ in the context of Estonia and the Data Embassy. Furthermore, drawing on my experiences of interacting and conducting interviews with Estonian elites and other relevant respondents, I reflect on how access was obtained (and sometimes stifled) before concluding with some thoughts on my approach to interviewing.

In Section 3.3, I turn my attention to the discourse that has surrounded the Data Embassy since its inception.
in 2013. From exaggerated international news coverage to a lack of analytical scrutiny from outside of the Data Embassy’s ‘inner’ circle, I reflect on how my own journey researching the Data Embassy has coincided with countless other narratives and affectively loaded discourses relating to geopolitics, cybersecurity and international law.

The chapter concludes by offering something of a departure from traditional methodological considerations. With Harrowell et al. (2017) recently calling for greater acknowledgement of, and engagement with, failure within fieldwork and research, Section 3.4 grapples with this very prospect throughout my own research journey. The Data Embassy, by its very nature, remains a precarious research endeavour, with both the initiative and my own research contingent on a number of externalities outside of my control. In calling for a greater discussion around the precarity of our research, particularly within the demands of a postgraduate setting, this section engages and attempts to tackle the many roadblocks and uncertainties faced throughout the process of completing doctoral research.

3.1 Researching emotion, affect and the anxious state

Can a state feel or experience an emotion? Some might point to the ‘national mood’ or collective sentiments of a population as an example of feeling like a state2 (see, for example, Closs Stephens, 2016; Mercer, 2014). However, is it possible for the state to collectively feel an emotion or affect in the same way? As Jonathan Mercer (2014) suggests, a person can feel like a state, but a state cannot feel like a person. For some time, scholars have simply viewed the state as something of a disembodied, monolithic institutional actor that is “ontologically incapable of having feelings” (Digeser, 2009: 327). Its lack of biological function, or ‘body’, thus suggests that the state is unable to experience individual emotions directly (Hutchinson and Bleiker, 2014; Mercer, 2014). How then, as this section explores, are we to theorise the state as an emotional and affective actor?

In terms of my own research, such a question speaks to a much deeper epistemological problem I have encountered throughout the completion of this thesis, as I contend that Estonia is experiencing a collective, state-level anxiety in relation to the Data Embassy (see Chapter 6). Put simply, can and (if so) how do we begin to theorise a collective entity, such as the state, as being anxious? Such a dilemma was raised to me during one particular interview:

---

2 The notion of feeling like a state is borrowed from James C. Scott’s influential work, Seeing Like a State (1998). A critique of ‘high modernism’, Scott writes about the way in which states have attempted (and often failed) to impose certain strategies, systems and controls – such as census data and uniform languages – in an effort to make a society more legible. It was a way in which a state could impose its authority and legitimacy over a population. To feel like a state, however, refers to the group-level emotions that a particular group or population may experience - Jonathan Mercer points to feeling shame or pride in one’s state as one such an example (2014: 515). We might also think of other national events, such as Brexit, and the way such events have invoked a plethora of emotions and collective feelings, as an example of feeling like a state; from a sense of joy, pride and expectation on one side, to a sense of fear, shame and anger on the other (Closs Stephens, 2019).
“So, if you wanted to prove anxiety [...] you would have to dig into the psychological profile of members of the government, or something like that [...] There is no easy way to demonstrate academically that this is an anxiety, as opposed to a rational calculus.”

(interview 10 - 31/05/18)

Such a contention is valid in that, empirically at least, demonstrating or measuring the emotional or affective state of the state is by no means an easy task. Without performing a wholesale psychological profile of government officials and subsequent psychoanalysis of the state’s apparatus, how would I be able to locate and identify (with any given certainty) such an anxiety at the heart of the state?

In this section, I introduce my methodological approach that aims to tackle this epistemological dilemma. First, I situate this problem within a growing body of scholarly work that aims to identify and theorise emotion and affect at a collective and political level, before introducing two methodological approaches that are based around Data Embassy discourse and my own ethnographic encounters in the field (these two approaches are then discussed further in Sections 3.2 and 3.3).

In this thesis I build on recent emotional and affective ‘turns’ across the social sciences that seek to make sense of and attend to a wide range of individual and collective “traditional and non-traditional political phenomena” (Hutchinson and Bleiker, 2014: 492 – see, also, Crawford, 2000; Hutchinson, 2016; Hutchinson and Bleiker, 2017; Koschut, 2017; 2020; Mercer, 2010; Moïsi, 2010; Pain and Smith, 2008; Ross, 2014). In particular, I draw upon Emma Hutchinson and Roland Bleiker’s work that has proved instrumental in developing a theoretical and methodological approach to studying emotion in world politics. Crucially, they ask: how do individual emotions – such as fear, boredom or embarrassment - become collectivised and political? For if emotions are to play an intrinsic part in global politics, they imply, then they must attend to some form of collective condition (Hutchinson and Bleiker, 2014). Their timely intervention in the study of emotion and world politics can also be drawn alongside similar developments in the study of affect, where scholars have sought to identify and make sense of the collective affective phenomena and elements of the inexpressible, non-representational, and embodied experiences found in everyday life (see, for example, Anderson, 2014; Closs Stephens, 2016; Hitchen, 2019).

In order to identify and examine the processes whereby individual emotions become collective and political, Hutchinson and Bleiker (2014) propose adopting a theoretical framework and approach at both a macro and micro distinction. At a macrolevel, this aims to develop “generalizable theoretical propositions about the emergence, nature, function, or impact of political emotions”, whilst a micro approach focusses on how
certain emotions function and “gain resonance” in particular political circumstances (2014: 493). By bringing both together, Hutchinson and Bleiker’s aim is to detect certain “commonalities” in how emotions link to people and political phenomena across a number of spatio-temporal dimensions (ibid).

Such an approach joins a growing number of studies, of relevance to this research, that have attempted to identify and examine emotion and affect at the level of the state (Eznack 2011; Linklater, 2014; Löwenheim and Heimann 2008; Mercer, 2010; 2014; Nugent, 2019; Sasley, 2011; Toal, 2017). Jonathan Mercer (2014) and Brent Sasley’s (2011) work is of particular importance here, as they develop thinking around group-level emotion and how this can lead to feeling like a state (see, also, Nugent 2019). For Mercer, group-level emotions are stronger than those experienced as an individual, stating how group members often “share, validate, and police each others’ feelings” (2014: 530). Emotions felt at both the level of a group and state can be powerful and pervasive, argues Mercer, and given their emergent properties cannot simply be “reduced to the individual experience of emotion” (2014: 516).

Their work on state-level emotion is an important contribution as it goes beyond the somewhat one-dimensional vision of a state as an individual actor – or, indeed, person (Wendt, 2004) - and instead as a group whereby its key members’ (e.g. the decision makers) “cognitive and emotional practices represent, comprise, and reflect that of the group (state) and so determine how the state will act” (Sasley, 2011: 454). As Hutchinson and Bleiker conclude, the state may therefore experience emotions “insofar that the state is essentially a group constituted by individuals that cultivate, share, and identify with each other emotionally” (2014: 500).

Yet, is this still applicable to every emotion and affective phenomena? As I highlighted in Chapter 2, my analysis of Estonia’s state-level anxiety is complicated even further by the notion that anxiety, at least from a Freudian perspective, is so often viewed through an individualistic lens. In the remainder of this section, I point to two approaches that attempt to identify Estonia’s anxiety at a collective level.

The first approach builds on the embodied, ethnographic encounters I experienced during the course of completing this research (see Section 3.2). Here, I take inspiration from David Nugent’s (2019) compelling study on delusion and paranoia at the heart of the Peruvian state during the 1930s (see Section 1.3). Whilst his analysis provides a crucial addition to the study of state formation and the collective affective phenomena that besieged the state during a particular period of political turmoil, Nugent’s epistemological and methodological approach also teaches us a great deal about the study of emotion and affect across a number of spatio-temporalities. Adopting an approach similar to Nugent’s, in this thesis I am making no claims about the “inner feelings” (2019: 249) and personal concerns of Estonian government officials – nor am I attempting to ‘dig’ into the individual psychological profiles of members of government, as criticised above. Rather, my intention here is to draw on the knowledge and expertise of those on the inside and
outside of government in order to understand the political motivations behind the decision to adopt the Data Embassy, and how these fit within the wider practices and performances of the state and its elite.

In other words, my analysis is concerned with how Estonian government officials – and those perhaps more critical at the margins – collectively “acted and communicated” (2019: 249) their message around the Data Embassy, rather than how they felt individually. A limitation to such an approach may be that certain narratives or discourses are purposively enacted and communicated by certain individuals. This could mean that a potentially warped projection of the state would be rendered visible through methods such as the aforementioned government ‘one-liner’⁵. As Section 3.2 explores, however, I attempt to mitigate this by speaking to those outside of the Data Embassy/government bubble in order to add empirical depth to this study. Furthermore, I would also gain a better understanding of the inner workings of state apparatus and how both the Data Embassy and Estonia were portrayed from numerous experiences at conferences and events during my time in the field.

The second approach, whilst augmenting the first, turns to recent attempts at interpreting and contextualising emotion and affect through discourse (Hutchinson and Bleiker, 2017; Koschut, 2017; 2020; Müller, 2013; Toal, 2003; Wahl-Jorgensen, 2019). In this approach, I adopt what Gerard Toal refers to as an ‘affect-attentive’ discourse analysis in order to examine the way in which anxiety may be present or indeed intensified by discourse around the Estonian Data Embassy and wider practices of the state (Gerard Toal, 2017). Simon Koschut’s call for engaging with a ‘discourse-emotion nexus’ is also of relevance here, driving our understanding of how discourse “evokes, reveals and engages” emotion and affect in world politics (2017: 482).

Koschut’s work develops a framework and dual strategy that identifies certain emotional/affective registers within political discourse and world politics. Building on Hutchinson and Bleiker’s (2014) micro/macro framework, this is first introduced by interpreting emotions at more of a microlevel through the use of emotional terms, connotations, or evocative metaphors and analogies. In this thesis I am particularly interested in the affectively “loaded” (Koschut, 2017: 483) discourse that the Estonian government and media have conveyed explicitly in relation to the Data Embassy. The use of evocative language and certain emotionally charged discourse – referring to a ‘country without borders’, or indicating the potential loss of territory

---

⁵ Here, I refer to the way in which members of the Estonian elite (e.g. policymakers, politicians and even those in industry positions) would often prophesise about the state, regurgitating popular mantras or statistics relating to Estonia’s journey post-independence and its digital society today. Examples would include reference to Estonia’s lack of wealth and resource in the aftermath of independence (in comparison to its relative success and prosperity twenty-five/thirty years later) and how this therefore promoted the state to pursue more frugal and innovative forms of policymaking in the 1990s, whilst more banal accounts might highlight how Estonians can file their tax returns digitally and in a matter of minutes (see Chapter 4). Such discourse has equally crept into journalistic accounts of Estonia’s digital society, where similar ‘one-liners’ are regurgitated by journalists who have been captivated by this message and ‘story’ (see, Heath, 2019; Heller, 2017; Reynolds, 2016). I discuss the role and effects of the state’s branded messaging efforts later in this thesis (see Section 5.3).
Koschut’s second strategy moves beyond discursive interpretations within discourse, instead to a macrolevel by contextualising emotional meaning across a variety of discourses and how they are registered and understood by particular audiences. Here, Koschut draws on notions of emotional aethering, intertextuality and performativity, referring to the way in which certain collective feelings are projected onto others, and how emotions (e.g. shame or humiliation) can resonate from certain events and be tied back to previous affective experiences or temporalities. These particular themes are of relevance to this research in the context of Estonia’s relationship to Russia, where an emotionally evocative security discourse continues to shape the Russian threat as part of the state’s cultural and political memory (discussed further in Chapters 5 and 6).

This section has outlined the methodological approach taken in this thesis that attempts to identify and examine the anxiety I believe is at the heart of the Estonian state (see Chapter 6). Recognising that identifying and locating Estonia’s anxiety is by no means an easy task, I have drawn upon key methodological and epistemological approaches that attend to emotions and affective political constructs at a collective level in world politics. In the subsequent sections, I build on these approaches in more detail as I reflect on the embodied ethnographic encounters and Data Embassy discourse experienced during the course of writing this thesis.

3.2 Embodied Estonian Encounters: elites, experts, networks
In this section, I reflect upon the many embodied ethnographic encounters I experienced whilst researching the Estonian Data Embassy and what this may have ‘masked’ (Abrams, 1988) or revealed about the state’s everyday practices and performances. In particular, I draw upon two key ethnographic studies in political geography that have shone a light on the usually opaque practice and discourse of the state.

First, building on Alison Mountz’s compelling doctoral research inside the Canadian government, I demonstrate the advantages of operating ethnographically in and around the confines of the state and its elite, and how this helps to reveal the “contingent, contextual, dynamic, and performative practices of the state” (2007: 39). I equally draw inspiration from Merje Kuus’ rich ethnographic accounts from the very heart of the European Union’s policy-making machine, where expert knowledge production, political expertise and individual and collective agency continue to shape a unique and ever-transforming geopolitical landscape (2013; 2014; 2016; 2018). Unlike Mountz and Kuus’ experience in Vancouver and Brussels, however, I would not be operating ethnographically solely from the centre of Estonian policy-making and diplomacy. Rather, as this section explores, I adopted a more flexible position that allowed me to engage—

Koschut also reflects here on the lexical and semantic variations in certain terms among different languages, cultures and contexts, and how researchers should be cognisant of the fact that some emotions can be “lost in translation” (2017: 483). This became clear during my own research through the use of the term anxiety in an Estonian context (see Section 6.3).
with those not only considered ‘elites’ within Estonian political discourse, but also those who were perhaps more critical towards its margins.

In this research, I draw on almost three years of ethnographic encounters and engagements with civil servants, cybersecurity experts and academic expositors – predominately in Estonia, but sometimes further afield⁵. Often, these took the form of the traditional sit-down interview, but also the form of chance encounters at an international conference or university seminar. As this section details, this would not always result in access to those in the highest positions of authority (e.g. Prime Ministers or Presidents), but instead allowed me to build a steady network of trusted gatekeepers and respondents from across a variety of fields and expertise. Nonetheless, such an approach (in the relatively small vacuum that exists within Estonia) would still prove fruitful for my endeavours, as I found myself privy to the many goings-on amidst numerous political ‘moments’ throughout the process of conducting this research (see Section 3.4).

In this section, I first discuss the merits of institutionally ‘studying up’ and performing a state-level ethnography (Section 3.2.1), before reflecting on the challenges found research those who are considered ‘elites’ within Estonian political discourse (Section 3.2.2). Here, I draw on some of the difficulties faced in maintaining access and the perpetual mobility of government officials during the course of writing this thesis. Finally, I offer some thoughts on my approach to interviewing and how adopting a reflexive approach throughout enabled me to adapt to changes in both the direction and content of my research (Section 3.2.3).

3.2.1 ‘Studying up’: ethnography and the state
To gain a deeper understanding of the inner workings of the Data Embassy, it became advantageous to spend time with and speak to those at the very heart of the initiative. To critically engage with those considered part of the Estonian elite – the statesperson, civil servant or government insider – would allow for this research to best address the conceptual phenomena that surround the Data Embassy. Such an approach builds on a growing recognition of ‘studying up’ from within political institutions and elite environments in order to better understand how they shape and structure daily life (Bilo and Mountz, 2016 – see, also, Kuus, 2014). Often considered a form of institutional ethnography, the process of ‘studying up’ within challenging bureaucratic environments such as the state can provide “a more nuanced rendition of

---

⁵ Many of my interviews took place in Tallinn, Estonia, but I was also fortunate to conduct interviews in Tartu (Estonia), London (UK) and Melbourne (Australia), with further discussions over Skype or email with a number of respondents (see Section 3.2.3 for a more detailed discussion).

⁶ Historically, ethnographic research has been predisposed in favour of the powerful studying the powerless – a process often labelled as studying down. In her influential 1969 essay, “Up the Anthropologist – Perspectives Gained from Studying Up”, Laura Nader (1969) called for a total redress and “reinvention” of the study of anthropology: to study up. What if, as Nader suggests, anthropologists were to “study the colonizers rather than the colonized, the culture of power rather than the culture of the powerless, the culture of affluence rather than the culture of poverty?” (1969: 290). A call to recast our ethnographic gaze towards those in power or with great influence – the politician, policymaker or CEO – the process of studying up has since proven incredibly influential across social science research (see, Aguiar and Schneider, 2012; Bilo and Mountz, 2016; Kuus, 2014; Mountz, 2007).
state practices by seeking to understand and locate the operation of power in the daily work done by civil servants” (Mountz, 2004: 326).

In this research, and in the context of the Data Embassy, I am particularly interested in how the Estonian state functions as a ‘daily entity’ and how the state is enrolled and ‘performed’ by an array of institutional actors across particular networks and discourses (Mountz, 2007). Yet, it is also widely acknowledged that accessing the state and other powerful institutions ethnographically is a complex and challenging endeavour (see, Aguiar and Schneider, 2012; Kuus, 2013; Mountz, 2004). As the following section goes on to show, my own attempt at performing an ethnography of the state (see, Gupta, 1995; Mountz, 2007; Yang, 2005) proved difficult, with my research design relying instead on interviews and the analysis of key texts and wider media discourse. Recognising how most ‘ethnographies’ in political geography and IR are constructed on a mix of interviews, discourse analysis and ‘some’ ethnographic observation, Merje Kuus has challenged the “viability and necessity” (2013: 116) of ethnography in a foreign policy setting, suggesting it can create “the illusion of access and engagement that hinders rather than helps” (2013: 127) the process of ‘studying up’. Nevertheless, through the deployment of various ethnographic methods – such as participant observation – this section outlines my own approach at ‘studying up’ in an Estonian context, embodied through my own interactions with the state - from conversations with civil servants and Data Embassy practitioners, to the more banal, everyday interactions experienced during my time researching the Data Embassy.

Initially, my ethnographic exploration into the Data Embassy and Estonian state would result in me attempting to gain access and embed myself as a researcher within the Data Embassy team. Supplementary to the more traditional interview approach, my intention was to spend a period of time (1-3 months) integrated as part of the team in the Ministry of Economic Affairs and Communications (MoEAC). Such an approach, alongside the development of the Data Embassy itself, would provide unparalleled access and insight into the day-to-day workings of the project, but would also go some way in revealing some of the everyday bureaucratic practices of the state. Lorraine Kaljund was granted similar access when she spent nine months engaging with “the Estonian engineers, lawyers, and cyber security experts” working on bringing the Data Embassy to life in its early stages (2018: 6). During an initial consultation period with the Data Embassy team in early 2018, I was positive that such access would be granted. However, over the course of the year, several roadblocks were faced that ultimately led to access never materialising. It was a tell-tale reminder that access to such elite environments was never a given;

---

7 Such an approach can also be considered in the context of other ethnographic studies based in Estonia (see, Martinez, 2018; Melchior, 2020; Smith and Burch, 2011; Tateo et al., 2018; Viires, 2007).

8 As I highlight later in the chapter, positional changes in government and the Data Embassy team scuppered initial access via gatekeeper contacts (see Sections 3.2.2 and 3.4). For example, after one brief conversation with one gatekeeper's successor it was pointed out that, due to my lack of Estonian language skills, it wouldn't be worthwhile me spending time in the team as meetings were conducted in Estonian. From then on, contact with the team working on the project fizzled out.
and to negotiate and maintain access with those institutions (and individuals), who are notoriously inaccessible to the researcher, can be fraught with unexpected twists and turns.

Forced to adapt slightly, my attention soon turned to what could be learned from those on the inside of the state’s apparatus from interviews and ethnographic encounters during my time in the field as a researcher. Explored further in Chapters 4 and 5, Estonia’s role as ‘pathfinder’, and reputation as digital government pioneer, is well renowned (Drechsler, 2018). This meant that finding those willing to share expertise, their own experiences or push forward its e-government agenda would not be an arduous process. From those public figures who were involved with the Data Embassy project from when it was a mere conceptual blueprint (like former government CIO, Taavi Kotka), to those less visible working tirelessly on bringing the Data Embassy to its actualised potential in Luxembourg, those authoritative voices from ‘inside’ the project would offer a first-hand account of the Data Embassy’s inner mechanics and development alongside my own project.

Yet, it was established from the outset that this alone would not be enough. Recognising that only a very specific knowledge of the state would be projected and ‘performed’ (Mountz, 2007) by those in government (arguably, intentionally), I felt that alternative voices from ‘outside’ the identified Data Embassy circle would provide a rich, empirical depth beyond the potential government ‘one-liner’ and the state’s well-established “perfection narrative” (Drechsler, 2018). Merje Kuus has reflected on this very point from her time in Brussels, highlighting the inherent risk of entrapment inside the “technocratic echo-chamber” of researching in elite policy circles (2011: 126). To avoid effectively becoming a ‘flag waver’ of the Estonian state (something I have had to remain mindful of during previous research in this context), I expanded my networks beyond the civil service and government departments and into industry and academia to offer differing perspectives and critique. These would not take the form of disgruntled government employees with axes to grind. Rather, the expertise and authoritative perspectives of those across cybersecurity think-tanks and academic circles proved just as vital to this story – not just in Estonia, but beyond its borders too. Crucially, I would draw on know-how in cloud computing law, public administration and e-governance, including those in diplomatic circles with whom future Data Embassy locations may also be found.

Furthermore, it would be the ‘small things’ – the “specificities, nuances, and mess-ups” (Kuus, 2014) – that would draw me further into the inner fabric of the state, Data Embassy and wider Estonian milieu. Highlighted above, it soon dawned on me that ‘Access All Areas’ would not be fully granted, and therefore alternative strategies and engagements would prove equally beneficial. By gaining access and attending numerous events and conferences – where the lines between public and private sector often became blurred – I would learn of how the state and ‘e-Estonia’ was being presented (and sometimes prophesied about) to
the wider world. Equally, by spending time as a visiting researcher at a local university, I benefitted from a more prolonged period of time in Estonia, allowing for greater access, reflexivity and scrutiny from across the wider academic community. By immersing myself fully within Estonia for three months, I was able to build greater relationships with key contacts and engage ethnographically at key conferences, events and seminars without much planning or preparation. During this time, I also began to keep a field diary as a way of reflecting on the many events, encounters and explorations experienced during my time in the field – although this stopped after a short period as I felt that other modes of data collection, such as the interview, were far more beneficial to this study.

As I called time on my protracted period of data collection and ethnographic experiences in the field, I felt a sense of familiarity and more attuned to the “daily hum” (Kuus, 2014) of the Estonian political machine and apparatus of the state. Due to the networks created and relationships built, I became acutely aware of the cultural sensitivities that existed between myself as a researcher and the environment I was researching – from discussions around Russia and attitudes to immigration, to Estonian humour and learning to laugh and joke whenever Brexit made conversation (a great ice-breaking topic nonetheless). After being initially drawn to Estonia’s powerful and pervasive nation-branding strategy myself (Jansen, 2012; Mäe, 2017 – see Section 5.3), I felt I also developed a more critical, nuanced perspective of the country over the course of a number of visits. As the remainder of this chapter will show, such a critical perspective became crucial as I encountered different forms of discourse from the state and media relating to the Data Embassy and Estonia more broadly – allowing me, at times, to cut through a great deal of PR hype and hyperbole. Despite not getting the level of access that I had initially hoped for, the various ethnographic encounters described throughout this section still proved beneficial for this research. Indeed, by adopting a more flexible (and somewhat critical) position at its margins, I believe I utilised the expertise and voices of those from across Estonian society (and beyond it) in an effort to build a more rounded and critical perspective on how the Data Embassy was established and brought to life.

3.2.2 Elite today, gone tomorrow…
One of the most striking observations during my time in the field was the merry-go-round nature of the Estonian public sector and its political intelligentsia. Often, between repeated trips to Estonia, I would find interviewees or contacts moving between roles, or moving in and out of government (to either the private sector or academia), in what can only be described as a constant movement of the researcher’s goalposts. Merje Kuus (2013) reflects on this challenge from during her own ethnographic experiences in an EU foreign policy setting, where forging relationships with elites became ever more complex in an environment

---

9 Notable events included: *Latitude 59*, an international startup and technology event (May 2018); *CyCon*, an international cybersecurity conference (May 2018); *eID Forum*, an international conference that focusses on digital identity (September 2018); *Tallinn Digital Summit*, an international conference that focusses on global perspectives regarding digital transformation (October 2018).

10 Nevertheless, a number of chapter prefaces in this thesis include short diary excerpts and reflections from the field, accompanying an image from a particular fieldwork site. Each fieldwork ‘snapshot’ is intended to reflect upon a particular theme relating to a given chapter, such as an interview encounter at the Office of the President in Kadriorg park (see Chapter 3), attendance at the Tallinn Digital Summit (see Chapter 4) and a visit to the city of Narva on the Russian border (see Chapter 6).
that is in a constant state of flux. As much as it is important to get initial access and a foot in the door, writes Kuus, elite engagements equally involve the painstaking process of maintaining relationships “beyond the initial encounter” (2013: 119). This fluidity experienced within Estonia was by no means unique, but, as the thesis developed, often led to communication breakdowns and thus the continual renegotiation of access within an ever-changing research environment. As this section aims to explore in greater detail, how can we as researchers navigate the complex, pressured and sometimes unforgiving process of interviewing those within elite circles?

In recent years, there has been a growing interest in examining the many processes and issues relating to gaining access to and interviewing ‘elites’ across a number of different contexts and scales (Aguiar and Schneider, 2012; Harvey, 2011; Herod, 1999; Ostrander, 1993; Richards, 1996; Rice, 2010). These have included studies that have aimed to shine new light on the agency and practice of politicians and policymakers in government (Lancaster, 2017; Neal and McLaughlin, 2009), to investigations into elite practices at more of a local scale (Cochrane, 1998; Ward and Jones, 1999; Woods, 1998). Defining the notion of an elite can be problematic in itself, due, in part, to the subjectiveness and general connotations it can provoke. As Hughes and Cormode argue, it is nonetheless the case that elites in powerful and influential institutions are often “key research subjects in studies which aim to engage critically with the changing character of cultural, economic, and political worlds” (1998: 2098).

Conducting research on elites also raises a number of methodological questions, from practical demands relating to access to issues around researcher positionality and status. As Section 3.2.1 illuminated, gaining access to the Data Embassy and its team was by no means a simple process. As my time in the field progressed, I would also encounter a sense of reluctance from potential respondents to be interviewed – some not believing they had the right knowledge or expertise to help, whilst others were simply unable to commit due to busy work schedules. Susan Ostrander (1993) has critiqued the exaggerated notion that gaining access and studying elites is a somewhat difficult and onerous process (see also Kuus, 2013). For Ostrander, there is a degree of luck involved along with a willingness to take advantage of opportunities that come your way. To what extent, then, is access to elite environments simply a matter of luck? Or can it be a case of ‘it’s not what you know, but who you know’ when attempting to infiltrate elite spaces and networks within institutions such as the state? There is no direct and obvious answer to this, as more often than not access can be entirely context dependent on the research and researcher, but also contingent on a whole host of externalities that are sometimes outside of one’s own control (see Section 3.4).

In terms of negotiating access to those close to the Data Embassy and those inside the Estonian government, I was fortunate in that during previous research in Estonia I had already developed a number of contacts and relationships with people who would ultimately serve as gatekeepers over the course of
writing this thesis. Initially, this led to me making contact and setting up interviews with two individuals working on the Data Embassy team. From here, I was then able to begin branching out and contacting individuals from across the civil service, such as the Ministry of Foreign Affairs and Ministry of Justice, in order to gain views and perspectives of those with different expertise, agency and knowledge (Kuus, 2013). Kenneth Goldstein (2002) has made the argument that spending a sustained period of time in the location or environment you are researching can be a vital method for “getting in the door” and establishing interviews with elites: “Elites will often have last minute breaks in their schedules and being on the ground and ready to conduct the interview at a moment’s notice is a huge advantage” (2002: 671). I found this to be true during my time in the field, as I initially faced complications and rejections due to respondents’ tight schedules and my own limitations during shorter visits to Tallinn. During my longer period of stay in Estonia (September-December 2018) this was less problematic and, due to having a foot ‘in the door’, interviews began to snowball.

There was, however, another method and tactic at my disposal that I can describe as ‘open-source access negotiation’. Often, researchers studying elite spaces have difficulties in locating or making initial contact with their respondents due to their perceptibility and the privacy they normally desire (Herod, 1999). Fortunately, in Estonia, this wasn’t the case as nearly all government officials and civil servants have their contact details (name, position, telephone number and email) listed on government portals, whilst other participants were also easily accessible via social media accounts and personal websites. For many researchers who potentially have to rely on months of negotiations with gatekeepers, Estonia’s fairly transparent public sector allowed me to broker initial access in a number of ways prior to visiting Estonia to conduct fieldwork. Whilst this wouldn’t result in a 100% success rate, more often than not I would be copied into an email with a colleague or relevant contact that enabled further discussions to take place.

Andrew Herod (1999) has discussed the inherent qualitative differences found in conducting interviews with foreign elites rather than of one’s own nationality. Particularly problematic are general issues around “transcultural communication and understanding” but also the “cultural positionality of the researcher and thus the presumed validity and meaningfulness of the knowledge they produce” (1999: 313-314). Herod

---

11 To paraphrase a government official during previous research on the Estonian e-Residency programme in 2015, they suggested that they would always look to help those who are interested in their country and government, as ‘you never know when it might come back to help you in the future’. This stuck with me as I found a number of Estonian respondents were incredibly receptive to helping me on my fieldwork journey in its initial stages. There were, of course, exceptions to this rule, but many respondents were keen to introduce me to friends and/or colleagues that could help me. Estonia’s relative size and general fluidity across its public/private sector also helped – at times, it felt like everyone seemed to know everyone (which had both positive and negative consequences).

12 I often faced interview roadblocks on my shorter visits to Estonia (e.g. a week) with respondents often pulling out at short notice and with no further opportunities to reschedule. I also had to learn the hard way after planning my first trip to Tallinn during the 2017 Estonian summer holiday (normally between the months of July and August) and finding that many participants were unavailable. With my flights and accommodation already booked, I used the trip as more of a reconnaissance for future trips. I later received a piece of advice from an Estonian contact that I should never plan ‘more than two weeks in advance with an Estonian’, as their diaries can be incredibly flexible.

13 I found this to be incredibly unique. In comparison, in the UK (whilst objectively more bureaucratic and larger in size), it is incredibly unlikely to find the contact details of a vast number of UK civil servants and ministers so publicly available.
writes of problems encountered around the insider/outsider dichotomy whilst interacting with an array of elites found within trade unions across the world. In terms of positionality, he goes on to discuss the way in which we may often find ourselves as researchers “consciously manipulating one’s own positionality” or how it may naturally change over time (1999: 321). Encountering a number of elites throughout the course of completing this research, these were frequent factors that played into my own position and performance as a researcher. For example, I was undoubtedly perceived as an ‘outsider’ to many participants due to my position as a British researcher in Estonia (compounded by my lack of Estonian language skills), but was equally considered an ‘insider’ by many participants due to my knowledge of the Data Embassy itself. This was a tightrope that I regularly walked, and found myself manipulating my own positionality at different points during this research process. Fortunate in being an interdisciplinary scholar I was also able to transition between identifying as a political geographer and that of a cybersecurity background – with the former being something of an unknown discipline in Estonia, I believe my cybersecurity credentials helped broker access that a political geographer could not14. At other times, I also believe that informing participants that I wasn’t from a ‘technical background’ assisted in eliciting more information or better explanations from interviewees.

3.2.3 Interviewing reflexively
So far in this section I have reflected on the embodied ethnographic encounters I have experienced whilst researching the Data Embassy. Although unfettered access to the Data Embassy and apparatus of the state ultimately did not materialise, the interview remained a key methodological approach and source of data for the subsequent empirical analysis. As Dunn (2016: 102) argues, the interview allows us to fill gaps in knowledge that other methods - such as participant observation or discourse analysis - sometimes cannot achieve. In other words, by interviewing those who had either worked close to the Data Embassy or who rather held a more critical position on its establishment, I was able to elicit data that may have not been obtainable via other methodological approaches.

Over the course of approximately two and a half years of fieldwork, I conducted twenty-eight semi-structured interviews across a range of different sites and locations15. Outlined in Figure 3.2 below, these included a mixture of respondents from across the public and private sector, as well as academia. I also outline the number of respondents I spoke to that were deemed Data Embassy ‘insiders’ (9) compared to ‘outsiders’ (19). Although this disparity may seem to signify a lack of access into the Data Embassy team (see Section 3.2.2), it instead reflects the small number of individuals that have actually played a pivotal role in the development and governance of the Data Embassy itself. Many of those who are deemed ‘outsiders’

---

14 Herod discusses the way in which academic fields and power relations are also inherent factors in researcher positionality, particularly in elite settings, asking, “are potential respondents more or less likely to talk to “geographers” than to “historians” or “economists” or “political scientists” or “sociologists” because of the ways in which these disciplines are perceived as academic fields?” (Herod, 1999: 321).

15 There were more ad-hoc conversations or brief encounters that have not been included here, but I still draw upon these in my research when making general points about the Estonian Data Embassy and state more broadly.
may still reside in the public sector but lacked a key role in the development of the Data Embassy. Demographically speaking, interviewees were also predominantly male (21), whilst the vast majority of respondents were Estonian (22). Although such statistics do not reflect an inherent bias within the sample size – they may, however, hint at gender imbalances within the Estonian public sector - any future research on the Data Embassy and Estonian state would benefit from other gendered voices, as well as perspectives from outside of the wider Estonian milieu (see Appendix B for further details on interview data).

Early on in the process I made a conscious decision to anonymise all of the participants in this study. This decision was in part an effort to make participants feel more relaxed and to allow them to speak more freely about the Data Embassy project and Estonia more broadly. It is well established that the process of anonymising data in research can be something of a balancing act, particularly between maximising participant anonymity and maintaining the integrity of data collected (Saunders et al., 2015). Niamh Moore (2012) notes the many political and ethical considerations required by the researcher, particularly around

---

16 I have classified respondents based on the role they held at the time of interview. This, as mentioned throughout this chapter, is important as many respondents changed roles throughout the course of writing this thesis. Taking Taavi Kotka as an example, he would have been classified as a ‘public sector’ Data Embassy ‘insider’ at the start of the process when he was government CIO. However, I interviewed him in July 2019 after he moved into the private sector, so I have now classified him as a ‘private sector’ Data Embassy ‘insider’.

17 Estonia has the largest gender pay gap in the European Union (23% - compared to 14.8% average), whilst an EU-average shows that men (67%) are far more likely to hold senior management positions in comparison to women (33%) (European Parliament, 2020). Such a disparity is thus likely to have impacted upon the gender imbalance within this research, with Estonian men more likely to hold ‘elite’ roles across both the public and private sector.
the future use of such data (e.g. replication or future research); whilst Kari Lancaster (2017) points to such
difficulties within a contested policy domain “especially if policy processes are being studied as they play
out in real time”, such as the Data Embassy and my own research. As I highlighted at the beginning of this
chapter, Estonia’s relative size and general fluidity of its political intelligentsia meant that quote attribution
brought with it many concerns around information sensitivity and reputational damage\textsuperscript{18}. Indeed, some
respondents were happy to be recorded and fully quoted (making it clear whether anything was ‘off the
record’), but with a few respondents anxious at this prospect, I felt the logical decision was to completely
anonymise all interview data presented in this thesis\textsuperscript{19}.

Interviews with respondents would normally last for approximately one hour, sometimes fitting into a
predesignated ‘breakfast meeting’, coffee or lunch-break. Locations would vary: from the casual backdrop
of a coffee shop or restaurant to the more formal office setting in a government ministry. Nearly all
interviews were recorded and later transcribed\textsuperscript{20}. Although Alison Mountz has reflected on how this
“inhibited” (2007: 41) her exchanges with participants, I felt this allowed me to concentrate fully on the
conversation at hand, allowing me to take in respondents remarks and observations fully but also allowing
for the conversation to flow and for critical follow-up questions to be asked.

Over the course of completing this thesis, I adopted a somewhat reflexive and grounded approach to my
interview process. This was to be expected, given the novelty of the Data Embassy itself and as it evolved,
my questions (and approach) changed over time as I began to learn more about the concept. For example,
during early initial interviews I focussed heavily on discussions around the Data Embassy’s impact on the
notion of data sovereignty. After a number of inte

\textsuperscript{*\textsuperscript{18}}\textsuperscript{\textsuperscript{18}} Again, due to Estonia’s size and the sensitivity of topics around the
Data Embassy, it is still possible that certain quotes could be attributed and identifiable – for example, through the casual use of colleagues’ names or subject matter discussed. Despite taking measures to mitigate this (as explored below), I acknowledge that this may not be enough and accept that ensuring the anonymity of every quote when discussing the Data Embassy, or Estonian politics more broadly, may not be possible.

\textsuperscript{*\textsuperscript{19}}\textsuperscript{\textsuperscript{19}} Highlighted at the beginning of this thesis, one respondent was an exception to this rule. Taavi Kotka, leading protagonist in the development of the Data Embassy, was insistent that he remained fully quoted throughout this thesis. Given his relative notoriety and primary role in establishing the Data Embassy, I didn’t believe this to be too problematic. To comply with University ethics guidelines and to assure participants felt fully informed/supported, I also ensured every participant signed an informed consent form before taking part in any interview (see example in Appendix D).

\textsuperscript{*\textsuperscript{20}}\textsuperscript{\textsuperscript{20}} A small number of interviews were not recorded and transcribed - either on request of the participant, or due to the environment that the interview took place e.g. a conference. As I outlined above, I have still used them as ‘data’ in this thesis.
This section has reflected upon the many ethnographic encounters I have experienced whilst researching the Estonian Data Embassy, whilst revealing some of the inherent difficulties faced when researching within ‘elite’ spaces – from issues around civil service mobility to busy work schedules. Despite wholesale access to the Data Embassy team not being granted, I was still able to learn a great deal from conversations and ethnographic encounters with those both inside and outside of government. Kari Lancaster points to how adopting a reflexive approach can be “essential for better understanding the dilemmas of research which are too often sanitised or lost in other methodological descriptions” (2017: 101). By adopting a more reflexive approach in this research, I was able to work around these hurdles while maximising the encounters I had throughout the process of completing this thesis.

3.3 Data Embassy discourse: reports, bilateral agreements and propaganda

My first ‘encounter’ with the Data Embassy was, like for many outside Estonia, through an over-dramatised news headline. The exact piece that originally caught my attention has unfortunately escaped my now vast archived collection, but it would soon be joined by a cavalcade of headlines that would thrust the Estonian Data Embassy project into the public spotlight.

“Estonian plan for ‘data embassies’ overseas to back up government databases”

(Burton, 2014)

As Lorraine Kaljund (2018) synthesises (in one of few social science studies on the Data Embassy to date), initial discussion within Estonian public discourse was scant (and arguably remains so today). Pointing to an excerpt from the magazine Life in Estonia, Kaljund notes the rather sensationalised tones in an article entitled “country without territory” (2018: 5) and how early discussions around ensuring Estonia’s ‘digital continuity’ were beginning to form.

It would be this mantra – country without territory – that initially piqued my attention back in 2015. For a scholar of geopolitics, it is an incredibly fascinating yet loaded maxim. What would this – if even possible - look or feel like? Is the Estonian government pre-empting a return to exile, as experienced in 1944? Or is it proclaiming to be moving towards a government, or state, existing and operating entirely in digital form in the face of numerous existential threats and anxieties?

“Estonia redefines national security in a digital age”

(McCluskey, 2015)
Needless to say, this rhetoric wasn’t an unusual discovery. During previous research on the Estonian government’s e-Residency programme, I became very interested in, and critical of, the government’s bold claim of moving towards a ‘country without borders’ (e-Estonia, 2015). As such, and as Chapter 5 explores in greater detail, it is rather telling that the Estonian government appears preferential towards the notion of an inducing slogan for its many technological innovations. As this state “perfection narrative” (Drechsler, 2018) begins to propagate even further, it is curious that so many are being drawn, maybe even indoctrinated, by such assertions – particularly when they are often problematic and contradictory.

“‘Land is so yesterday’: e-residents and ‘digital embassies’ could replace country borders” (Reynolds, 2016)

Nevertheless, this section wishes to delve a little deeper into the discourse that has surrounded the Data Embassy. Serving as supplementary to the previously discussed rich, embodied encounters in the field, it aims to draw together the vast amount of Data Embassy discourse that has been produced, managed and circulated both inside and outside of Estonia. It is a journey, based largely on my own experiences and interpretations, through the many documents, press releases, news reports and government legal texts, in an effort to establish how the Data Embassy has been framed (or sometimes distorted) by various stakeholders, and the impact this has had on the perceived nature of the Data Embassy, state and my own research.

In terms of the discourse analysis conducted, texts (such as the newspaper articles and policy documents cited throughout this section) were sourced through early desk research and through typical search engine queries using terms such as: ‘Data Embassy’, ‘Data Embassy Estonia’, ‘Data Embassy Luxembourg’. This was an iterative process, and I one I would complete periodically throughout the completion of this research in order to gain more up-to-date perspectives on latest Data Embassy developments, whilst also collating news and research articles relating to Estonia’s digital society and wider Baltic security in relation to Russia. Cataloguing each article and document through internet browser bookmarks (and later through reference

---

21 The Estonian government’s ‘country without borders’ thesis was a dominant narrative during the launch of the e-Residency program. In previous research (Robinson, 2015), I critiqued the slogan as an unhelpful return to largely outdated neoliberal debates during the 1990s that centred on a supposed borderless world (Ohmae, 1990), but also how it was in direct conflict with Estonia and the EU’s own stringent border politics/policies. Although it was later dropped in the government’s official framing of e-Estonia and e-Residency, the expression is still commonly referred to by e-Estonia evangelists today.

22 Searches in Estonian were also considered but due to a lack of native language skills and poor browser translation, they were not considered critical to the data collected (exceptions do exist, and were often used to triangulate key dates and announcements). Interestingly, as discussed in Chapter 4, one respondent would tell me that ‘Data Embassy’ or any related terms searched in Estonian would yield little results, and how this perhaps meant that the project was more aligned to an international audience (interview 19 – 21/11/18). I also utilised Twitter’s search function as a key tool for identifying any key articles/wider conversations - a process that quite often elicited better insights and data in comparison to traditional search engine methods.
management software Zotero), I was able to analyse overall trends in Data Embassy coverage and wider security discourse relating to the Russian threat (discussed further in Chapter 5).

3.3.1 Letting your (geopolitical) imagination run free
Despite a lack of credible conversation within Estonia itself so far, the Data Embassy has certainly received greater attention outside of its borders. Journalists would latch onto certain tropes and geopolitical imaginaries regarding the role of Russia, the valued significance of NATO, and the existential security of a ‘tiny’ Estonia.

“With an eye on Russia, Estonia seeks security in cloud computing”

(Scrutton and Mardiste, 2015)

Gerard Toal, citing François Debrix’s ‘Tabloid Terror’ (2007), points to the dominant style of tabloid culture in twenty-first century geopolitics (2017: 49). Referring to the ‘state-produced dramas’ and ‘hyperreality’ disposed by the likes of Fox News and Russia Today, Toal notes a resurgence in Cold War narratives around “conspiracy theories and nationalist heroics” (2017: 51) that seem to exude potent political affect today. In the context of the Estonian Data Embassy, however, this would not simply centre around overt, provocative state-produced narratives surrounding a supposed Russian threat – as many interviewees would hint, why would you want to provoke and appear alarmist to your allies at the same time? (see Section 5.3)

Instead, this gap would largely be filled by the international journalist and news agency, captivated by the geopolitics and security of the Baltics, and an emboldened Russia and supposed territorial ambitions of its leader Vladimir Putin. Again, speaking to Toal’s (2017) critique of ‘thin’ geopolitical discourse (see Section 2.4), the immediate connections made between the annexation of Crimea and the geostrategic and socio-cultural significance of Narva were perhaps a little ‘lazy’ and one-dimensional (see Chapter 5).

“Estonia is so scared of a Russian cyberattack that it’s opening a data centre in the UK”

(Shead, 2016)

I would come to find, however, that many of these stories were at the unease of some Estonian officials and those working close to the project:

“Whenever the foreigners come, they want to get the answer that it is geopolitical. And we only do things because of the Russian threat and so on – and actually it’s
not the case, I guess. If you talk to government people, some say it out loud, but some don’t. But then with the journalists they always…if they can’t get the answer from one person, they will find somebody to have the answer – because this gives the project more attention and something to write about.”

*(interview 6 - 18/05/2018)*

Despite it being true that many of these stories were largely hyperbolic – lacking any detailed sourcing or local perspectives (particularly in relation to Narva) – it did emphasise an interesting tension between the Estonian government and discourse around the perceived Russian threat in relation to the Data Embassy (a recurring theme throughout the remainder of this thesis – see Chapter 5).

To augment the insights and geopolitical imaginaries that are conjured up by the Data Embassy even further, I would also spend time engaging in map design in order to contextualise and visualise the Data Embassy in manifold ways (see Fig. 3.3). Not only would this allow for a better visualisation of what a potential network of data embassies would look like from a personal perspective, but it would also serve as a useful tool and prompt when used in interviews and during academic presentations to wider audiences. Taking inspiration from Kotka and Liiv’s (2015) early interpretation of such a network, the map was utilised as a useful starting point on geopolitical discussions around diplomatic relations and potential future data embassy locations.

![Figure 3.3 – A map indicating what a network of Estonian 'Data Embassies' may look like in the future when in full operation (author’s own image)](image)
For those not familiar with the inner workings and mechanics of the Data Embassy, the map would allow for a better understanding around its intended functionality and strategy - although many would profess that such a vast network would be unlikely (or unthinkable) in the near future given the project’s relative novelty at present. Considering the Estonian government’s insistence that only “friendly foreign” (MoEAC, 2015) countries would be preferred for future data embassies, I settled on those locations with whom strong diplomatic and digital cooperation were already established (e.g. Canada and Japan). This in itself allowed for greater conversation and for geopolitical imaginations to flow around the project – for instance, why certain locations would/wouldn’t work became a useful discussion topic throughout this research (see Chapter 7).

3.3.2 Terminology matters
With nothing more than a number of elementary news reports to go on during initial desk research, it would be the discovery of more detailed, government-led research that would lead to a clearer understanding of the inner workings of the Data Embassy. As my own interest in the initiative intensified, the Estonian Ministry of Economic Affairs and Communications (MoEAC), tasked with delivering the Data Embassy project, published two feasibility studies in collaboration with the global technology giant Microsoft (MoEAC, 2015; MoEAC, 2016).

Both research reports would provide detailed policy and technical analysis regarding the use of public cloud services and the storage of Estonian government data abroad. Although not directly related to the components of the Data Embassy Initiative that this research focuses on (see Section 4.2), they would still serve as a crucial entry point to the conceptual nature of the Data Embassy, setting out provocative questions relating to cybersecurity, data sovereignty and the role of government and state in the face of an emergency.

The foreword by then-government CIO, Taavi Kotka, would also lay foundation to many of my own initial research motivations and enquiries around the Data Embassy:

“Changes in the world are unrelenting, and solutions that have worked previously are no longer good enough. Geopolitical events in 2014 brought the question of continuity to the forefront of national conversations in Estonia.

[…] Estonia must be able to continue to function as a government, and as a people, even in the direst of scenarios, including the loss of our territory. Since we do not have paper backups of data, our demands for data protection, security, and privacy are unparalleled. Any breach could have catastrophic consequences. Our digital services need to not only be the best in the world, but also the most secure and resilient.”
This somewhat prophetic statement and warning, considering the real possibility of cyber catastrophe and hinting at Estonia’s own existential worries, carried powerful, affectively “loaded” (Koschut, 2017: 483) connotations that would sit entirely at odds with the aforementioned claim of an exaggerated Russian threat in relation to the Data Embassy (see Section 3.3.1). How could the Estonian government, on the one hand, wish to downplay the Russian threat to journalists and researchers, yet on the other seemingly refer to it in everything but name with regards to the overall motives and goals of the Data Embassy? Indirectly referring to the ongoing Ukrainian crisis in 2014, but also the threat of cyberattacks and “natural disasters” (MoEAC, 2016), we again see an interesting and extremely selective tension between various key individuals, stakeholders and voices regarding Russia and/or motivations for the Data Embassy (explored further in Chapter 5).

As the Data Embassy continued to develop, so did the scope and intellectual diversity of my research. In June 2017, the announcement of the first Data Embassy to be located in Luxembourg brought with it a number of legal milestones that were debated and passed in Riigikogu (Estonian parliament). This presented an opportunity to engage with national and international legal texts (such as the Vienna Conventions – VCDR, 1961; VCCR, 1963) as the Republic of Estonia and Grand Duchy of Luxembourg signed a first-of-its-kind bilateral agreement regarding the extraterritorial hosting of data and information systems (see section 4.2). By engaging with a number of legal documents and texts (all with strict and precise language, semantics and structure), this research was subject to much wider debate and discourse over normative legal developments regarding data embassies and extraterritorial data storage more broadly (Robinson et al., 2019 – see also Section 7.2).

3.3.3 Where lies the scrutiny?
As highlighted already, this research has developed in parallel to the Data Embassy itself. Whilst this has served its benefit in being able to trace its numerous milestones and hiccups along the way, it has also meant that lots of initial research was conducted ‘blind’, with little opportunity for engaging with wider analysis and critique. A lack of credible conversation, not just in Estonia but globally, around the implications of extraterritorial data storage and security have meant that there are still many unanswered questions of which this research aims to illuminate (see Chapter 7).

---

23 The selective nature and general overtness around Russia can vary from institution to institution, sometimes individual to individual. This may be exemplified by the language, tone and content used by the annual Estonian Foreign Intelligence Service (Välisluureamet) ‘International Security and Estonia’ report. Nearly entirely focussed on the threat emanating from Russia, its message rarely changes: “The only serious threat to regional security, including the existence and sovereignty of Estonia and other Baltic Sea states, emanates from Russia. It involves not only asymmetrical, covert or political subversion, but also a potential military threat.” (Välisluureamet, 2019).
From a perspective of academic critique, rigor and impartiality, we have also seen little analytical debate from those ‘outside’ the Data Embassy community. Indeed, even at the time of writing this thesis, the two Microsoft reports remain the only in-depth and publicly available accounts of the Data Embassy (MoEAC, 2015; MoEAC, 2016) - accompanied by further strands of research from Taavi Kotka and those working internally on the project itself (Kotka and Liiv, 2015; Kotka et al., 2016a; Kotka et al., 2016b). With almost all the research emerging from within – and with a sole focus on the public cloud component of the initiative – I initially had concerns in terms of overall objectivity and detachment from the Estonian government. Fortunately, this has changed during the development of this thesis, as we now see a greater body of work and analytical attention on the physical Data Embassy component, of which this research contributes to (Kaljund, 2018; Robinson and Martin, 2017; Robinson et al., 2019; Sierzputowski, 2019).

This section has shown that encapsulating the true essence of a Data Embassy discourse has been a complex endeavour, challenged by its own novel and temporal character. Whether this has been through the early geopolitical imaginaries being allowed to run free by journalists and news reports, or through the powerful brand and image posited by government officials, we see a concept that has been allowed to propagate and propagandise with little (public) scrutiny so far. This has been complicated even further by a much more expansive ‘e-Estonia’ discourse that I, too often as researcher, became captivated and seduced by (discussed in greater detail in Chapters 4 and 5). Reflecting on this point in previous research during a visit to the e-Estonia showroom – where a plethora of Estonian ICT solutions and government success stories are put on show – the enchantment of this brand has been difficult to resist throughout my time researching in Estonia:

“As I take a look around the showroom I notice a wall already covered in pictures of international delegates and other VIPs. Japanese Prime Minister Shinzō Abe is one of them…

It was difficult to remain detached and impartial as a researcher, as the amalgam of presentations, interactive displays, Q&A sessions and take away e-Residency cards just add to the experience. It’s hard to understand why anyone who visits (whether that be journalist or international delegate) would leave without wanting to implement their own version or vision of e-Estonia. I know I certainly did.”

(Robinson, 2015)

To navigate this challenging research environment and to remain, to a certain degree, impartial has affected my own direction throughout this process. In terms of my positionality, I also had to remain cognisant of not becoming a state ‘flag-waver’ in the process of completing this research and to offer a critical
perspective on the Estonian state and Data Embassy. This was, at times, a difficult balance for me as a researcher as to heavily scrutinise or challenge the Estonian government and Data Embassy team on this project would, of course, have consequences and potentially limit my own access. In the following section, I reflect on these researcher anxieties in more detail, and how my own time in the field was shaped by the uncertainties surrounding the Data Embassy itself.

3.4 Failure in the field: the precarity of research/the Data Embassy

When reflecting on his own doctoral research, Jonathan Darling (2014) notes how entering the field may become a daunting, demanding and bewildering experience. More than simply adhering to stringent university guidelines on best practice, the realities of fieldwork often demand the development of “situated judgements” (2014: 203) which exceed ‘tick-box’ code of ethics procedures and formal research design and training. Such experiences may coalesce around insurmountable barriers in terms of access, navigating tricky power dynamics and relationships with research participants, or simply finding yourself at the mercy of political and socio-economic externalities out of your control.

The final section of this chapter serves as a reflection on the many challenges and opportunities found when conducting fieldwork – in particular, ruminating on the numerous potential pitfalls found when researching novel, innovative enterprises like the Estonian Data Embassy. Call it the researcher’s own ‘anxiety’ over the future of the research project, or conducting fieldwork in risky environments that may fall out of one’s own control, this section wishes to engage with the precarity of academic research.

The term precarity, argues Millar (2017), has recently seen a proliferation within the social sciences, whilst also being “at the risk of losing its analytical purpose.” Often seen as a “double-edged” phenomenon, precarity can be understood as either a condition or possible point of mobilisation (Waite, 2009: 413). With the latter, we have witnessed a growing usage of the term within work/labour geographies that stress the impact and intensification of the neoliberal state upon such aspects of society (Anderson, 2010; Hitchen, 2019; Lewis et al., 2015; Strauss, 2017). For Ettlinger (2007), precarity inhabits the microspaces of everyday life, and its affective, inbetweenness (Gregg and Seigworth, 2010) may also find resonance with influential work centred on emergencies and the precarious future of the neoliberal state (Adey and Anderson, 2012).

But whilst such work has been important in advancing our understanding of precarity and its impact upon the everyday – or, more importantly, the researched - there has been little discussion around the precarity of our own research and its subsequent impact on the researcher. Whilst we often reflect and take stock of our own positionality with regards to issues relating to identity, gender, race, or power relations in the field, rarely do we open up conversations relating to the processes and practicalities of ‘doing’ research itself: from its day-to-day precariousness to the demanding expectations around maintaining regular access, or even the potential of our research to fail altogether. To that end, the remainder of this chapter wishes to
focus on the precariousness of the Data Embassy and its impact upon my own research and role as researcher.

3.4.1 Researching a ‘government as a startup’

As alluded to previously, the Data Embassy is a novel conceptual creation. At the time of writing this thesis, it still finds itself in a continuous state of ‘becoming’, with various milestones that can be plotted alongside the development of my own research24. From humble beginnings, where both Data Embassy and my own research were simply ‘ideas’ and conceptual framings, aforementioned imaginations were set free and even my own beliefs over where this initiative would develop were accentuated. As time has moved on, however, expectations have become somewhat tamed. Interviewees would remain coy or uncertain over future developments, speculating on it being a ‘number of years’ before a fully-fledged network of data embassies would be operational; whilst others would remain sceptical over the project even taking off at all.

In terms of this research, the precarity also serves as a double-edged sword for my own position as researcher: not only are large parts of the research design reliant and contingent on successful (and sometimes prolonged) access to elite environments, and the continual progression of the Data Embassy alongside the three-plus years of actual doctoral research, but are also contingent on the successful nature of the Data Embassy itself. Discussed further in Chapter 5, the Data Embassy is very much emblematic of the Estonian government’s ‘startup’ mentality, in that novel technological solutions are often trialled with little burden on their expenditure and initial success rates. Introducing innovative approaches to e-government – such as internet voting and e-Residency – has proved relatively successful over the years, with the Western media often lauding Estonia’s startup mentality and digital transformation efforts (see Chapter 4). However, such an approach does raise pertinent questions over the longevity and stability of such political projects – but also the wider impact upon research and researcher too.

As quickly as technologies and novel initiatives are conceived and ‘put to work’, they can also be at risk of being stopped or thrown onto the metaphorical scrapheap. Nine out of ten startups are known to fail (Griffith, 2014) and, like startups, government-led initiatives are likely to face growth and financial challenges, alongside internal organisational struggles, along the way (see Section 3.3.2). This had varying impacts upon my positionality as researcher, as by continually asking myself ‘what if?’ in relation to access and the permanence of the Data Embassy, I would often toy with the prospect of no longer having a project to research. If the Data Embassy was stopped or ‘shelved’ tomorrow, what would happen to this thesis?

24 Many significant Data Embassy breakthroughs have occurred during the completion of this thesis. Most monumental was the opening of the first Data Embassy in Luxembourg in 2018 (the official date is not public knowledge), but I was also fortunate to trace the evolution of the concept alongside less momentous occurrences. These include the initial announcement between Estonia and Luxembourg in 2016, the signing of the bilateral agreement in 2017, and the passing of legislation through parliament in both Estonia and Luxembourg in 2018 (see Section 4.2 for a more detailed timeline of events). Personally, it has been fascinating writing a thesis alongside such developments, as I have witnessed the inception of the first Data Embassy getting closer and closer. As I tweeted on March 22 2018: “Yesterday, the Riigikogu (Estonian Parliament) approved the establishment of the first Data Embassy in Luxembourg - one step closer!” (source: www.twitter.com).
Would it all of a sudden symbolise an abject failure on my behalf? Or could we instead learn just as much from the failings of an ambitious government-led initiative, that would ultimately speak to a much wider discourse around the drivers and barriers found in public sector innovation?

Recent important work by Harrowell et al. (2017), has advanced calls for addressing failure in academic research. The general ubiquity and necessity of failure are too often stifled and avoided by academics, perhaps under the intense pressures and precarity of careers in academia (Butler-Rees and Robinson, 2020). In challenging this problem, Harrowell et al. (2017) point to the value that can be found in the critical examination and supportive reflection of failure in the field. Such a timely intervention and introduction to the literature has also led me to reflect upon the very precarious nature of the Data Embassy project itself. From the very start - when ideas have been formulated, and when initial access to the field has been brokered – there has been a very real need to engage with the prospect of failure.

3.4.2 No confidence, no Data Embassy?

On 9 November 2016, Estonian Prime Minister Taavi Rõivas was delivered a vote of no confidence by the Estonian parliament, leading to the fall of his government and subsequent resignation. I remember at the time reflecting rather anxiously on what this could mean for the Data Embassy and my research. Would the new Center Party-led coalition change course and no longer see the relevance for such a project? Might government ministers and civil servants become distracted by such turbulent political times? Thankfully, the Data Embassy remained on track, but it was a stark reminder that Estonian (as well as global) politics have seldom stood still during the process of completing my PhD. As well as the election of Donald Trump as U.S. president and Brexit (both having collateral impact upon this research), the Data Embassy has also endured two Estonian national elections and changes in presidential leadership. As it transpired, these political moments would not come to define my research, yet, the prospect of delay or failure, would continue to affect my day-to-day positionality as a researcher.

Joseph Chambers (2019) has recently written about this in the context of his fieldwork and research on the development and impact of Internet of Things (IoT) technologies in Nairobi, Kenya. In his work, Chambers reflects on the heightened tensions during a key domestic election period, and how the ensuing political turmoil led to a severely disrupted research plan and failed interviews, but also the sense of an “entrenched” (2019: 3) position as an outsider. It is a stark reminder that as a researcher you cannot afford to be rigid and have to move with an array of dynamic relations that are constantly in flux.

In dealing with the ‘what ifs’ in my own research, from potential changes in governments (leading to changes in overall policy and direction) to the perpetual mobility of government officials, I was forced to develop a

---

25 Mentioned earlier in the thesis, the election of Donald Trump as U.S. president led to a greater sense of insecurity across the Baltics after he described the NATO Alliance as ‘obsolete’ (see Section 1.2). Highlighted in the following chapter, Brexit also had an impact on the Data Embassy as it led to uncertainty over the location of the first Data Embassy (see Section 4.2).
certain elasticity to my methodology and research design, along with a renewable contingency plan in the event of any unforeseen roadblocks. As I highlighted in section 3.2, one roadblock in particular surfaced mid-way through my fieldwork in 2018, when a key contact and gatekeeper in the Data Embassy team moved on to a new role in the private sector. At that time, one primary methodological motivation was to embed myself as a researcher in the team developing the Data Embassy during future visits, part of my ethnographic study of the state (Mountz, 2007). Their replacement, however, was less convivial in their communications and any form of contact with the Data Embassy team subsequently ended. By adapting my methodology – renegotiating access with participants outside of government and attending a wider range of events and conferences to network - I was able to pursue an alternative strategy that opened up my research to wider analytical critique outside of the Data Embassy ‘inner’ circle.

To conclude, somewhere between the irony of researching anxiety in relation to the Estonian state (see Chapter 6), and my own anxieties surrounding my research project, there are very important and clear messages to be taken from the precarious nature of our research. As Paul Gready (2014: 196) notes, unavoidable, unforeseen ‘unknowns’ may present themselves within the complex and messy world of fieldwork, of which formal, theoretical training can only prepare you so far. When researching the Data Embassy, not only would large parts of the research design be reliant/contingent on successful (and sometimes prolonged) access to elite environments, but would also be contingent on the overall success of the Data Embassy itself. Arguably, the break-down of research due to many of the externalities described above would not spell the end for my PhD (in fact, a great deal could be learned from such events), but the perpetual anxiety and sense of not knowing what was around the corner would remain an enduring factor throughout.

I was also reminded of how important it is to continually reflect upon our positionality (particularly in relation to our own research and its design), and maintain stable and effective communicative relationships with respondents throughout the entire research process. Equally crucial would be to remain reflexive and cognisant of an ever-changing research environment, and to circumstances that are sometimes out of one’s control that may have direct ramifications for both the research and researcher. There may be substance in the claim that by developing a certain degree of flexibility (Chambers, 2019; Doyle and McCarthy-Jones, 2017) and “ethical sensibility” (Gready, 2014: 196), I was better prepared for the (albeit minor) political turmoils and precarious moments experienced throughout the course of completing this thesis.

3.5 Conclusion
In this chapter I have outlined and explored the methodological approach adopted in this research. My aim has been to demonstrate the complex processes and practices involved with researching a concept as novel as the Estonian Data Embassy. As I have highlighted throughout this chapter, I have completed this thesis alongside the emergence of the Data Embassy itself and thus did so with little guidance or analytical scrutiny
from the beginning of this process. In many ways, writing this chapter has become something of a reflexive (and cathartic) process in itself, as I paused to reflect on the number of challenges and revelations discovered during my time ‘in the field’.

Front and centre of this chapter’s aim has been the question of: *how do you research the Data Embassy?* I have addressed this in a number of ways throughout the chapter and, whilst not claiming to be exhaustive, have examined the Data Embassy and wider Estonian milieu through a mixed-methods, grounded theory approach. First, attending to one of this thesis’ main claims that the Estonian state is experiencing an anxiety at its centre, I open a discussion around how we might be able to theorise a collective entity, such as the state, as being anxious. Recognising that demonstrating or measuring the emotional or affective state of the state is by no means an easy task, I tackle this epistemological dilemma by drawing on a growing body of scholarly work that has attended to emotion and affect at a state-level in world politics. Specifically, I point to two approaches that attempt to identify Estonia’s anxiety at a collective level: first, through the embodied ethnographic encounters experienced during my time completing this thesis; and second, through an ‘affect-attentive’ discourse analysis of the Data Embassy in both media and state-produced discourse (see Section 3.2 and 3.3). Building on the work of Emma Hutchinson and Roland Bleiker (2014), Simon Koschut (2017), and more recently, David Nugent (2019), I am particularly interested in how the Data Embassy has been acted and communicated by an array of different stakeholders (for example, by the affectively loaded language around territory and security discourse regarding Russia). As I show in the remainder of this thesis, the aim of such an approach is to highlight the way in which the Data Embassy has been framed by certain actors but also what this may or may not reveal about the Estonian state itself.

In this chapter I also wanted to develop a methodology that explored the relationship between the Data Embassy and Estonian state, questioning what this may have revealed (or indeed masked) about the state’s everyday practice and performance. As Philip Abrams (1988) once argued, “the state is not the reality which stands behind the mask of political practice. It is itself the mask which prevents our seeing political practice as it is.” In revealing the complex and multifaceted processes by which the state’s mask is made and unmade (Nugent, 2019), I examine the merit of studying the Estonian state ethnographically (Section 3.2.1). Despite wholesale access to the Data Embassy team (and thus the inner strata of the state apparatus) not being granted, my own ethnographic journey allowed me to adopt a slightly different strategy that then allowed me to engage with those who may be more critical of the state at its margins. The remainder of the chapter then focussed in on a number of challenges faced during the completion of this research, from navigating/negotiating access within tricky elite environments to the way in which the Data Embassy allowed geopolitical imaginaries to run free with little analytical scrutiny. In doing so, this revealed two points that are continuously reflected on throughout the remainder of this thesis. First, how the Data Embassy has become something of a window through which the everyday practice and performance of the state is subsequently revealed. Second, how such an approach also reveals something incredibly interesting
about working within a state context that is, in itself, still being defined by transition and restoration (see Chapter 4).

Finally, I also reflected on my own experiences during the process of completing this thesis. In doing so, I highlighted the often-contingent nature of our research. From being required to continually (re-)negotiate and maintain regular access to elite environments over a prolonged period of time, to navigating political uncertainties and changes in government, I often felt at the mercy of my research and the environment it inhabited. Whilst this may not be an uncommon experience for many researchers conducting fieldwork, it particularly merits discussion within a postgraduate context, where pressure can often build (and overwhelm) on producing ironclad methodologies that subsequently lead to flawless results. With minimal support and little practical experience to draw upon, common instances of rejection or feelings of failure during the process of writing a thesis can be half-heartedly covered up or ignored completely. By opening up to such anxieties and reflecting on the contingent nature of our research, I hope this chapter will contribute to the growing recognition and consideration of the many hurdles we can face as researchers across a multitude of contexts and spatio-temporalities (Butler-Rees and Robinson, 2020).
“Sat behind the Estonian Prime Minister, Jüri Ratas, and his National Digital Advisor, Marten Kaevats, I listened as other dignitaries from around the world shared their experiences and vision for a future digital society. Despite not being his area of expertise, Ratas, thanks to Kaevats, was across his brief and confidently discussed issues around responsible and secure AI and cross-border data flows. I lingered at the end of the discussion, hopeful for a brief encounter with the prime minister, but he was unfortunately whisked away before an opportunity arose. Later on, I chatted to Kaevats during a drinks reception where I explained my research and why I was in Tallinn. He agreed to meet in a few weeks’ time, although the interview sadly never materialised.”

(December 2018)
Chapter 4 – A Catalyst for the Cloud

Estonia is a country that is continually trying to reimagine itself virtually, above and beyond its own physical limitations. Whether this is through the rather bold attempt of amassing 10 million e-Residents by 2025 (Tammpuu and Masso, 2018), or the storage of over one million Estonian patients’ healthcare records on a blockchain (Einaste, 2018), its role as a “digital power” (Areng, 2014) and “pathfinder”¹ (Drechsler, 2018) in digital governance is often lauded around the world. For a country that struggled to provide a basic phone line for half of its population at the start of the 1990s (Lungescu, 2004), Estonia now proudly boasts one of the most technologically advanced digital societies in the world.

But, as this chapter asks, how did Estonia arrive at this point today and what can we learn about how the digital state is imagined, framed, and operationalised? Are we able to learn anything from the leadership and political dexterity of successive Estonian governments since the restoration of independence in 1991? Or did unique and innovative forms of policymaking, coupled with a ‘restorationist geopolitics’ (Aalto, 2003), lay the concrete foundations from which the Data Embassy was subsequently established? In other words, what was the catalyst that led the Estonian government to turn to the cloud?

While there is no simple definitive answer to this final question, nor a single political policy or ‘moment’ that points to the Data Embassy’s emergence (see Chapter 5 for a greater discussion on the Estonian government’s motivations), I believe we can learn a great deal from Estonia’s journey post-independence, and what this can inform us about the role and function of the state today. In this chapter, I draw on Gerard Toal’s (2017) notion of ‘geopolitical culture’ as a theoretical tool for understanding the way in which Estonia, as a small state, sees and positions itself within a wider global system. For Toal, a state’s geopolitical culture refers to how states “see the world, how they spatialize it and strategize about the fundamental tasks of the state: security, modernization, the self-preservation of identity” (2017: 10). Toal’s work offers timely insights into Russian geopolitical culture and how, under Vladimir Putin, Russia’s role as an ‘independent great power’ has been characterised by attempts to re-establish and project state power (2017: 72), whilst simultaneously asserting a sense of victimhood against the West².

Estonian geopolitical culture, I argue by contrast, is dominated largely by Estonia’s relationship to Russia itself. As a small state, this is felt through issues of identity, culture and existential security, with Estonian geopolitical culture seeking to distance itself from Russia and its associated post-Soviet framings, whilst seeking closer alignment with the West in the process through institutions such as NATO and the EU. By introducing a number of prevailing narratives and storylines – Estonia in transition/restoration; Estonia

---

¹ Wolfgang Drechsler (2018) has borrowed the term ‘pathfinder’ from Daniel Vaarik (2015), a former advisor to the Estonian president. Part of Estonia’s communication strategy and nation-branding, the term is now common parlance across government discourse, referring to Estonia’s visionary approach to digital transformation (discussed further in Section 5.3).

² Toal argues that Russian geopolitical culture is dominated by three distinctive (and often competing) visions of Russia: a liberal European Russia, a revived imperial Russia, and an independent great power Russia (2017:72).
and the exceptional/existential; and Estonia as a digital pioneer – this chapter examines how the Data Embassy has been framed as part of Estonia’s wider ‘geopolitical culture’, and how this has enabled the state to accentuate and often sensationalise notions of resilience, creativity and trust in order to survive (and thrive) post-independence.

The next section (4.1) recounts this journey so far, tracing Estonia’s transition from Soviet ‘backwater’ (Taylor, 2018: 174) to today’s digital ‘powerhouse’ (Heath, 2019). Despite initial struggles in the immediate aftermath of independence – still in recovery from the “alienation and lethargy of the late-Brezhnev era” (Raun, 2001: 222) - Estonia underwent a period of immense change and reform, typified by the thought and leadership of President Lennart Meri (1992-2001) and administrations of Prime Minister Mart Laar (1992-1994 and 1999-2002). By 1994, Estonia was already being hailed as the “shining star” of the Baltics (Hansen and Sorsa, 1994); a decade later, Estonia had achieved its main national policy goal of membership of the European Union and NATO (Lauristin, 2003). Throughout this period, and perhaps still today, Estonians experienced what I will refer to as a ‘conveyor-belt period’ of technological innovation and development, as the introduction of a mandatory national identity card (2002) arguably set in motion a long-line of digital ‘firsts’ for the everyday Estonian. Many refer to the government’s ‘startup mentality’ and the propensity to trial novel technological projects and solutions with little burden on their success (see Section 5.3) – the antithesis of approaches we see from many Western governments today. In a contemporary Estonia, the government has adopted its own moniker, ‘e-Estonia’ (used to denote its success and expertise in e-government, cybersecurity and growing startup community), that it now proudly exhibits to the wider world.

Once the e-Estonia foundations were set, how then did the Data Embassy come to fruition? The final section (4.2) traces the project from its conception, all the way to the server racks and quasi-diplomatic status within a Luxembourgian data centre. In asking, ‘what is a Data Embassy?’, this section sketches out its conceptual makeup and highlights its role within a wider government cloud project. Fortunate in developing this thesis concomitantly to the Data Embassy itself, I assess the changing nature of the project as it faced numerous hurdles (political, technical and legal) along the way. I also aim to uncover what the Data Embassy is not. Something of a misnomer, the Data Embassy is not actually an embassy. Despite initial intentions to utilise embassy locations around the world, the Estonian government was forced to change tack and utilise a solution that functioned like an embassy instead. I explore this journey in detail, offering insight into the decision-making processes of Estonian officials and the state, and how the Data Embassy project in Luxembourg came to be.

4.1 Tigers and Unicorns: Estonia’s rise to digital powerhouse

Estonia’s transition to a free-market Western liberal democracy in the 1990s has been well-documented (Farivar, 2011; Kattel and Mergel, 2018; Lauristin, 2003). It is a story that is marked by Estonia’s rapid economic rise in comparison to its post-Soviet counterparts (Norkus, 2007; Panagiotou, 2001), but also by
its success in digitally transforming its public sector (Kattel and Mergel, 2018). Today, Estonia is held up as a beacon of digital prosperity, particularly in mainstream media, and is regularly cited for its prowess in digital governance, cybersecurity, and its thriving tech and startup scene (see, for example, Hammersley, 2015; Heath, 2019; Heller, 2017; Reynolds, 2016; Schulze, 2019).

By the same token, there are many in the Estonian government and Western media who like to portray a somewhat romanticised ‘rags to riches’ story. The following section offers a more nuanced portrayal, however, detailing many of the storylines and framings that constitute Estonia’s geopolitical culture. Often framed synchronously through a lens of restoration and transformation, I also consider how recent political shifts (both domestically and internationally) may have played a vital role in the emergence of the Data Embassy project. First, I examine Estonia’s journey in the immediate aftermath of independence that is characterised by risk-taking and ‘crazy ideas’ adopted by its leaders and pioneers (Section 4.1.1), before focussing on the country’s ‘pivot’ Westwards during the 2000s following accession to the EU and NATO (Section 4.1.2). The final section (4.1.3) brings us up to the present, with some reflections on Estonia’s role as a small state and digital governance pioneer and the global influence this now heralds.


“No one ever said that making the transition from communist totalitarianism to democracy would be easy”, remarked former Estonian Prime Minister Mart Laar, a little over four years after Estonia regained its independence from the Soviet Union (Laar, 1996: 96). At the time, it was a significant leap into the unknown: efforts to rebuild the state had been hampered by political instability and economic stagnation, whilst conflicts over land borders with Russia and ongoing debates surrounding citizenship, language and identity continued to cause division3 (Aalto and Berg, 2002; Berg, 2000; Berg and Oras, 2000; Feldman, 2001; Trimbach, 2014; 2017). As Pami Aalto (2003) has reflected, this period was also characterised by a ‘restorationist geopolitics’4 that would play a crucial role in Estonia’s state-building and foreign/security policies throughout this period (see also, Aalto, 2000; Berg, 2003; Kaljund, 2018; Trimbach, 2014).

It is widely considered that the collapse of the Soviet Union provided Estonians with a ‘clean slate’ and the opportunity to ‘start again’ – but also an opportunity to do so on a “lean, if not emaciated” budget, that stripped out needless bureaucracy and expenditure (Priisalu and Ottis, 2017). Due in large part to its

---

3 Relations between Estonia and Russia have been delicate since the collapse of the Soviet Union. Whilst both have remained close together through economic ties, issues around Estonian citizenship, language and identity – particularly within Russian-speaking demographics - remains a controversial topic today (Trimbach, 2017). A dispute over the border between Estonia and Russia remains unresolved, with more than 2000km of Estonian territory (annexed by the Soviet Union after 1945) still under Russian control today. The land was granted to Estonia following the Treaty of Tartu (1920) and negotiations to sign and ratify the border treaty remain ongoing. In 2015, following Russia’s annexation of Crimea, Estonia announced it would be building a 110km fence along its border, further escalating tensions (Whyte, 2018).

4 Restorationist geopolitics refers to the construction of a homogenised political space and ‘restored’ Republic in the aftermath of Estonian independence in 1991. This was characterised by an identity politics and the introduction of certain cultural policies during the 1990s (e.g. stringent citizenship laws and language requirements that were exclusionary for many ethnic-Russians who were effectively made stateless) that were justified by the “principle of restitution” (Berg and Oras, 2000: 607).
geographical proximity, Estonia began to initially align itself with a Scandinavian model of governance that embraced neoliberal economics and social policies on welfare and individual rights\(^5\) (Kattel and Mergel, 2018). Laar, along with President Lennart Meri (see Fig. 4.2), are often credited as the driving force behind Estonia’s dramatic economic development throughout the 1990s. Thirty-two years old at the time of taking office, Laar was emblematic of a youthful, forward-thinking government that was keen to leave its Soviet vestiges behind, when, at the time, Estonia was considered “*terra incognita*” across much of the West (Drechsler, 1995: 111). Principal to these changes were radical economic reforms - a shift to a market-based economy, the introduction of the *Kroon* as its own currency, and “a dramatic liberalization of trade and economic life in general” (Laar, 1996).

The introduction of projects *Tiigribüve* (Tiger Leap) in 1996 and *Look@World* in 2001 served as catalysts for Estonia’s overall digital transformation agenda\(^6\). Funded from both the public and private sector, they drove large-scale improvements to IT infrastructure and education with the bold aim of bringing all Estonian schools online and boosting overall internet penetration across the country (Ehandi, 2001; Farivar, 2011; Kattel and Mergel, 2018). Estonia was soon to be referred to as “The Little Country That Could” (Laar, 1996: 97), with its powerful post-Soviet vision primarily calling upon technology to streamline government institutions and nurture innovation, in a tiny country otherwise bereft of any infrastructure or resources.

\(^5\) As one interviewee told me, during the early 1990s Estonian officials actually travelled to Sweden for training on “how to build a government so you wouldn’t get oligarchs and things like that. How you build procurement systems, how to do a lot of these things” (*interview* 28 - 17/07/19).

\(^6\) Project Tiger Leap, often credited as spearheading much of the digital transformation that has benefitted Estonia today, was driven forward by then Minister of Education, Jaak Aaviksoo, and then ambassador to the United States, Toomas Hendrik Ilves, who would later become president (2006-2016).

\(^7\) This was the moniker given by American weekly news magazine, *Newsweek* (Laar, 1996).
Rainer Kattel and Ines Mergel point out that, despite Laar’s admiration for Thatcherite neoliberal free-market economics, Estonia’s digital transformation did not in fact follow Laar’s Smithsonian ‘invisible hand’ free-market pathway (2018). Instead, channelling Albert Hirschman’s (1967) ‘hiding hand’ principle, they point to a digital doctrine that was characterised by policymakers (sometimes naïvely) “pushing visionary changes without anticipating all the challenges and risks involved upfront” (2018). Throughout the 1990s this was symbolised by a desire to shake off any remnants of Soviet legacy across society (in ICT in particular), and to not simply catch up with the West but to “leapfrog” it in terms of technological development (Kattel and Mergel, 2018: 4). Strong R&D&I (Research and Development and Innovation) within academia and industry would prove instrumental in this early success, with the telecommunications and banking sector proving vital in this regard (Kalvet, 2007; 2012; Kitsing, 2011).

By the end of the 1990s, the government would also begin to reap the benefits of forward-thinking, technology-driven policies following the re-election of Laar as prime minister. In an effort to cut costs and streamline government decision-making, they introduced the world’s first ‘paperless’ cabinet in 2000, enabling ministers to debate and approve legislation digitally. The move would mark the first in many digital transformations spearheaded by government advisor and e-visionary Linnar Viik, widely regarded as one of the ‘founding fathers’ of Estonian e-governance. After the first paperless cabinet meeting was held in August 2000, we are able to trace what I refer to as a ‘conveyor-belt period’ of technological innovation for Estonians of which the remainder of this chapter will illuminate in greater detail.

Kattel and Mergel highlight how many of the “future-oriented and almost utopian solutions” that were first pioneered by the likes of Viik throughout the 1990s are still prevalent in Estonia today (2018: 4). Viik, according to Wolfgang Drechsler, acted like an independent minister and would often be allowed to simply ‘do things’ and experiment without fear of consequence (2018: 8). This mantle has since been adopted by a second generation of e-governance visionaries - in particular Taavi Kotka, who initially pioneered the Data Embassy concept (see Section 5.3 for a detailed critique of this approach to public administration).

---

8 Laar has famously claimed that the only economics book he read prior to becoming prime minister was Milton Friedman’s ‘Free to Choose’ (1980) – and many refer to his “Scando-Thatcherite” approach as pivotal in Estonia’s transition to a free-market economy (Meek, 1999). In 2006, the Cato Institute awarded him the Milton Friedman Prize for Advancing Liberty.

9 The paperless cabinet system (or e-cabinet) is built upon the principle of streamlining the government decision-making process. Ministers are able to view bills and determine their position in advance of meetings – should a bill fail to register an objection, it was agreed that it would be automatically adopted, saving ample time for other debates. It is believed that the process has cut the average length of a weekly cabinet meeting from 4-5 hours to roughly 30-90 minutes – mitigating unsustainable paper usage in the process (e-Estonia, 2019). Its formulation has been met with widespread interest and intrigue, with Prince Charles and Elton John having both requested to ‘see’ the paperless cabinet in action when visiting Tallinn (Farivar, 2011).
4.1.2 Estonia’s pivot to the West: a story of resilience, alliances and strategies (2001-2008)

“I’ve said that the goal of my first government was to turn Estonia from the east to the west and the goal of my second government was to make this turn irreversible.”

(Mart Laar – quoted in Farivar, 2011)

In 2004, Estonia joined the European Union and NATO. Signifying a historical pivot to the West, it was a decision that was not only driven by a promise of economic prosperity, but by a much deeper desire for ontological security (Mitzen, 2006). For a small state like Estonia, integration into these two international alliances would not only assist in empowering Estonia on a regional and global stage, but also prove pivotal in dealing with the multitude of hard and soft security threats now faced in the twenty-first century (Areng, 2014; Crandall, 2014; Gold, 2019; Kattel et al., 2010; Lupel and Mäkssoo, 2019).

Adopting a ‘small but smart’ approach within an ever-changing post-Cold War international system, has afforded many states the opportunity to become more visible and influential within large multilateral institutions, such as the EU (Browning, 2006; Joenniemi, 1998). For Estonia, its newfound role as “digital power” in the 2000s also allowed it to leverage a competitive advantage in “niche” areas of expertise, such as e-government and cybersecurity (Areng, 2014: 11). Building on the foundations set during the 1990s, the following decade saw an acceleration in Estonia’s digital transformation, with a shift towards digital governance and the adoption of e-services (Kalvet, 2007). Laar’s second administration (1999-2002) was defined by “frugality” – with government ICT projects circumventing external vendors - and a DIY culture that encouraged ministries to move towards more creative in-house “open-source solutions” (Kattel and Mergel, 2018: 6-7). The resulting parsimony, however, did not result in public-sector inertia. Instead, it became the catalyst for many of the technological innovations and solutions that have become cornerstone features of Estonia’s digital society today (see Table 1).
Two central pillars of a modern digital Estonia are X-Road (2001) and its national ID-card system (or eID – 2002). X-Road\(^\text{10}\) is often referred to as the “backbone” of Estonia’s digital society, enabling encrypted data to be securely exchanged between a plethora of different information systems, databases and institutions - both in the public and private sector (e-Estonia, 2019). In many ways, X-Road is the

\(^{10}\text{Since 2018, the Estonian government have reverted back to the use of its Estonian translation X-Tee. For consistency and clarity, however, I will continue to refer to X-Road throughout the course of this thesis.}\)
infrastructural artery that allows all of the state’s information systems to connect, communicate and operate in harmony (see Fig. 4.3). Developed by Estonia’s Information Systems Authority (RIA – formerly the Estonian Informatics Centre) and Cybernetica\(^\text{11}\) during the 1990s, X-Road was purposefully built as a way of uniting various state registries and databases in a decentralised manner (thus avoiding the inherent risks of a central ‘superdatabase’ (Veldre, 2016)) and soon found value in providing its services for Estonian businesses and citizens alike. Today, nearly all Estonian e-services (e.g. e-Health, e-Tax Board, e-Police), private sector services (e.g. banks, telecoms) and public-sector registries (e.g. Population, Health and Business registries) interlink via X-Road, enabling them to be used efficiently and securely\(^\text{12}\). Such is the success of X-Road, that today we see its technology and platform being exported around the world, with similar solutions in Kyrgyzstan, Iceland, Japan and the Faroe Islands (e-Estonia, 2019). In November 2015, Estonia and Finland became the first two nations to develop an interoperable joint data exchange platform on X-Road, enhancing cross-border services for citizens in both countries.

![X-Road architecture](image)

**Figure 4.3 - A popularised overview of Estonia’s X-Road architecture (source: www.ria.ee)**

An equally important facet of Estonia’s story to becoming a digital pioneer is the introduction of its mandatory, state-issued digital identity. Launched in 2002, the Estonian eID has since emerged as one of the most advanced national ID card systems in the world. Today 98% of Estonians carry one, with 67%

---

\(^\text{11}\) Cybernetica AS was established in 1997 and is one of Estonia’s key R&D centres. A spinout from Tallinn University of Technology’s (TTU) Cybernetics institute, Cybernetica has played a vital role in Estonia’s private sector and has spearheaded many of the country’s cybersecurity and e-government solutions in use today (Kalvet, 2012: 150).

\(^\text{12}\) X-Road’s unique architecture is coupled with a host of regulatory/organisational/technical measures that ensure data are collected, stored and transferred efficiently and securely. Since 2007, Estonia has adopted the ‘Once-only’ principle, meaning that data are collected only *once* by individual institutions, prohibiting the creation of separate databases for the same data. On X-Road, this ensures that data are not duplicated in different locations, reducing the risk of data silos and enabling complex enquiries to be made between multiple agencies and information sources. Over 1 million queries and requests are made over X-Road every day, with 985,878,107 being made in 2018 alone. There are nearly 3000 Estonian services that are used via X-Road, with approximately 500 institutions and enterprises (both public and private sector) benefitting from its infrastructure (X-TEE, 2019). Updated statistics on X-Road can be found at: [www.ria.ee/en/state-information-system/x-tee.html](http://www.ria.ee/en/state-information-system/x-tee.html).
using it on a regular basis (e-Estonia, 2019) – all of this despite varying attitudes globally to national identity card schemes, due to concerns over privacy, deployment costs, data management and doubts regarding overall utility (Martin, 2017: 398). Its everyday function is largely underpinned by Estonia’s Public Key Infrastructure (PKI) which allows for secure authentication, digital signatures and access to a wide range of digital services provided by the state. The everyday Estonian not only uses their eID to access online banking services and medical records, but can also (via an automated system on X-Road) submit their tax returns digitally and in a matter of minutes. Estonians can also benefit from the eID’s encryption functionality that enables data to be securely transferred and digitally ‘signed’ – a function that is now as legally binding as a handwritten signature (Kull and Kask, 2019: 33).

Perhaps one of the eID’s most unique functions so far has been to allow Estonian citizens the opportunity to participate in democratic elections online (and to do so from almost anywhere in the world). In 2005, Estonia became the first country in the world to hold national elections over the internet, allowing citizens to vote online during local elections. Initially, online voter turnout was low, with 30,275 Estonians (3.4% of the registered electorate) opting to vote over the internet during the 2007 national parliamentary elections. However, its popularity has gradually improved since then and during the most recent parliamentary elections (March 2019), a record 247,232 people (43.8% of the electorate) voted online\(^\text{13}\) (Valimised, 2019).

While the ‘i-Voting’ system has been lauded by many across the world, it has not been without its share of criticism. Some have pointed to purported “architectural limitations” and “procedural gaps”, as well as insider threats and more sophisticated state-sponsored cyberattacks, as inherent security concerns that could threaten the integrity of any future Estonian elections (Springall et al., 2014). The Estonian government have largely pushed back against what it believes to be ‘political’ criticism, instead pointing to its proven successes and clean security audits during elections so far\(^\text{14}\). Estonian researcher Tarmo Kalvet has suggested that its relative success and lack of serious security incident to date can be put down to the government’s own explicit and effective risk management strategy, which addresses “all expected risks by enhancing the capacities of the procurer, carrying out in-depth risk analyses, and endeavouring to generate trust through consistent dialogue and openness” (Kalvet, 2012: 152). In a recent study of the broader procedural components of Estonia’s i-Voting system, Nurse et al. (2017) also point to the ways in which measures adopted by the Estonian government go some way towards building trust and transparency in the system both domestically and internationally, most notably through the publication of system documentation, use of open source software and an “open-door policy” for auditors and electoral observers (2017: 14).

\(^\text{13}\) It is important to note that, by and large, internet voting is not seen as a replacement for traditional paper-based elections. Rather, many consider its additional functionality in terms of voting convenience (e.g. those with disabilities or living remotely), potentially increasing voter turnout and reducing overall administrative costs (Krimmer, 2012; Krimmer et al., 2020).
\(^\text{14}\) It must be noted, of course, that just because no reported attacks or breaches have been reported so far, this does not equate to the system (thus the wider democratic process) being secure.
The vast majority of the world’s democracies still largely rely on paper-based voting systems. Whilst there are now examples of electronic voting being used to either cast or count votes (e.g. Brazil, India), there are still a host of difficulties and concerns over the use of electronic voting machines, as demonstrated in the U.S. (Perrigo, 2019). If nothing else, despite such criticisms, Estonia’s foray into internet voting in 2005 has become another useful yardstick for illustrating just how far technologically the country had come in such a short space of time.

As I briefly highlighted at the beginning of this thesis, Estonia’s journey to this point was also marked by another critical juncture in April and May 2007. Following the controversial relocation of the ‘Bronze Soldier’ statue, a Soviet World War II memorial, to a military cemetery on the outskirts of Tallinn, violent clashes erupted on the streets of the capital between local authorities and large numbers of the city’s Russian-speaking community. Often remembered as the ‘Bronze Night’ (26 April), protesters first congregated around the statue itself before spilling over into the city centre later that evening with widespread rioting and looting taking place, resulting in over one thousand arrests, a number of injuries and one fatality. Although local authorities ensured a sense of normality returned to the streets the following day (27 April), the disruption soon shifted to cyberspace as the country fell victim to what is widely believed to be the first instance of a state-sponsored cyberattack (see, for example, Burton, 2013; Greenberg, 2019; Hansen and Nissenbaum, 2009; Herzog, 2011; Kaiser, 2015; Kaska et al., 2010; Kello, 2017; Ruus, 2008).

For the next 22 days (27 April – 18 May), the country was hit by “several waves” of sustained distributed denial-of-service (DDoS) attacks that targeted the computer systems of the Estonian government and private sector (Priisalu and Ottis, 2017: 446). While it is thought that the cyberattacks were not intentionally designed to damage critical national infrastructure or cause any harm to human life, they succeeded in disabling a number of government and news portals, with many banking services also severely disrupted.

In the immediate aftermath, fingers began to point at Russia as political relations between both countries had all but collapsed in the weeks preceding the attack. The Russian government began to immediately distance itself from such claims, whilst credible attribution proved difficult (and remains so today) despite

---

15 The decision to move the Bronze Soldier statue was highly contentious and widely thought to be a politically motivated one (see, Kaiser, 2015; Tikk et al., 2010). Erected in 1947 to commemorate Soviet soldiers that had lost their lives in World War II, many ethnic-Russians believed the statue represented victory and triumph over Nazi Germany (and its relocation was thus further proof of their marginalisation), whilst for most native Estonians it was a material and symbolic representation of decades of Soviet oppression. The Russian government also vehemently opposed its relocation, with foreign minister Sergei Lavrov describing the decision as “blasphemous” and stated that there would be “serious consequences” for their relations with Estonia (Myers, 2007).

16 During the 3-week period of attacks, 58 websites were defaced or shut down (including the websites for the Estonian president, Parliament and a number of government ministries), whilst major banks, media organisations and political parties were severely disrupted (see, Ottis, 2008; Tikk et al., 2010 for a more detailed account of the attacks and their impact).

17 The relocation of the Bronze Soldier became a lightning rod for rising tensions between Estonian and Russian nationalist movements; but can also be seen as part of a much broader breakdown in political and diplomatic relations between Estonia and Russia. Prior to this moment, political rhetoric had already intensified with the Russian government accusing Estonia of human rights violations regarding the ongoing treatment of its ethnic-Russian population (Herzog, 2011: 53 – see further explanation in Chapter 5). During this tense period, the Estonian embassy in Moscow was also besieged by pro-Kremlin protestors for a number of days (seen as retaliation to events in Tallinn), with Estonian ambassador Marina Kaljurand reportedly physically attacked during a press conference (Ottis, 2008).
the best attempts of Estonian, EU and NATO cybersecurity experts (Traynor, 2007). The Estonian government, however, has maintained its position that Russia was responsible – either directly or indirectly - via state-sponsored ‘hacktivists’.

Often cited as the world’s ‘first’ cyberwar, the general fallout and hyperbole surrounding the 2007 incident (particularly within Western security discourse – see, Kaiser, 2015; Kello, 2017) has been incredibly powerful. Ten years on, the BBC has described how the attacks transformed and “still shape the country today” (McGuinness, 2017) – a point that is difficult to denounce with a number of societal and political after-effects still being registered today. In this thesis, I am particularly interested in how the 2007 cyberattacks may have played a vital affective role in Estonia’s subsequent security discourse and policymaking. As I build on and argue in the following chapter, the cyberattacks not only served as a wakeup call for the Estonian government but also stressed the intrinsic value of cybersecurity for the wider global community and its value for a state’s national security. Although we may not be able to draw a direct link between the events of 2007 and the establishment of the Data Embassy, it is clear that it has served as a catalyst for many developments in Estonia since then (see Section 5.2).

One of the key affective developments has been Estonia’s transformational shift in its approach to cybersecurity. This led to a number of strategic, organisational and legislative changes, pursued largely in accordance with the country’s first National Cyber Security Strategy in 2008 (MoD, 2008). Seen as a direct response to the 2007 cyberattacks, the strategy was pivotal in coordinating expertise from across the public and private sector (at an inter-agency level and including key stakeholders from academia, industry and think tanks), which in turn served as a vital platform to allow Estonia’s cybersecurity capabilities to mature and flourish.

With a desire to learn lessons from 2007 and drive Estonia’s role as a leader in cybersecurity internationally, the strategy became inspiration for a number of states to follow suit with their own national cybersecurity strategy in the years ahead (see Robinson and Hardy, 2021).

---

18 Initial analysis from CERT-EE (Estonia’s Computer Emergency Response Team) indicated that the vast amount of attacks originated from sources outside of Estonia, and were directed with malicious intent. Pointing to “political signatures” that were detected in the malicious traffic (e.g. Russian IP addresses, some originating from state institutions), Estonian cybersecurity researcher Rain Ottis argued at the time that all the circumstantial evidence pointed to the plausibility of Russian involvement (or influence) in the attack – a view that has since been largely backed up by the wider cybersecurity community. Experts have also pointed to the role of Russian-language forums both prior to and during the attacks, with clear instructions being posted on how to attack and ‘flood’ Estonian networks in retaliation to the movement of the Bronze Soldier. Highlighting the difficulty surrounding cyberattack attribution, however, many have pointed out how IP addresses/malicious traffic may have been ‘spoofed’ (to make it appear that the attack had originated from Russia) and is therefore a lack of real evidence. Affording the Russian government plausible deniability, they have thus been able to shake off any accusations and lay the blame firmly at non-state actors. Members of pro-Kremlin youth movement, Nashi, have claimed responsibility, whilst Sergei Markov (Russian State Duma) claimed that an unnamed aide was responsible for its orchestration (Tikk et al., 2010: 23). In March 2008, Dmitri Galushkevich, a young IT student from Tallinn, was convicted of participating in the attacks (and fined 17,500 Kroons), the only arrest made in connection to the ‘Bronze Night’ cyberattacks.

19 The publication of a national cybersecurity strategy coincided with a number of organisational and legislative changes across Estonia. One notable shift saw the creation of the Estonian Defence League’s Cyber Unit (EDL CU): a voluntary collaboration of cybersecurity experts from across both public and private sectors, with the aim of strengthening cyber defence skills and support capabilities in the event of another attack (see, Kaska et al., 2010; Tikk et al., 2010).
Other key strategic developments during this period have been the introduction of Estonia’s first Information Society Strategy 2013 (2007-2013 - RIA, 2007) and its Digital Agenda 2020 strategy (MoEAC, 2013). Bringing together some of the best minds across the Estonian public and private sector, the aim of both strategies was to set out plans for a well-functioning, cost-effective and secure digital society that facilitates the development and use of smart ICT solutions. For example, the Digital Agenda 2020 strategy’s goals were to drive forward citizen inclusion/participation in ICT and government services, the security and capability of eID and authentication services (including internet voting), and the introduction of a ‘no-legacy’ principle across the public sector\(^{20}\). The strategy can also be credited for spearheading early policy discussion and analysis on e-Residency and the Data Embassy (see Section 4.2).

Whilst such strategies have played a key role domestically and have arguably shaped many of the developments we see in Estonia today (including the Data Embassy), it is important to also consider their role in repositioning the country as a global leader and forerunner in areas such as cybersecurity and digital governance. As Josh Gold (2019) notes, Estonia’s role in shaping NATO doctrine has been central to its respective National Cyber Security Strategies. In its latest iteration, the government advocates:

"The strength of Estonia’s cyber trademark requires a conscious and integral approach to international topics. Estonian foreign relations on cyber themes must be proactive to keep up with the stiffening global competition. In this endeavour, Estonia can rely on its existing strengths, but it will have to continue to develop areas where Estonia could be in the lead role and continue to be globally visible. As a good example, the NATO CCDCOE in Tallinn makes it possible for Estonia to be in the lead role on NATO cyber defence issues.”

(MoEAC, 2018)

As the subsequent section (and Section 5.3) goes on to show, such a narrative is vital for enabling greater awareness around Estonia’s role and expertise on a global stage (a key aim of Estonia’s most recent National Cyber Security Strategy – 2019-2022) with its strategy and approach to cybersecurity and e-government often being cited as prototypical for other states around the world (Barnett, 2019).

---

\(^{20}\) The no-legacy principle mandates that ICT solutions in the public sector should not be any older than 13 years (MoEAC, 2013). Such an approach may seem radical, but as the recent widespread WannaCry and NotPetya cyberattacks illustrated, vulnerabilities in legacy operating systems can have catastrophic consequences. Arguably, however, given Estonia’s size and lack of political legacy and infrastructure, such a policy may be easier to mandate than in less agile bureaucratic countries (discussed further in Chapters 5 and 6).
4.1.3 The ‘Skype effect’: framing creativity, trust and diplomatic cooperation (2008-present)

If the first two decades of re-independence can be characterised by ‘crazy ideas’, risk-taking and a degree of thriftiness across the public sector, the last decade has witnessed a consolidation of these values. Now firmly positioned within the EU and NATO, and with a growing authority in areas of cybersecurity and digital governance, there are many who believe Estonia may well be ‘punching above its weight’ on the international stage. That said, Estonia now sees itself as a prominent voice within the small state community, and ‘pathfinder’ (Drechsler, 2018) by way of innovating and experimenting with novel technological solutions and policies21.

In many ways, this has been exemplified by Estonia’s own thriving tech and startup scene, often labelled as the Baltics’ very own ‘Silicon Valley’ (Cassidy, 2014). At the time of writing this thesis, Estonia has just welcomed its fifth tech ‘Unicorn’ - a privately held startup or company valued over $1bn – with the customer relationship management (CRM) platform Pipedrive joining Bolt (formerly Taxify), TransferWise, Playtech and internet telecommunications giant Skype as Estonian-crafted gems in the global startup world (see Hunt, 2018). The original software developers behind Skype’s technology originated from Tallinn in 2003, and there are many who refer to the ‘Skype effect’ (Cellan-Jones, 2016) and the lasting impact the company has had on Estonia’s burgeoning startup community22. Skype’s legacy can arguably still be detected across Estonia today: first, through the entrepreneurial mindset of its relatively young population; but also, in the high density of Estonian software developers and engineers that perforate its startup, e-government and cybersecurity communities23.

This entrepreneurial mindset and willingness to push technological boundaries has been embodied by the public sector too, with many recent policy instruments and innovations emblematic of a ‘government as a startup’ (see Section 5.3). In 2014, the Estonian government announced its e-Residency programme, promising to unleash the world’s ‘entrepreneurial potential’ and move towards the idea of ‘a country without borders’ (e-Estonia, 2015). e-Residency provides “entrepreneurs and residents of other countries with global access to Estonian e-services via state-issued digital identity” (Tammpuu and Masso, 2018: 544), with e-Residents able to establish and manage their own EU-based company online, from (almost)

---

21 In recent years, the Estonian government has made significant developments at the intersection of technology and law, particularly around the use of AI in the public sector. For example, since March 2017, the testing of self-driving vehicles on public roads has been legalised. The government is also working on a “Kratt law” to help adjust and regulate legislation on artificial intelligence in both the public and private sector, focussing on current societal debates around algorithmic liability (see, Hankewitz, 2019; MoEAC, 2019). Kratt is a magical creature from Estonian mythology and is used as a metaphor by the Estonian government to communicate the potential utility and risks of AI across society.

22 Throughout my time in Estonia, at various tech conferences and events, I would often hear the term 'Estonian Mafia' (#EstonianMafia) being used to describe the country's vibrant startup ecosystem. At times it felt almost cult-like, but has equally played a crucial role in Estonia’s nation-branding strategy. As of 2019, there are over 550 startups operating in Estonia—the highest number per capita in the world (Startup Estonia, 2019).

23 There are many who believe that Estonia’s tech-literate society of today is largely a bi-product of the Soviet-era, and an educational legacy in mathematics and other hard-sciences (Jansen, 2012; Keen, 2016). Sue Curry Jansen notes of how the Soviet Union set up scientific institutions across the Baltics in the 1950s, and “by chance” Estonia ended up with the Institution of Cybernetics, “which gave it a significant head start among former Soviet client states in developing its computer industry” (2012: 83).
anywhere in the world (e-Residency, 2020). The programme typifies the governments ‘startup mentality’ and, despite various criticisms, has since seen exponential growth with over 75,000 e-Residents and 15,000 companies now operating digitally in Estonia (e-Residency, 2020).

In 2016, the Estonian government took another bold step into the unknown by announcing that it would store over one million Estonian healthcare records on a blockchain. In doing so, patient medical records are now time-stamped and stored on government databases in such a way that makes their usage transparent and it impossible to alter, delete or update any information in an unauthorised or accidental manner. The decision to utilise such a novel technology held inherent political risk. But with a greater dependency on its digital infrastructure, a national conversation around trust, accountability and data security (or more precisely, data integrity) was becoming noticeably more mainstream. Estonian president at the time, Toomas Hendrik Ilves (2006-2016) – who is often regarded as one of the first European presidents to fully understand and embrace digital technologies and cybersecurity (Taylor, 2018: 196 – see Appendix A for more on Ilves) – publicly embodied this message:

“For I can perhaps live with someone knowing my blood type, but I cannot possibly live with the fear that it has been changed”

(Toomas Hendrik Ilves, opening the CyCon conference in Tallinn on June 4 2014 – President.ee, 2014a)

Strong political discourse around data integrity and cybersecurity was perhaps justified in light of the 2007 cyberattacks. But the decision to store healthcare records on a blockchain, alongside many of the other technological developments mentioned so far in this chapter, may also speak to a distinctive Estonian governance model, as well as attitudes towards data privacy and levels of ‘trust’ between citizen and state.

Indeed, the narrative that Estonians are generally more ‘trusting’ in their government was one that I would hear time and time again throughout my time researching in Estonia (Huber, 2019). Linnar Viik, e-Estonia visionary, believes this is a process that has developed piecemeal over the past three decades: “we are building trust step by step, service by service, communication by communication” (Plantera, 2018). This could arguably be traced back to the mid-1990s with the introduction of a population database and personal identification system (isikukood or Personal Identification Code), along with the aforementioned X-Road

24 Since its inception, e-Residency has hit many roadblocks regarding the use of banking services for its e-Residents. Following a recent money laundering scandal that hit the Estonian branch of Dankse Bank in 2018, the risk of e-Resident ‘shell’ companies being used to launder ‘dirty money’ were also raised – but later refuted (Rang, 2019).

25 e-Residency was the focus of my Master’s research in 2015 (Robinson, 2015). When visiting the seven person-strong team in Tallinn, the depiction of ‘government startup’ was extremely visible. I became acutely aware of how avant-garde (but also how fragile) the programme was, with many facets of e-Residency yet to be developed or ‘go live’. If the programme was to fail or not work out, then, as many told me, it would simply be cast aside. Fortunately, this has not been the case, and e-Residency has continued to grow. Like a true startup, e-Residency ‘2.0’ was recently announced, with phase II seeking to scale the programme further (see Section 3.4 and 5.3 as I highlight similar dynamics during the completion of this doctoral research).
and national ID card at the turn of the century. Jaan Priisalu and Rain Ottis have argued how these fundamental pillars in Estonia’s digital society legislated a common-sense approach to data usage by government institutions, but also allowed individuals to take control of their own data (2017). Citizens ‘in control’ of their own data would be yet another mantra I would continually encounter – I pushed one interviewee to explain what they believe this means:

“There are many other governments that think we should build backdoors into information systems, but Estonia is really taking the opposite direction and giving all its citizens and people using the infrastructure an opportunity to encrypt the data. Which is a complete opposite as well [to other governments], so I think this shows the mindset that if people are trusting of the government then the government should trust the people […]

[…] At eesti.ee - which is the central portal where you can access government services – you can login and see which government institution has looked at your data and when. And if you recognise something wrong there – like, ‘why has this doctor seen my data, because he or she isn’t my family doctor?’ – then you can always make a notice, and if there are no grounds [for access] then there are legal consequences for that. Probably he or she will lose their job. If the police are looking at data from a celebrity, then those cases are taken really seriously. Which means that you have this trust on both sides, and I think with GDPR coming in, this opportunity to see who, in government, has seen your data is really an asset and really a thing that should be exported. It’s as important and cool as Data Embassies and e-Residency. For us, it’s so normal, but actually for German or French people it would really be something to justify the digital government. With papers, you can never ever know who has accessed when and why.”

(interview 6 - 18/05/18)

From this, I gained a sense of a model of digital governance that many believe to be built on transparency and an inherent degree of trust between citizen and state, particularly in terms of issues around data privacy, ethics and surveillance. For many citizens, a digital identity and the use of personal data in this way is simply the normality and part of the taken-for-granted background of everyday life. Was this, as I have since reflected, also characteristic of perceptions towards the Data Embassy? Why are everyday Estonians so comfortable with its government storing their data outside of its own borders? Has there been a public conversation on this topic? “Not at all”, replied one interviewee:
“When I first started to find information about it – when I didn’t have access via my current channels – and I was just trying to find ‘news’… ‘Data Embassy’ in English would give me way more than anything I would search in Estonian. So, this could be an indication that this is not really for the Estonians, really. But no, I don’t think the Estonians know, or care really.”

(interview 19 - 21/11/18)26

Regarding overall attitudes towards data privacy, surveillance and trust between Estonian citizens and the state, a critical body of research remains underdeveloped (although attempts have been made to address this on an Estonian and wider post-Soviet level, see: Björklund, 2016; Kalvet, 2012; Svenonius and Björklund, 2017; Tammpuu and Masso, 2018). Wolfgang Drechsler has been openly critical of this point, questioning whether levels of trust are actually that high – instead pointing to its general decline in comparison to an OECD average (2018: 12). Drechsler goes on to suggest that it is more an “absence of fear” of government that drives Estonians’ trust of the state27. As Chapter 5 will explore in more detail, such attitudes, at least from an outsider perspective, may also be wrapped up in the government’s strong branding and marketing power where trust is posited as the “cornerstone” of its digital society (Plantera, 2018). Indeed, the cultivation of trust appears to play a central role in Estonia’s framing as a ‘digital pioneer’. Whether the everyday Estonian feels the same way, however, is currently lacking real scrutiny and in need of urgent analytical critique.

A security flaw discovered on the chips used in the Estonian ID card in August 2017, however, held potentially disastrous consequences for levels of trust between government and citizens. The ‘ROCA’ vulnerability put approximately 800,000 ID cards at risk – theoretically allowing every private key to be generated from the public key – which may have allowed attackers to access sensitive information, exploiting the victim’s cryptographic keys that are used daily by Estonians for authentication and digitally signing documents (RIA, 2018). Working fast to revoke the digital certificates and update the affected cards, the Estonian government were praised for their handling of the crisis, pooling expertise from across government, the private sector and academia (similarly to the 2007 cyberattacks) but also in their transparency and openness with the public (which included affected e-Residents outside of Estonia). Whilst accepting that there have been very strong ‘lessons learned’ from the incident, the government have also

---

26 In Chapter 3, I reflected on how there wasn’t a great deal of public discourse around the Data Embassy in Estonia – and I also found this to be the case during conversations with locals and Estonian friends. With the Data Embassy and the novel process of extraterritorially storing citizens’ data outside of its borders receiving little public critique, I’m led to assume that many Estonians are simply unfazed and used to such dramatic developments. I would often joke with respondents and Estonian friends about how any such decision in the UK, France or Germany (more established, bureaucratic states) would be met with uproar and derision. Why is Estonia so different? Ultimately, further research on this topic – including wider Estonian attitudes to data and trust – is urgently required.

27 As Kadi Vooglaid’s (2018) reading of Drechsler’s work suggests, it is this absence of fear that “makes Estonians less paranoid of power, which, in turn, makes it easier for them to entrust personal, and even sensitive information, such as medical records or voting data, to state information systems”.
indicated that trust has not been “corroded”, highlighting that 10 million digital signatures were used in February 2018, compared to 6 million in the year before the attack (RIA, 2018).

Reputational damage (arguably) intact, Estonia’s diplomatic profile and influence has continued to grow over the last few years. In 2017 (July-December), the country held the Presidency of the Council of the European Union. One of the key Presidency priorities was the notion of a ‘digital Europe’, culminating in the Tallinn Digital Summit, where Estonia made the case for the ‘free movement of data’ as the fifth freedom of the EU\(^2\) (e-Estonia, 2017). In June 2019, Estonia was elected for the first time as a non-permanent member of the UN Security Council (2020-2021). Delivering a clear message endorsing international cooperation on matters of security, trade, and more niche areas of cybersecurity and e-government, Estonia also believes it will give a voice and advocate the interests of other small states in the activities of the Security Council (MoFA, 2018; Raik, 2019). By utilising its small state mindset and skilful diplomacy, suggest Lupel and Mälksoo (2019: 10), Estonia is well-placed within the current geopolitical climate to provide “an important, credible voice with moral authority to remind all member states of their obligations under international law, reaffirm normative commitments to compliance, and advocate for a recommitment to a multilateral, rule-based order that is of collective benefit to the entire world.”

Conversely, a lurch to the far-right in recent parliamentary elections (March 2019), with the election of EKRE (Eesti Konservatiivne Rahvaerakond – Estonia’s nationalist party) into a new coalition government, could have damaging repercussions for Estonia’s growing reputation as a forward-thinking, tolerant and innovative country. Rhetoric of an ‘indigenous Estonia’, attacks on journalists, and stoking division between ethnic-Estonians and ethnic-Russians, are the antithesis of many of the core values Estonians have tried to promote on a global stage in recent years. Fuelling these tensions may well be playing into Russia’s hands too, suggests Kristi Raik, Director of Estonian Foreign Policy think-tank ICDS:

“Russia wants to sow division and polarisation in European society and that’s why the rise of EKRE creates a more favourable environment for Russia’s interference, when the level of stability and cohesion in society is weaker.”

(BBC interview – Mackenzie, 2019)

It may be a little too early to suggest that EKRE will have any impact on the Data Embassy and its functionality, especially given their minority role in government. However, the premise of extraterritorial

---

\(^2\) Data would join the free movement of goods, services, capital and persons within the EU. In line with the European Commission’s priority of a Digital Single Market, the proposal would inhibit EU member states from imposing restrictive measures on data flows across member states’ borders.
data storage and e-Estonia’s ‘country without borders’ (e-Estonia, 2015) vision will certainly go against many of its regressionist principles.

In 2008, Mart Laar summed up Estonia’s rise (to date) with two clear lessons. Before proceeding with any arduous economic reforms, take care of politics first; the second, embodying multinational sportswear giant, Nike, he proclaimed: ‘Just Do It’.

“To be successful in the new future, a clear break must be made with the totalitarian past and with the structures and people representing it.”

(Laar, 2008: 69)

This section has highlighted Estonia’s ‘can-do’ attitude in the aftermath of restoring independence and how this still plays a major part in the direction of the country today. The preceding fifty-one years of occupation are often acknowledged as ‘lost time’ (Kattel and Mergel, 2018) and Laar was clear that Estonia had to open up to the world, both skilfully and fast. Decisive economic reforms in the aftermath of regaining independence, along with the ‘shock therapy’ it may have caused, have seemingly been worth it in the long-run.

But in recognising and attesting the many successes Estonia has achieved over the past three decades, we must also recognise its uniqueness given its relative size and lack of political legacy. Many of the ‘crazy ideas’ and technological advancements have been emblematic of its political dexterity as a small state, when other countries are perhaps encumbered by slow, bureaucratic institutions and traditions. When, for example, considering Estonia’s approach towards e-Residency, the Data Embassy, and now developments with a national AI policy, Estonia’s favourable legislative environment has also been seen as a key enabler for many of its technological experiments and achievements over the years (Barbaschow, 2018; Kalvet, 2012).

This has allowed Estonia, as Drechsler (2018) puts it, to position itself as a ‘pathfinder’ as it lays claim to being the, not a, leader in cybersecurity and digital government (see Section 5.3). Today, a parade of senior officials and delegations from all over the world regularly travel to Estonia to learn of its ‘story’ and success in digital government. As such, ‘e-Estonia’, the government’s very own powerful nation-branding strategy, now plays a crucial role in exporting Estonia’s “digital power” (Areng, 2014) to the rest of the world (Jansen, 2012; Tammpuu and Masso, 2018 – see Section 5.3). With the arrival of the Data Embassy, Estonia
now believes it has another story-telling resource to add to its already expansive collection of frames and narratives that surround its post-1991 state transformation.

4.2 Framing the Data Embassy

Having outlined the prevailing storylines of Estonia’s journey to becoming the “most advanced digital society in the world” (Hammersley, 2015), the remainder of this chapter brings the Data Embassy back into focus, tracing the project from its conception and highlighting some of the key hurdles faced by the Estonian government along the way. In doing so, it aims to answer two fundamental questions: what is a Data Embassy and why does it matter to Estonia’s framing of itself as a ‘digital pioneer’?

Is a Data Embassy, as one sceptical academic put it, nothing more than a “hyped-up” (interview 7 - 18/05/18) ICT ‘disaster recovery plan’? Or, does the Data Embassy’s promise of extraterritorial storage for state data and information systems radically alter future state approaches to the public provision and justification of national security? An early definition of the term described a Data Embassy as:

“a physical or virtual data center in an allied foreign country that stores data of critical government information systems and mirrors of critical service applications.”

(Kotka et al. 2016a: 104)

Admittedly, however, this does little to unpack what a Data Embassy actually is, nor what it does in practice.

In this section, I situate the Data Embassy within part of a much wider Government Cloud initiative that the Estonian government has been developing since 2013 (Section 4.2.1). With an increasing reliance on its digital infrastructure, the Estonian government (like many others) has been drawn to the promise of cloud computing. As I argue, however, this became married to growing concerns over data security and the territorial integrity of the state, and a proposed solution emerged that would be situated outside of Estonian territory.

This section will also uncover what the Data Embassy is not. As I illuminated at the beginning of the chapter, the Data Embassy is not actually an embassy. Despite initial intentions to utilise embassy locations around the world, the Estonian government were forced to change tack and utilise a solution that functioned like an embassy instead. Section 4.2.2 traces this journey in detail, offering insight into the

---

29 A Disaster Recovery Plan (DRP) can be considered an integral security component in data centre management for cloud service providers (CSPs) and part of a much wider business continuity plan. In the event of a disaster or emergency, a DRP minimises the effect on normal operations with a goal of rapidly restoring services. I believe the meaning behind the interviewee’s scepticism was to question what made this so unique in comparison to other disaster recovery and business continuity plans enacted by major corporations (such as Amazon and Google) on a daily basis.
decision-making processes of Estonian officials and a number of organisational, legal, diplomatic and technical challenges along the way. In the final section (4.2.3), I examine more recent Data Embassy developments, outlining how issues around Brexit and subsequent diplomatic engagements with an EU partner would lead to the establishment of the world’s first Data Embassy in Luxembourg.

In 2013, Taavi Kotka was sat around a table in the Ministry of Economic Affairs and Communications with fellow civil servants drafting Estonia’s new digital strategy – *Digital Agenda 2020* (MoEAC, 2013). It was during these early discussions, that the idea of a Data Embassy was first floated:

“That was the first time we had it on the board. So I drew a huge mind-map, to understand what are the questions to deal with, and it wasn't called a Data Embassy back then, but it was on the mind map that we might need - how to say? - we might need additional computing power and storage, that is not located, physically, in Estonia.”

*(Taavi Kotka interview - 15/07/19)*

During our time together Kotka reflected candidly about this moment like it was yesterday, even sketching out the layout of the room for me on a scrap piece of paper:

“So in the Ministry of Economy, we had two big meeting rooms. And we were sitting in the smaller one, I was sitting here, there was a screen to lead the meeting, and [Toomas] Vaks was sitting here. I remember that. And we discussed the new national cybersecurity strategy.”

*(Taavi Kotka interview - 15/07/19)*

Providing fascinating insights into some of the everyday practices of the state, from the mind-mapping conversations scribbled over whiteboards to the gradual formulation of integral national policy, such

---

30 At this point in time, Taavi Kotka was the Estonian government’s Chief Information Officer and played a leading role in the development of this strategy. As I highlighted in Section 4.1, the strategy’s aim was to outline, develop and drive forward the country’s national ICT policy across all areas of society, with a number of key priorities in areas of telecommunications, e-governance and cybersecurity. It was here that Kotka played a key role in driving Estonia’s ‘no-legacy principle’ and e-Residency programme, noting that “the aspiration for Estonia is to become as re-known [sic] for its e-services as Switzerland is in the field of banking” (MoEAC, 2013: 3).

31 Reflecting back on these conversations, Kotka in fact credits the title of ‘Data Embassy’ to his colleague Toomas Vaks. At the time, Vaks was a key government advisor and Director of Cyber Security of RIA, the national Information System Authority *(Taavi Kotka interview - 15/07/19).*
conversations also speak to wider concerns and established narratives within the Estonian government at the time regarding the capacity and capabilities of state infrastructure – particularly in the event of an emergency (see Chapter 5). Kotka would go on to write his Master’s thesis on the topic, assessing what kind of computing power and infrastructure a modern-day Estonia needed to fulfil its daily capabilities and growing digital ecosystem (Kotka, 2014). The resulting analysis spoke of a need to implement a Government Cloud concept to meet the growing demands and security needs of the state – and would, in part, explicate the need for a cloud-based solution outside of Estonia’s borders to ensure the ‘digital continuity’ of the state. From here, I argue, the Data Embassy concept was officially born. In the following sections, I trace how these early conversations developed and how the Data Embassy went from early visionary ‘pipe dream’ to an integral part of the country’s overall security strategy in just a matter of years.

4.2.1 Government cloud
As Kotka and Liiv (2015: 150) note, the idea of moving state infrastructure – data, registries, services – to the cloud has received significant interdisciplinary attention in recent years (see, Gleeson and Walden, 2016; Wyld, 2009). At a state level, interest has piqued in cloud computing and cloud-based services, with governments (and even multilateral institutions such as the United Nations and NATO) drawn to reduced public-sector costs and an improvement in availability of data and government services (Robinson and Martin, 2017). Table 2 below illustrates different government policies and approaches to cloud computing in the public sector. Crucially, however, much of the public-sector uptake on cloud-based services has been pretty fragmented so far (with many taking up contracts with vendors such as Microsoft or Amazon AWS – Amazon’s public cloud service).
As the previous section has highlighted, Estonia today is at a point where the preservation and availability of its digital infrastructure is of paramount importance to the continuity of the state. The government recognises that many of its databases, registries and services (e.g. land/population registry and tax databases) only exist in digital form. It is this lack of a paper trail – and the evidential value each register or database holds – that is the cause of great anxiety for the Estonian government (see Chapter 6). As one interviewee

During the Obama administration in 2010, the U.S. government made significant strides in ‘moving to the Cloud’ by moving its ‘Recovery.gov’ system to Amazon AWS, saving it $750,000 in one year (Kundra, 2010). Since then, Amazon has served as the primary vendor for the U.S. government at a federal, state and local level. In 2019, Microsoft was awarded a $10bn cloud computing contract by the Pentagon – known as JEDI (Joint Enterprise Defense Infrastructure) – to store vast amounts of classified data and enhance military/defence capabilities through artificial intelligence (AI).

In 2013, the UK adopted a “Cloud first” policy, aimed at speeding up public-sector uptake of its “Platform as a Service” (PaaS) cloud model (GDS, 2017). The policy is currently under review, with an alternative procurement framework expected to replace its ‘G-Cloud’ online marketplace in due course (Donnelly, 2019). Since 2015, Crown Hosting Data Centres Ltd., a joint venture between the Cabinet Office and Ark Data Centres, has provided data centre space for public bodies to host their computer servers and systems that are not in the cloud.

In February 2018, the Australian federal government and Digital Transformation Authority announced its Secure Cloud Strategy, making it easier for government agencies to move to a public cloud platform. According to Deloitte (2019), 23% ($1bn AUD) of Australian public cloud spending now comes from its government sector.

The Singapore government recently announced that it would be migrating a large proportion of its IT systems to the public cloud – with more sensitive systems moving to a private government cloud. A leader in e-government and digital transformation, Prime Minister Lee Hsien Loong was quoted: “the question for the government is not whether we do it, but to what extent we can use the cloud” (Rohaidi, 2019).

Japan could be seen as one of the earliest adopters of cloud computing in the public sector, after launching the “Kasumigaseki Cloud” in 2009. The Japanese government sought to consolidate government information systems by developing a ‘Government Shared Platform’ (like the UKs PaaS model).

Since 2009, the Estonian government has utilised Amazon AWS (Amazon’s public cloud service), but this only applied to non-sensitive ‘digital assets’ in the form of its tourism website visitestonia.com (Kotka and Liiv, 2015: 150).

The EU’s current cloud computing policy is set within its wider Digital Single Market Strategy, also building on its 2012 European Cloud Strategy. Pooling expertise and funding from across the EU, the policy aims to “promote the development and uptake of cloud services, focusing on certification, switching of cloud service providers and security” (European Commission, 2019).

Table 2 – An overview of different public-sector approaches to cloud computing
told me, “the ID card crisis last year showed us that there is no agency that is ready to go back to pen and paper, it just not feasible” (*interview 13 - 03/10/18*).

Kotka and Liiv point to the certain “idiosyncrasies” or “peculiarities” in Estonia’s digital society – that differentiate the country from many of its European counterparts - as a “mandate” for developing a novel government cloud concept (2015: 150). Due to the rapid digitisation of both the public and private sector, and the aforementioned ‘paperless’ doctrine within Estonia’s public sector, Kotka and Liiv believe that the need for ‘digital continuity’ is fundamentally higher than in most other countries. Furthermore, with Estonia now catering for thousands of e-Residents that rely on Estonian public services and infrastructure, there now seems a greater incentive (from both a financial and reputational perspective) to ensure services remain available at all costs:

“It will make sense as we are able to increase service availability, it will help us to build more reliable services for e-Residents. For example, e-Residents are from all over the world and it will be helpful for them if some services are running in Luxembourg’s data centre or in UK data centre.” (*interview 1 - 09/08/17*)

To tackle this, in 2013, the Estonian government began pursuing its own government cloud concept: The Data Embassy Initiative (Kotka and Liiv, 2015; Kotka et al., 2016a; MoEAC, 2015; MoEAC, 2016). The Initiative consists of three core components:

i) **Government Operated Cloud**: to increase the number of purpose-built, government-operated data centres within Estonia, with the aim of improving the uniformity and maintenance of backups from critical government databases and services.

ii) **Virtual Data Embassy**: to backup ‘non-sensitive’ data to a private company’s public cloud such as Amazon AWS or Microsoft Azure.

iii) **Physical Data Embassy**: to backup critical databases and services to physical Estonian embassy locations or government-operated data centres in ‘friendly’ countries.

Increasing the number of government-operated data centres within Estonia is nothing out of the ordinary; in fact, it is not too dissimilar to other governments’ cloud strategies (see Table 2). During the process of completing this thesis, however, this component was something of a moot feature. To date, there has been no evidence of any government-operated data centres being established within Estonian territory; it seems...
to not be of highest priority right now. Regardless, by virtue of its geography and relatively poor communications infrastructure, Estonia has little data centre infrastructure anyway32. In any event, to solely rely on its internal data centre infrastructure could be a risk:

“Usually our cyber security experts say, to have a proper built information system you need to do backups in at least two different locations. The distance between those two different locations should be around 150km at least. If we take Estonia, 150km basically means one data centre in the West of Estonia on an island [e.g. Saaremaa] – where the internet connection is very bad – and another data centre on the Eastern border [e.g. Narva] which is not acceptable for our security. So, therefore, we have some data centres here around Tallinn as it is our most populated place, and definitely we need to do backups somewhere. No possibility in the East, none in the West, so we’re looking outside.”

(interview 1 - 09/08/17)

Speaking to the archival and infrastructural realities facing the state today, as well as an everyday affective geopolitics and enduring threat posed by Russia, such a response from an Estonian civil servant is incredibly revealing and emblematic of the state-level anxiety I argue Estonia is experiencing later in this thesis (see Chapter 6).

Mentioned in the previous chapter, the Virtual Data Embassy component has so far made up the majority of research in this area (Kotka et al., 2016a; Kotka et al., 2016b; MoEAC, 2015; 2016). Working with private companies’ public cloud services, the Estonian government plans to migrate its so-called ‘digital monuments’ – websites and other non-sensitive resources that hold national symbolic significance – to the cloud. Resources such as Riigi Teataja (State Gazette – the online depository for all Estonian legislation since 2010) or the President of Estonia’s official website (www.president.ee) do not hold sensitive information, but could be significant targets in the event of a cyberattack:

“Image wise, definitely, we have a lot of these monuments […] I would say that, yes, [the] president website is really important. Government office website, this is really important. And there are like 11 ministries together with the president

32 Estonia has no direct link telecommunications link to central Europe, and relies on internet exchanges across the Baltic sea via Helsinki and Stockholm. At present Estonia has 11 data centres (7 located in Tallinn) with no Tier IV data centres. A Tier IV data centre is the most advanced type of data centre, and is built with a high degree of redundancy and fully fault tolerant/resistant – meaning that a Tier IV data centre is less prone to downtime and faults, offering uptime of approximately 99.995%. Although a Tier IV data centre is more advanced than a Tier I, II and III data centre, this does not mean that it will automatically suited for every business (or government) need (Hewlett Packard Enterprise, 2019). Recent plans were announced to build the ‘largest data center in the Baltics’ in Tallinn, at a cost of approximately €100m (The Baltic Course, 2019) – work started in 2020, but it is unclear as to whether this will be a Tier IV data centre.
and there are loads of web pages which could be considered as monument web pages [...] Let's say that somebody starts to spread their, I don't know, God knows what message is, in the context of something, then if it comes from the government web page; and this is especially bad, it is, if the web page is taken over in a way that is not understandable. So it's not defaced. But it's amended in certain areas where it is important not to amend.”

(interview 17 - 29/10/18)

Such concerns, particularly in the context of growing digital misinformation and cyber vandalism, appear warranted, whilst further research on the impact of defaced, distorted or disabled ‘digital monuments’ on public discourse and the perceived authenticity of states would be beneficial in understanding the value of Virtual Data Embassies on a wider scale.

Between 2014 and 2016, the Estonian government conducted two feasibility studies with Microsoft to assess the policy and legal implications of migrating Estonian data and services to its public cloud (MoEAC, 2015; 2016). Legal analysis has shown that amendments to existing domestic Estonian law would be required for “critical” or “sensitive” data and services to be stored in a public cloud (Kotka et al., 2016a: 104), but even so, it is unclear whether this would ever be the intention moving forward due to data protection risks. Post-Snowden, and in an age of increasing data monopolisation and mis-management from large multinational tech corporations (see, the 2018 Facebook-Cambridge Analytica scandal), concerns over storing any government data in a public cloud may be justifiable. As one respondent warned:

“Well, and of course, it doesn’t come without cost, half the digital embassies are supposed to be in clouds, in commercial clouds. In commercial clouds? How can you give your country to Microsoft?”

(interview 21 - 28/11/18)

The Estonian government was keen on a solution that mitigated the risks mentioned above relating to data protection and inadequate data centre infrastructure. As Kotka et al. (2016a: 104) suggest, this may require more than just the preservation of critical databases within Estonia itself: “A solution needs to be developed for situations, admittedly improbable, during which the Estonian state might need to operate some services outside of its current borders.” In doing so, the Physical Data Embassy component of the government cloud was built upon the premise of hosting Estonian data outside of Estonia’s borders, whilst crucially under the control of the Estonian government. The following section explores this novel component in more detail.
4.2.2 From embassy to data centre

In their initial exploratory research and analysis on an Estonian government cloud, Kotka and Liiv (2015) proposed two distinct solutions that would enable state information systems, data, and even e-services, to be housed and operated from outside of Estonian territory. In keeping with the initiative's moniker, the first solution planned to utilise existing Estonian embassy locations across the world in an attempt to improve the regularity and scale of existing backup methods.

Interestingly, the Estonian government has been performing equivalent manual backups of this process for over a decade, with several critical databases backed up onto magnetic tapes, being physically transported (via a diplomatic bag) to Estonian embassy locations on a quarterly basis (interview 1 – 09/08/17 - see Section 5.1). The proposed solution would, therefore, be deemed a pragmatic upgrade on this somewhat inefficient and cumbersome method, with the digital equivalent allowing for near-instantaneous backups or ‘mirroring’ of almost all critical state information systems and databases. In the event of an emergency - be it a large-scale cyberattack, natural disaster or any deemed threat to Estonia’s territorial integrity and political independence - the Estonian government would be able to effectively ‘switchover’ and operate from the extraterritorial embassy.

By utilising existing embassy buildings and infrastructure, it was felt that the Estonian government could pursue several possibilities with regards to securing and protecting its data. For example, Articles 24 and 27 of the Vienna Convention on Diplomatic Relations (VCDR - 1961) were deemed most pertinent, ensuring the inviolability of mission archives and communications. Ultimately, however, the proposed solution had numerous organisational, legal and technical challenges (Kotka and Liiv, 2015). First, embassy locations do not meet the required security specifications for the housing of critical databases and hosting of data, comparable to that of a high-tiered data centre. From being able to operate to a greater level of redundancy, to limitations and vulnerabilities over existing telecommunications infrastructure, or even the level of technical competency found within an embassy, they were deemed unsuitable and even susceptible in the event of a crisis (either within Estonian territory or within the ‘receiving State’ itself). Furthermore, Estonia currently only maintains 38 diplomatic missions abroad. In keeping with the Estonian government’s intention to operate within ‘friendly’ states (Kotka and Liiv, 2015: 157), the scope of Data Embassy locations globally would be somewhat limited (for discussion on future locations, see Section 7.2.1).

The second solution, and the one on which this thesis centres, then emerged as the most viable alternative. Under this proposal, the Estonian government would effectively acquire server space within an existing government-operated data centre outside of Estonian territory; fulfilling the necessary security and technical specifications that the first embassy solution lacked. The Estonian government would then sign a bilateral agreement with the host State, ensuring that the latter would fulfil specific obligations regarding the hosting of Estonian data and information systems. Initially, it was perceived that the Data Embassy
would function on a similar precept to a physical diplomatic mission. A small, demarcated area of an existing data centre (see Fig. 4.4) – conceivably a separate, enclosed room with restricted access (to Estonian officials only) – would effectively be deemed Estonian jurisdiction, whilst similar provisions such as inviolability of the premises and diplomatic immunity would be deemed applicable.

![Figure 4.4](image)

Figure 4.4 – A visual representation of how the Estonian Data Embassy could be situated (and demarcated) within a government-operated data centre, including the use of key-card access (NB: this is the author’s own depiction and does not claim to accurately represent the data centre design – nor is it to any scale).

Although core principles of the Vienna Conventions were indeed applicable, there were still uncertainties regarding the overall applicability of the Conventions outside the context of a diplomatic mission. Broadly speaking, the Vienna Convention concerns the comprehensive protection and inviolability of the staff, premises and communications of an embassy.

Given that its predominant function is to codify the rules for the exchange of embassies (but also the establishment, maintenance and termination of diplomatic relations) between sovereign states (Denza, 2016), there may be consensus that the Data Embassy goes against the overall purpose of the Vienna Convention. This could first be interpreted by the Data Embassy not actually residing within a traditional diplomatic mission itself. Outlined above, the decision to utilise dedicated server space within
existing government-operated data centres ultimately refutes the premise that the Estonian information systems could be protected under the ‘broad church’ of the Vienna Convention - specifically, Article 22 of the VCDR (1961) which ensures “[t]he premises of the mission shall be inviolable”. Although specific text within the Luxembourg bilateral agreement refers to the Estonian server space as “premises”, this is not in direct reference to a diplomatic mission itself as it is not directly recognised or registered as an embassy. Similarly, the Data Embassy also comprises of no staff or personnel (that work directly for the Republic of Estonia) that are involved in its day-to-day functioning, immediately conflicting with another one of the Vienna Conventions’ core principles. Further, a distinct lack of legal precedent in this area would also be of concern:

“Estonia didn’t want to be the first one to test it, because you can’t be sure until it is tested in court […]

[…] we didn’t want to do the project, or build a Data Embassy, on the Vienna Convention as it is at the moment and hope that it will cover the digital means as well. But, when something happens – occupation, natural disaster – and Luxembourg, for example, doesn’t take the information as diplomatic post and the archives of the Estonian Republic and would give them to whoever…like what happened with Estonian gold. So, then we thought that we would put an extra-legal layer on it and do the bilateral agreement, and if we were to do it with other governments as well we would also sign a bilateral agreement.”

(interview 6 - 18/05/18)

As the following section will explore in greater detail, the proposed bilateral agreement with Luxembourg would serve as an ‘extra-legal layer’ that afforded similar powers and immunities to both ‘sending’ and ‘receiving’ state. Its reinterpretation of the Vienna Convention would afford embassy-like provisions to Estonian state data within a small demarcated space within a data centre – how this may (or may not) impact international law in the future will be discussed further in Chapter 7 (see also, Robinson et al., 2019).

4.2.3 Brexit, Betzdorf and bilateral agreements
With the Data Embassy concept beginning to take shape within a much broader government cloud project, the Estonian government began actively looking for partners to implement the data centre solution outlined in Section 4.2.2. Initial prerequisites, according to those working on the project, should ideally include membership to the European Union or NATO, strong diplomatic relations (both with Estonia and the wider international community) and good data centre infrastructure.
During my own early desk research and correspondence with respondents in 2016, it became apparent that the UK was an early contender for the first Data Embassy. In addition to the prerequisites mentioned above, the British government has held strong diplomatic ties with the Estonian government for over a century, and had recently committed to collaborating on digital transformation in the public sector (Cabinet Office, 2013). This was soon corroborated by a number of news reports, including in the *Financial Times* (Jones, 2016), that negotiations were under way. In the same article, however, it was suggested that the decision to open a Data Embassy in the UK was also under threat due to Brexit, and that Estonia was “also in talks with Luxembourg as a result” (ibid). The story was soon picked up by an online security magazine, *Security Week*, that ran the headline:

"Estonia's "Data Embassy" Could be UK's First Brexit Cyber Casualty"

(Townsend, 2016)

The article, slightly blown out of proportion (and centring on extraneous concerns over GDPR post-Brexit), suggested that if the UK was to fall out of favour, then the reason would “likely to be emotional as it is technical” (Townsend, 2016). One British diplomat would later tell me, however, that this wasn’t strictly the case. Pointing to a lack of government-owned data centres in the UK, they also posited that the process was an unfortunate “victim of time” (*interview 25 - 04/04/19*). On the UK side, Foreign Office officials were still pursuing further legal advice and rigour over data protection, whilst for Estonia, a looming EU Presidency may have served as both a distraction and pressure to get things completed. Nevertheless, with the UK position unclear (Brexit or not), it wouldn’t be too long before the rumoured negotiations with Luxembourg were apparent.

![Figure 4.5 - Screenshot of Twitter conversation between Taavi Kotka and Gilles Feith on the morning after the Brexit vote (source: www.twitter.com)](source: www.twitter.com)
On the morning after the 2016 Brexit vote, Taavi Kotka jokingly tweeted that the EU now had ‘1GB of free space’ following the UK’s decision to vote to leave the European Union (see Fig. 4.5). Gilles Feith, CIO of the Grand Duchy of Luxembourg and Director of its government IT centre, soon responded hinting that ‘Luxembourg has nice #datacenters under eu legislation ;)’ - Kotka subsequently 'liked' the tweet. Although this tweet wouldn’t turn out to be the catalyst for the first Data Embassy to be established in Luxembourg, it was an early (albeit understated) indication that both countries were working towards a Data Embassy solution33. Kotka would later tell me that perhaps, on reflection, Brexit was the ‘final nail in the coffin’ and the tweet helped move things along with Luxembourg over the coming months:

“We said, ‘Forget it.’ And then I spoke with Gilles [Feith]...and then with him it took months to finish it. And he understood, definitely. I said, ‘I can’t pay you more than 200, 300K.’ No problem. I won’t do it as a showcase. It probably cost more to him, but by a couple of months, we were up and running. Not physically up and running, but the project itself”

(Taavi Kotka interview - 15/07/19)

As Kotka suggests, things did start to move fast after a somewhat stagnant period of negotiations with the UK. On 16 November 2016, an MoU was signed (digitally) between Estonia and Luxembourg, stating that the concept would be going ahead. By 20 June the following year, Prime Ministers Xavier Bettel and Jüri Ratas (Luxembourg and Estonia respectively) signed a historic bilateral agreement regarding the hosting of Estonian information systems and data in one of Luxembourg’s many high-security data centres. Later that evening, Bettel and Ratas addressed fellow dignitaries at an event commemorating the agreement:

**Bettel:** We sign today a first experience that I am very proud to say will be done in Luxembourg. We now have an e-embassy in Luxembourg with Estonia where we were able to have an agreement between both countries based on trust and friendship, and the competencies that we also have in that field, here in Luxembourg. I am very proud because this is fully in line with our Digital Luxembourg strategy […]

[…] It is a co-operation between two countries and between two administrations, where we were able to have a trust relation in order to have this first Data Embassy, with Estonian data here in Luxembourg. I think it’s a great first step, I’m sure, in projects that other countries will follow.

33 A certain level of public Data Embassy diplomacy between Luxembourg and Estonia would continue throughout the course of writing this thesis – particularly on Twitter (see Fig. 4.6).
Ratas: I agree that we would like to make this Data Embassy and I could say that we had quite a lot of different candidates on the table. I’m very happy that, today, we sign with your prime minister this co-operation between Luxembourg and Estonia. The Data Embassy is very important for us and also for our society. I 100% agree with what your prime minister mentioned: I hope, I really hope that this will be a good initiative for the other states inside the European Union…and why not the rest of the world as well.

(20 June 2017 - Digital Luxembourg, 2017)

Such an ambitious project, according to Bettel, was built upon ‘trust’ and ‘friendship’. I view the decision to establish a Data Embassy in Luxembourg as the formalising of a new kind of diplomacy – with a digitally informed leadership, along with shared economic and security values, the agreement was a signal that the two countries were entering a new era of diplomatic relations via the extraterritorial storage of state data (explored further in Chapter 7). Despite a few reservations over why Luxembourg was chosen – “not knowing the reasoning at all, I remembered that news, and I was thinking ‘why on earth Luxembourg?’” (interview 9 - 28/05/18) – there was a general agreement amongst interviewees that Luxembourg was an ideal partner for the first ever Data Embassy.

An explanatory memorandum between the two governments also noted a number of reasons as to why Luxembourg had been prioritised as a partner for this project (Riigikogu, 2018). Mentioned above, Estonia lacks any high-security data centres of its own within its territory. Luxembourg, on the other hand, has the highest density of Tier IV data centres in Europe, already positioning itself as a data storage leader for large corporations across the continent (Digital Luxembourg, 2019). Geographically located at the centre of the ‘Golden Internet ring’ between Frankfurt, Amsterdam, London and Paris, the country’s superior telecommunications infrastructure also offers extremely low latency and resilience across its colocation network (EBRC, 2019). It is of no surprise, in light of Luxembourg’s agreement with Estonia, that it now sees itself as a ‘hub’ for other governments to begin extraterritorially storing their data within its borders (explored further in Chapter 7). For the last few years, NATO, the European Patent Archives and EU Commission have all hosted their data in a similar way to the Estonian Data Embassy, with Luxembourg ensuring the inviolability of their respective archives (EPO, 2017; MacGregor, 2016; NSPA, 2016). With Monaco looking to potentially follow Estonia’s lead with a Data Embassy of their own (Lambert, 2018), we may also see a flurry of smaller states adopting a similar approach to data security moving forward (see Chapter 7).
As stated, on 20 June 2017, the prime ministers of both the Republic of Estonia and the Grand Duchy of Luxembourg signed a bilateral agreement concerning the hosting of Estonian data and information systems. Although the server racks were yet to be installed, and data was yet to be ‘backed up’, the Data Embassy’s political and legal processes were all but agreed and the world’s first Data Embassy was thus established (see Fig. 4.6). As Section 4.2.2 illustrated, it was deemed necessary for the Estonian government to take additional measures to ensure the data and information systems in Luxembourg were suitably protected under international law. Further to this, it was crucial that additional powers could also be exercised with regards to Estonian jurisdiction outside of its own borders. As there was still a clear lack of precedent within international law, the bilateral agreement between Estonia and Luxembourg serves as the “extra-legal layer” (*interview 6 - 18/05/18*) that would afford similar powers and immunities to both ‘sending’ and ‘receiving’ states (Estonia and Luxembourg respectively).

![Image of Jüri Ratas tweeting about the signing of the bilateral agreement](https://www.twitter.com)

Figure 4.6 – Estonian Prime Minister Jüri Ratas tweeting after the signing of the bilateral agreement between Estonia and Luxembourg (source: www.twitter.com)

In effect, the bilateral agreement between Estonia and Luxembourg laid the foundational structure from which the Estonian government could begin to systematically backup its information systems, databases and registries that are deemed critical to the continuity of Estonia. Located within one of Luxembourg’s high-security, Tier IV data centres in the small town of Betzdorf, the Data Embassy will protect Estonian information systems and data in a similar capacity to a traditional diplomatic mission. Via the bilateral agreement, Luxembourg will agree to protect the inviolability of the separated Estonian server room “in the spirit” of the Vienna Convention (Riigi Teataja, 2017). Despite not being located within a traditional diplomatic mission, both governments have agreed to reinterpret some of the key principles of the VCDR (1961), and, once fully established and operational, the Data Embassy will stand as the first example of two governments agreeing to provide this kind of inviolability.
“The Grand Duchy of Luxembourg shall grant the premises the same treatment as granted to diplomatic missions in respect of its official communications and the transmission of all its documents.”

(Article 6(3) - Riigi Teataja, 2017)

The agreement, containing ten articles, specifies the means for effective cooperation, support and operations regarding the premises of the dedicated Estonian server room in the data centre, whilst also governing the legal status of the premises, guaranteeing the necessary immunities and privileges on the basis of existing national and international law (Kask et al., 2018). The afforded inviolability would mean that no Luxembourg officials would be able to enter the Data Embassy or access the data without the Estonian government’s approval – as is the protocol that exists within a traditional embassy. Crucially, the agreement is referred to be operating ‘in the spirit’ of the VCDR, and, although such wording is commonplace throughout international agreements today, the agreement’s preamble deliberately emulates aspects of the Vienna Convention through similar language, semantics and structure. Despite this, and to avoid conflation with the Vienna Convention, the agreement refrains from using the term ‘Data Embassy’ in any capacity. Although there was clear intent to reflect the Convention, Estonian officials believed this to be problematic from a semantic and legal perspective (see Section 7.2.2).

Significantly, the bilateral agreement was then ratified by both respective parliaments (21 March 2018 in Estonia). The process was more than a symbolic MoU signing (which are extremely commonplace and generally not legally binding), and was debated and passed within both state executives. Moreover, this would be the first time two states have ever agreed to provide this kind of inviolability - for Luxembourg, they are providing certain privileges and immunities akin to that of an embassy, whilst for Estonia, they are extending the ability to exercise their powers of jurisdiction outside the traditional diplomatic mission. Uncertainties still remain over how certain immunities will be upheld, particularly over communications in the event of a DDoS cyberattack. However, as mentioned above, Luxembourg has already entered similar agreements with other international organisations and believes a precedent has now been set with regards to providing immunity outside of a diplomatic mission.

Full details of the Data Embassy’s technical specifications and architecture are, due to sensitivity, scant at present. During initial trial periods in early 2018, it was indicated that four databases would be backed up on a trial basis: State Gazette, Land Register, Business Register and e-File (Liive, 2018). Once fully operational, however, ten critical databases are expected to be backed up to the EBRC Betzdorf data centre. These are:

1. State Gazette (Riigi Teataja)
2. Population Register
3. Register of Citizen’s Identification documents
4. Estonian Geoportal information system
5. Land Register
6. Business Register
7. Information system of State Budget
8. Register of Social Security
9. Criminal Register and e-File (online information system for criminal proceedings)
10. E-Tax Register

Each critical database forms an integral part of Estonia’s X-Road infrastructure (see Section 4.1.2) and, in keeping with its decentralised architecture, responsibility is given to each database owner to maintain its overall security. In much the same way, each database owner or government ministry will be given the responsibility of ensuring its data is securely encrypted and backed up in the Data Embassy in Luxembourg.

The initial plan is to store copies of existing databases in an effort to continuously backup the data, but the planned end-goal is to improve the frequency of the backups and to facilitate a ‘mirroring’ of critical Estonian infrastructure and e-services in the event of an emergency:

“Our next phase would be that we could do data recovery or even a secondary site that you can run your services from. So, the idea that maybe even if there is no takeover of the country, but just the large-scale cyberattack, then we could switch it over to somewhere else and can run our services day-by-day without any hitch.”

Whether or not the Data Embassy reaches this ultimate goal depends on a number of factors, not least the success of the project’s first phase and the financial viability of hosting an entirely mirrored, extraterritorial digital ecosystem from a Data Embassy in one or maybe multiple locations around the world. In terms of initial financial allocations, the Estonian government has budgeted approximately €1 million for the project, with Luxembourg being paid between €200,000-300,000 per year to host its information systems and data. Such costs will rise exponentially if Estonia decides to build any more Data Embassies in the future.

---

34 This is in line with the government’s own mandatory three-level baseline ICT security standard across the public sector (ISKE). Adopted in 2003, ISKE is based on a German information security standard, IT Grundschutz. ISKE is a three-level baseline security system, meaning that every information system or database is measured and assigned on a three-tier security system (Low → Medium → High). In 2008, ISKE became obligatory for state and local government institutions that use databases.
Over the course of writing this thesis, the Data Embassy has progressed from nothing more than an early ‘moonshot’ proposal between two government colleagues, to the opening of the world’s first Data Embassy in Luxembourg in 2018. When the project was a mere blueprint, little did Taavi Kotka and his team know that the first Data Embassy would be opened in Luxembourg only a few years later. The process is emblematic of the government’s ‘startup’ approach (see section 5.3), where the country’s political dexterity and ‘can-do’ mentality means that projects like the Data Embassy are able to get off the ground at such speed and scale. At the time of writing this thesis, the Data Embassy is still very much in its beta-phase, meaning that the initial project in Luxembourg serves as the ‘guinea pig’ before any future decisions are made on ‘scaling up’. As such, it could be some time before we see a network of Estonian Data Embassies emerge across the globe (see Fig. 3.3).

As with other pioneering startups, it wasn’t long before others began to sit up and take notice of Estonia’s innovative Data Embassy solution. As one government official told me, it wouldn’t be long before several countries followed suit – with many contacting Estonia shortly after the Data Embassy was publicly announced, to see if they could strike similar agreements (interview 6 – 18/05/18). Highlighted above, officials from Monaco have been the first to publicly announce that they are planning to host their data in a similar fashion in Betzdorf, Luxembourg. In terms of future research, despite Estonia instigating the Data Embassy concept, this has now become just as much a story about Luxembourg, and it will be interesting to trace how the country potentially positions itself as a Data Embassy ‘hub’ – or perhaps ‘haven’ – for other countries in the future (see Chapter 7).
<table>
<thead>
<tr>
<th>Date</th>
<th>Key Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013</td>
<td>The Data Embassy idea is first discussed during meeting between Taavi Kotka and government advisor Toomas Vals during the formulation of the <em>Digital Agenda 2020 for Estonia</em> (MoEAC, 2013).</td>
</tr>
<tr>
<td>February/March 2014</td>
<td>Russia unlawfully annexes Crimea – leading to further instability and conflict in eastern Ukraine.</td>
</tr>
<tr>
<td>2015</td>
<td>Publication of key concept paper from Taavi Kotka and Innar Liiv ‘Concept of Estonian Government Cloud and Data Embassies’ (2015), followed by joint-research project with Microsoft (MEAC, 2015).</td>
</tr>
<tr>
<td>23 June 2016</td>
<td>The United Kingdom votes to leave the European Union. Negotiations between Estonia and Luxembourg over first Data Embassy begin to advance in the following days.</td>
</tr>
<tr>
<td>16 November 2016</td>
<td>Memorandum of Understanding (MoU) signed digitally between Luxembourg Prime Minister Xavier Bettel and Estonian minister Kristen Michal stating Data Embassy will go ahead.</td>
</tr>
<tr>
<td>20 June 2017</td>
<td>Bilateral agreement signed in Luxembourg between Prime Ministers Xavier Bettel and Jüri Ratas regarding the hosting of Estonian data and information systems.</td>
</tr>
<tr>
<td>2018</td>
<td>Estonian officials begin process of ‘building’ the Data Embassy inside of the data centre in Luxembourg. This involved the instalment of sever racks, cabinets and other general infrastructural technologies.</td>
</tr>
<tr>
<td>20 February 2018</td>
<td>The bill to ratify the agreement passed its first reading in Riigikogu (Estonian parliament).</td>
</tr>
<tr>
<td>21 March 2018</td>
<td>The second reading of the bill regarding the hosting of Estonian data and information systems is passed and thus adopted.</td>
</tr>
<tr>
<td>26 March 2018</td>
<td>The president declared the bill to be published in Riigi Teataja – this was completed on March 29th 2018.</td>
</tr>
<tr>
<td>April 2018</td>
<td>Data is reportedly backed up to Luxembourg for the first time on a trial basis.</td>
</tr>
</tbody>
</table>

Table 3 – A timeline of key events in the development of the Data Embassy
4.3 Conclusion

Estonia’s transformation over the last three decades to one of the most advanced digital societies in the world has been an extensive, ad-hoc and ongoing process. In this chapter I have highlighted the complex and multifaceted nature of this transformation, but also how the decision to establish a Data Embassy cannot be easily deduced to a single policy or historical ‘moment’ since the restoration of independence in 1991. Rather, by introducing a number of prevailing narratives and storylines – Estonia in transition/restoration; Estonia and the exceptional/existential (e.g. ‘wakeup calls’ in 2007 and 2014 – see Section 5.2); and Estonia as a digital pioneer – I have examined how the Data Embassy has been framed as part of Estonia’s wider ‘geopolitical culture’ (Toal, 2017) that aims to accentuate and often sensationalise notions of resilience, creativity and trust in order to thrive post-independence.

As Section 4.1 explored, this transformation was first characterised by an intense period of risk-taking and ‘crazy ideas’ largely spearheaded by Prime Minister Mart Laar, President Lennart Meri, and e-government visionaries Linnar Viik and Toomas Hendrik Ilves (the latter becoming president himself in 2006). In many ways, the transformation was driven by a desire to open up and compete with the West, but also to shake off its Soviet legacy in the process (Kattel and Mergel, 2018). It was the adoption of a Scandinavian governance model in the intervening years post-independence that may have certainly played a significant role in Estonia’s shift from an analogue society to a digital one (see Chapter 5). Another key moment in this journey came in 2004 when Estonia joined the European Union and NATO. Whilst the country didn’t change overnight, Estonia’s role in both alliances has undoubtedly led to periods of greater economic prosperity and ontological security. Echoing the words of Mart Laar earlier in the chapter, Estonia’s pivot from east to west does now appear to be irreversible.

Throughout the 2000s, Estonia oversaw perhaps the most significant period of transformation, and I point to a ‘conveyor-belt’ period of technological innovation and development – from the introduction of X-Road (2001) and an ID card (2002) to the development of internet voting (2005) – as pivotal in this regard. Such developments have arguably laid the foundational bedrock of Estonia’s digital society, without which I believe technological innovations such as the Data Embassy would not have emerged. The cyberattacks that targeted the country in 2007 may also be seen as a critical juncture in this story, subsequently improving cybersecurity maturity and awareness (see Section 5.2).

In summation, however, it would not just be one of these individual policies, technological innovations or political ‘moments’ that would lead to the establishment of the Data Embassy. Rather, it appears that a combination of these factors over the past three decades have led to an almost ‘perfect storm’ from which Estonia’s digital society has developed to be both simultaneously infallible yet fragile; as the Estonian government stresses its need to preserve its databases and infrastructure that it now so heavily relies upon.

In the following empirical chapters, I aim to delve a little deeper into the motivations and affective
responses produced by the Data Embassy, examining how certain practices of the state – from archiving to an ongoing difficult relationship with Russia – perhaps point to an anxiety at its centre.

In this chapter I have also introduced the Data Embassy concept in more detail, tracing the project from its conception and highlighting some of the key challenges and milestones faced/met by the Estonian government since 2013 (see Table 3). By doing so I have attempted to shine a light on some of the dynamic and performative practices of the state (Mountz, 2007) as the Data Embassy went through its own period of transformation. As highlighted in Section 4.2, the central challenge to the Estonian government was the decision around whether existing embassy locations could be used for backing up critical databases and services. Fortunate to document such challenges alongside the development of my own thesis, I examined how the Estonian government pursued alternate strategies and how ongoing political uncertainties (such as Brexit) led to the Data Embassy being located in a government-operated data centre in Betzdorf, Luxembourg.

In response to the earlier suggestion that the Data Embassy is nothing more than an overhyped Disaster Recovery Plan, it may be the case (at least technologically) that the Data Embassy is nothing out of the ordinary (for example, many large technological corporations, such as Amazon and Google, host data in overseas data centres with similar business continuity plans in place - in short: what makes the Estonian case so special?). However, in revealing what the Data Embassy is not, in this section I have also outlined the significance of the Data Embassy for scholars interested in emerging themes around geopolitics, diplomacy and international law (e.g. data sovereignty, extraterritoriality and virtual embassies/states). I return to this in Chapter 7, by examining the theoretical and practical implications of the Data Embassy upon such conceptualisations in a twenty-first century context.
Figure 5.1 – A pivot from East to West? An image from ‘downtown’ Tallinn where the modern business district stands in sharp contrast to the city’s existing material Soviet architecture (author’s own image)
Chapter 5 – Cloudy Geopolitics

Commenting on the Data Embassy in a recent podcast for POLITICO, Estonian President Kersti Kaljulaid appeared to confront the somewhat simplistic trope that the Russian threat was front and centre in the government’s decision to begin extraterritorially backing up its state data and information systems outside of its own borders:

“I’m always very angry when people say this is a preparation for losing geographical independence. It is not at all. It’s a normal security measure that I think every country nowadays should take.

Because everybody has digital registries and they should actually make sure they have copies which are time-stamped so that you would always know which copy of your state is the right copy at the particular moment in time. It is a wonderful project between Estonia and Luxembourg, another small and quite flexible country – because it is small, it can be as flexible as we are. This is something which I would advocate every country - while it is taking technology more into account in providing public sector services - should actually consider doing.”

(POLITICO, 2018)

Kaljulaid’s reflections are emblematic of the tensions and inconsistencies that have existed around the Data Embassy since its conception in 2013. On the one hand, initial government discourse invoked existential concerns over territory loss and state continuity in light of ongoing events in Crimea and Eastern Ukraine (MoEAC, 2015). On the other, we have since seen a government narrative develop that centres around a sense of pragmatism – one that ultimately downplays the Russian threat and instead builds on a practical business case that ‘every’ state should logically follow in the twenty-first century. The Estonian government stresses that its overarching aim is to ensure the “digital continuity of the state” (MoEAC, 2015) – but is there more to it than meets the eye?

Delving deeper into these tensions that exist around the Data Embassy and Estonia’s digital society more broadly, this chapter aims to better understand what primary motivations are behind the Estonian government’s decision to begin extraterritorially storing its data and information systems outside of its own borders. Are we able to simply determine, like many in the media have done, that Russia and the provocative actions of its leader Vladimir Putin, are the sole motivation for such a radical step change for the Estonian government? Or perhaps we are able to view the Data Embassy as the next vital cog in Estonia’s enticing nation branding strategy that positions the country as the innovative and forward-thinking digital pioneer? This chapter argues that there is a great deal of inconsistency in the message deployed by the Estonian
government, and that the overall motive has been intentionally ‘cloudy’ in order to manage the state’s geopolitical culture and narrative around the Data Embassy.

Drawing on ethnographic engagements and discourse encountered during the completion of this research, I point to three distinct motivations and accompanying narratives that shape the Data Embassy:

1) a logical business case and model that any country should follow in a digital age (*Section 5.1*);

2) a rational response to an ever-present Russian threat (*Section 5.2*); and

3) yet another innovative solution or ‘crazy idea’ (see *Chapter 4*) that helps to crystallize Estonia’s image as an e-government and cyber security pioneer in the twenty-first century (*Section 5.3*).

The chapter begins with the story and narrative that those in government (or close to the project) often shared with me (*Section 5.1*). This ‘government line’ – positing the Data Embassy’s logicality as “something which you need to do anyway” (*interview 17 - 29/10/18*) when your country is highly dependent on its information systems and digital infrastructure – was at odds with media and initial government discourse that centred on ongoing tensions with Russia and events in Crimea. In this section I draw on Estonia’s sense of ‘pragmatism’ with regards to the Data Embassy and how its emergence can be traced alongside the country’s own shift from analogue to digital practices, especially in the public sector.

In *Section 5.2*, I address the Russian threat itself and whether this has played a critical role in the emergence of the Data Embassy. By first drawing on historical and contemporary security discourses between Estonia and Russia, I highlight how a continued difficult relationship has potentially contributed to an “ingrained belief” (Hammersley, 2015) that Estonia’s sovereignty and independence may once more be under threat. I then consider the emergence of the Data Embassy alongside two recent flashpoints – the 2007 cyberattacks against the Estonian state and 2014 annexation of Crimea – arguing that they served as significant wakeup calls to the Estonian government over future data and cyber security practices. Assessing the likelihood of Russian interference, both conventionally and in cyberspace, the section concludes by asking whether the Russian threat is simply hyperbolic, or whether the Data Embassy does in fact serve a deterrence purpose for the Estonian government.

In *Section 5.3*, I examine how the Data Embassy has been packaged, marketed and sold as part of Estonia’s wider nation branding strategy. Focussing first on the country’s efforts to rebrand itself post-independence, I trace how Estonia moved from a perceived post-Soviet backwardness to becoming recognised as one of the world’s most digitally advanced societies in the world today. Here, I question whether the Data Embassy’s emergence is simply another ‘crazy idea’ (see *Chapter 4*) for boosting its reputation as a digital pioneer, or whether it plays a crucial role in managing anxieties relating to Russia. Second, I critique the
Estonian government’s professed startup mentality, assessing whether its somewhat improvisatory approach to the Data Embassy may have damaging consequences for the state further down the line.

5.1 Pragmatism for the digital age
The Data Embassy entered wider public discourse surrounded by alarmist headlines that centred around the existential crisis facing the Estonian state in the face of the ‘Russian threat’ (see Chapter 3). I believe this shaped my own early preconceptions around the Data Embassy, but over the course of completing this thesis, the intrinsic value of the Data Embassy for the Estonian government in a digital age was frequently brought to my attention. In this section, I draw empirically from the narrative and discourse shaped largely by those who are close to the project, and explore its “completely rational non-anxiety-driven business case” (interview 10 - 31/05/18) in greater detail. In particular, I focus on how the state’s shift from analogue to digital practices during the late 1990s and early 2000s, enabling a greater dependency on the state’s digital infrastructure and archives, may have facilitated the Data Embassy’s emergence.

5.1.1 Archiving the state: analogue to digital
For many countries around the world, the vast majority of archival records still exist in paper form. From birth certificates to land cadastres, many major cities will have vast cavernous spaces (normally underground) with shelves packed full of analogue government records. The Swiss Federal Archives in Bern, for example, currently administers over 60 linear kilometres of archival records – a figure that is growing by 1.5km a year (SFA, 2019). As Elizabeth Yale (2015: 333) writes, archives are seen as “crucial sites for the exercise of political power”, but they play an equally integral role in shaping national memory and identity (Featherstone, 2006). When, for example, Kuwait’s national archives went missing in the wake of Saddam Hussein’s 1990 Iraqi invasion, it not only brought to light the precariousness of the analogue archive (Cox, 2012; Montgomery, 2015), but also denied the Kuwaiti government and its citizens “access to the evidence of their existence as a community within a sovereign state […] while fighting false proclamations and irreplaceable losses” (Al-Alawi, 2017: 4). In light of the UK’s recent Windrush scandal, we might also reflect upon attempts to destroy or ‘conceal’ the archive in an attempt to palliate colonial legacies1 (Sato, 2017; Vargha, 2018).

But the way in which archives are being captured, preserved and made accessible by states is changing within a digital age. Increasingly, states are administering extensive digitisation measures for historical analogue archives, whilst catering more and more for the storage and preservation of ‘born digital’ records. Archivists are quick to point out, however, that the long-term preservation and management of such digital records are still not without challenges, with major concern over policy, legal and technical issues (Bailey, 2007; Barata, 2006). Indeed, as we begin to see more large-scale, state-level processes of digitisation,

---

1 This speaks to an important body of work that has focussed on the imperial/colonial archive (see, Craggs, 2008; Duncan, 1999; Richards, 1993).
how are we to mitigate against digital archives from becoming inaccessible, rendered illegible, or “obsolete by the pace of innovation in information technology” (MacLean and Davis, 1999: 11)?

Arguably for Estonia, a conversation around the preservation of digital records started much sooner than most. Some interviewees reflected on the difficulties faced at the beginning of the 1990s and how, after restoring independence, issues around assigning citizenship and land ownership remained:

“You’re freed from occupation. Now how do you know who is Estonian and who is not?”

(Taavi Kotka interview - 15/07/19)

Relying largely on “old church books and records” (interview 6 - 18/05/18) the restored Republic prioritised giving land back to old landowners as it attempted to rebuild the country from scratch – but how would this work in practice today? As Lorraine Kaljund notes, “The paper-based archives that facilitated the restoration of the Republic of Estonia in the early 1990s simply no longer exist in contemporary Estonia” (2018: 8).

To better understand why this is the case, it is important to reflect upon the journey taken by Estonia following the restoration of independence. Key to a move from analogue to digital practices was the adoption of a Scandinavian governance model - and the creation of a population database and national identity system (isikukood) – which placed gradual emphasis on technology and the unreliability of paper-based archives (see Chapter 4). The gradual process of digitisation that ensued throughout the 1990s, built on principles of efficiency and frugality, culminated in the implementation of a paperless governance policy in 2000, and led to nearly every government service becoming digital by default (OECD, 2018). For its time, operating a highly sophisticated, ‘paperless’ digital society did herald many benefits, but the Estonian government was cognisant of the fact that inherent risks and challenges arise when there is a greater dependency on its information systems and digital ecosystem. As the previous chapter pointed out, critical databases such as the land and population registries now only exist in digital form, and a realisation that, in a time of crisis (e.g. cyberattack, natural hazard or military occupation), vast quantities of Estonian archives and records are at risk of being wiped, altered or held to ransom. Such “archival realities” (Yale, 2015) still rang true during many of my interviews as respondents reminisced over the early 1990s (regardless of their age) and the possibility of having to ‘return to paper’ in the event of an emergency.
Since 2005, the Estonian government has taken bold steps to alleviate such worries by beginning to store ‘cold’ backups² of critical databases and registries in Estonian embassies across the world (see Section 4.2). To briefly recap, on a quarterly basis, the Estonian government has been backing up its core databases and registries onto magnetic tapes³, placing them in a diplomatic bag, and transporting them to Estonian embassies as ‘diplomatic mail’.

“So, basically, we will make backups of critical registries. We will wrap them in magnetic tape. Put those magnetic tapes in suitcases. Take those suitcases to Foreign Ministry of Affairs. Foreign Ministry of Affairs take those suitcases to their physical embassy.”

(interview 1 - 09/08/17)

Intended for the “confidential conveyance of documents between a government and its mission abroad”, the diplomatic bag has been used by states for centuries (Nelson, 1988: 494). Taking many different forms (briefcase, suitcase, duffel bag, cardboard box or even shipping container), the diplomatic bag can contain all manner of diplomatic documents or articles, but may only contain those intended for official use. Under Article 27(3) of the Vienna Convention on Diplomatic Relations (VCDR – VCDR, 1961) the diplomatic bag “shall not be opened or detained” by a host state, and thus its contents shall remain inviolable (Denza, 2016). For the Estonian government, this meant that the hard drives could be transported to Estonian embassies without fear of them being tampered with or intercepted. Article 24 of the VCDR also states that, “[T]he archives and documents of the mission shall be inviolable at any time and wherever they may be” (VCDR - 1961), meaning that the tapes would be protected within the mission.

There is no publicly available evidence to show that other countries have attempted ‘cold’ backups in this way as a means to safeguard valuable digital data in overseas embassies⁴. The British Foreign and Commonwealth Office (FCO) has stated that some archives have been held outside of the central archive “at overseas posts”, but these are likely to be analogue records and thought to be of routine management, finance or consular interest (FCO, 2013). We may, however, be able to draw historical parallels with the use of overseas diplomatic missions as archival sanctuaries during the Second World War, as numerous governments, including Czechoslovakia, Norway and Poland, were forced into exile by Nazi Germany and

² ‘Cold’ backups refer to offline backups that are performed whilst a database or system is offline. Although they are not used for continuous 24/7 backups (i.e. a ‘hot’ backup), they hold advantage in that they are immune to power surges and accidental overwrites and deletion (Rouse, 2016).
³ Magnetic tapes have historically been used for electronic data storage, primarily due to their “high capacity, low cost and long durability”. Whilst it may have been superseded as a primary backup storage solution (e.g. disk or cloud storage), it still has value in industries such as oil and gas that use tapes to “capture, transport and store valuable data” (Rouse, 2018).
⁴ It has been challenging to find evidence of states currently using embassies for backups of digital or analogue records, presumably for reasons of national security. We may be able to assume that some states use embassies in this way, but not on a scale similar to Estonia in the example above.
sought refuge in London (Jakubec, 2019). Diplomatic historian Martin Brown (2006) writes of how, in the immediacy of a Nazi Germany invasion in 1939, Czechoslovak intelligence officers transported papers and records to London for safety. As the story of Ernst Jaakson and August Torma illuminated in Section 1.1, embassies are not only symbolic representations of the state in an overseas territory, but can also serve as protective shelters for diplomatic archives and precious artefacts for states under threat of persecution or loss of political independence.

The physical backups made by the Estonian government are of importance to this research as they tell us that the government held deep concerns over the security and preservation of its most critical databases as early as 2005. This proactive approach, predating the 2007 cyberattacks, shows that the issue of continuity with regards to state records and archives mattered prior to any real form of political provocation post-independence (see Section 5.2). In this thesis, I argue that such an approach illustrates a deep-seated anxiety over preservation of Estonia’s archival records (both analogue and digital) that is embedded in the state’s collective memory (see Chapter 6). For Taavi Kotka and the government, this approach simply made “sense”, with backups becoming “the most effective method of protecting data from being lost” (MoEAC, 2015: 1). In truth, however, the process of continually backing up state archives and transporting them to embassies was risky and a little burdensome:

“We had a capacity issue there. The transfers were done using tapes and big briefcases, and actually was very sensitive things to be carrying it to an embassy. And we have so little staff and resources to spend on travel - this is not sustainable. So the interest was there to find creative ways to communicate data to embassies.”

(interview 26 - 21/05/19)
The introduction of a Data Embassy almost a decade later could, therefore, be considered such a ‘creative’ solution. Furthermore, it was considered by many in the Estonian government as a sensible, pragmatic upgrade on a previously inefficient and laborious method:

“So we were already doing backups of data onto magnetic tapes before then on hard drives. So, you know, that’s always been a part of the plan. I wouldn’t even be surprised if other countries did this too. Even the fact that we store them in embassies, it’s kind of already a realisation of ‘hey, we already use embassies for moving data’.”

(interview 10 - 31/05/18)

Representing its digital equivalent, the use of a Data Embassy over the conveyance of magnetic tapes allows for near-instantaneous backups over the public internet without the costly, logistical drawbacks associated with physical transportation. Alluded to in Section 4.2, to ensure an extra layer of security, all data and communications sent between Estonia and the Data Embassy will be encrypted at source (by each government ministry). To use an analogy, we might wish to envisage the encrypted data travelling between Estonia and the Luxembourg Data Embassy in a similar way to which diplomatic cables have been traditionally exchanged between embassy and foreign ministry – or even the use of a diplomatic bag for analogue data. As the bilateral agreement signed between Estonia and Luxembourg states, in whichever format the information is carried, including through the cables in encrypted form, they will be considered the archives of Estonia (Riigi Teataja, 2017) – thus mirroring the use of the diplomatic bag for magnetic tapes and the protection afforded by the VCDR. Future iterations or ‘phases’ of the project hope to include ‘hot’ backups, which would mean that databases and Estonian e-services could be ‘mirrored’ to the Data Embassy itself and ensure that a near-instantaneous backup could take place (interview 4 - 17/05/18 – see Section 4.2.3).

Beyond mitigating the obvious logistical headache for the Estonian government, the Data Embassy solution outside of Estonia’s borders may also herald many financial benefits in the long term. It was made clear to me on a number of occasions that any Data Embassy solution or agreement (e.g. with Luxembourg) would be a lot cheaper than trying to host such services in government-operated data centres within the country:

“We don’t have big data centres here in Estonia. To build a Tier IV class data centre here in Estonia would cost enormously. In order to provide the same kind of service for other governments, they probably won’t be that interested in, so it is not a business case to build that kind of data centre here.”

(interview 6 - 18/05/18)
Similarly, any attempts to retrofit a room (or “broom closet” – interview 28 - 17/07/19) within an existing embassy would also prove costly and have less operational security (see Section 4.2):

“If you would use a regular network, and you would develop those data centres under the basements of embassies, then still you have a certain level of SLA [Service Level Agreement] which you need to deliver. And it’s way more expensive than renting some sort of a rack in [an] already existing place.”

(interview 17 - 29/10/18)

Thus, given the relative inexpensiveness of hiring dedicated server space within a Luxembourgian data centre (see Section 4.2.3) in comparison to building a Tier IV data centre in Estonia, or retrofitting a room within an existing Estonian embassy, the plan to establish a Data Embassy within a pre-existing space (with the required technological infrastructure) was considered the most prudent and economically beneficial to the Estonian government.

To briefly conclude, this section has explored the pragmatic business case often stated by the Estonian government for the Data Embassy in a digital age. Indeed, as many respondents outlined, the solution does make ‘sense’ given the country’s dependency on its information systems. Crucially, however, this hasn’t always been the government position, with early discourse from 2013 onwards framing existential logics around territory and the Russian threat as key to the Data Embassy’s establishment (see Section 5.2). As the remainder of this chapter explores, I believe this revision in strategy has been preferential for the Estonian government as it seeks to distance itself from, and play down, the purported existential threat posed by Russia. As one interviewee concluded:

“There is also the general argument that any country should be doing this sort of resilience […] so I wouldn’t say it’s accurate to say ‘the only reason we’re doing this is because we think we’re about to be invaded’. You know, we think it’s prudent for any country.”

(interview 10 - 31/05/18)

In the following chapter, I examine how this sense of pragmatism may also be entangled in a deeper post-Soviet geopolitics and collective memory regarding the archive and preservation of state infrastructure. Reflecting further on many of Estonia’s “archival realities” (Yale, 2015), I suggest that the Data Embassy’s
emergence may be rooted in an anxiety that is embedded in the performative practices (and psyche) of the state.

5.2 Paranoid about Putin?

“You know our national enemy is the bears across the border. I would say that of course it could come from something else, but Estonia has been relatively remote to the ISIS threat and many other global highlights, so I would say that Russia is the number 1 [threat] and the number 2…and the number 3, probably.”

(interview 9 - 28/05/18 – own emphasis added)

In this section, I examine the perceived Russian threat and the role it has played in the development of the Data Embassy. As I alluded to at the beginning of this chapter, the narrative around Russia and the Data Embassy has remained inconsistent during the completion of this research. This narrative was first situated across media and initial government discourse (with the latter referring to Russia in everything but name), before a noticeable shift led to the project being framed simply as a rational, pragmatic solution for any twenty-first century digital society (see Section 5.1).

As I argue in this chapter, this may be emblematic of attempts by the Estonian government to deflect or play down the role of Russia in relation to the Data Embassy. Such a variation in narrative and message was also detected during interviews, where the subject of Russia - either in relation to the Data Embassy or Estonia’s foreign policy more broadly – was met with a sense of uncomfortableness by some:

“But yeah, regarding to Russia, we don’t want to stress that we build data embassies because of [a] fear of Russia. This is something we don’t want to stress. But definitely it’s there, it’s behind there.”

(interview 1 - 09/08/17)

Such views, of course, did fluctuate depending on who I spoke to and what role (or previous role) and experiences that individual had. As the quote at the beginning of the section shows, there were individuals who were all too happy to share their views on Estonia’s foreign policy and relationship to Russia. Significantly, this led me to think more critically about the role of Estonia’s near-neighbour and the narrative that was being shaped in relation to the Data Embassy. Is it a little simplistic or naïve to suggest that the sole driving force behind the Data Embassy is the threat of Putin’s Russia? Furthermore, what role (if any) does Estonia’s troubled history and memory of occupation play in the formation of the Data Embassy?
In this section I attempt to address this conflicting message and to understand the role of Russia within historical and contemporary Estonian security discourse. First, I situate the Data Embassy against an uneasy backdrop surrounding occupation and fluctuating tensions between Estonia and Russia since the breakup of the Soviet Union in the 1990s (Section 5.2.1). Next, I analyse two important flashpoints – the 2007 cyberattacks and 2014 annexation of Crimea – and question what role they may have played in the development of the Data Embassy (Section 5.2.2). Finally, I question whether the Russian threat can be seen as largely hyperbolic, or whether the threat facing the Estonian state is visceral for its government with the Data Embassy thus serving as a vital deterrence measure in the twenty-first century (Section 5.2.3).

5.2.1 ‘It might happen again'
Estonia has spent a majority of the last 800 years between a number of feuding empires. From the Danish and German conquests during the Livonian Order in the thirteenth century, to falling under subsequent Swedish and Russian rule in the sixteenth and eighteenth centuries, Estonia has stood, both geographically and strategically, as an important gateway between East and West. Punctured by a ‘national awakening’ in the middle of the nineteenth century, Estonia finally declared its independence in 1918, in the aftermath of World War I and the collapse of the Russian Empire, only for it to be snatched away once more in 1940 by the Soviet Union (see Section 1.1).

It is of no surprise, suggests journalist Ben Hammersley (2015), that even after regaining independence in 1991 there is still the “ingrained belief” that they’re destined to become part of an empire again at some point. Whilst it may be difficult to prove, or indeed locate with any given certainty, where such beliefs are held or felt, this was still a viewpoint casually shared by some Estonians I would speak to:

“If you look back through the history of Estonia, and if you know that history often goes in circles, then you probably feel that it might happen again at some point […]

[…] It is still in the back of the head of our people.”

(interview 6 - 18/05/18)

Upon completion of this thesis, the Republic of Estonia will have held independence for precisely the same amount of time it had lived under occupation (fifty-one years). For that reason, it comes as no surprise that the issue of independence is still widely discussed by many. This has undoubtedly intensified post-Crimea: often flamed by international media discourse, but also entangled within a much darker cultural and political memory that shapes Estonian society, identity and policy (Trimbach, 2017). Estonian historian Marek Tamm acknowledges how Estonian national history and collective memory is predominantly viewed
through the enduring logic of “losing and gaining liberty” (2008: 505), and it is clear that such a logic is prevalent in contemporary Estonian security discourse today.

It is often the case today that any Estonian security discourse or framed threat towards Estonia’s sovereignty is inclined to emanate from its eastern border. As one interviewee told me, it is clear that over “the last 400 years […] the threat has always been coming from one direction. It’s as simple as that” (interview 20 - 27/11/18). Whilst this statement is not strictly true (as noted above, both German and Swedish rule have previously been imposed on Estonia), it does point to a geographic predisposition to frame and conflate any Russian threat today with a Soviet past. Such a tendency is prevalent across contemporary Western discourse and policymaking (Carpenter, 2018) but perhaps also “indicative of a threat perception that confuses Soviet and post-Soviet, conflating Russia with the USSR and casting everything Russian as a threat”5 (Jæger, 2000: 24).

Estonian political geographer Merje Kuus (2002) has written candidly about the framing of the Russian threat, and how a security/sovereignty dichotomy is largely construed in geopolitical terms and of geographic origin. Writing in the context of Estonian integration to the EU and NATO at the time, Kuus’ insights into the framing of the Russian threat in terms of Estonia’s own existential worries and framing of security may still be of relevance today:

“The Russian threat is indeed crucial to Estonia’s pursuits of international integration, as the elimination of that threat would also eliminate the urgency for international integration. Fears of the loss of sovereignty thus persist in part due to the very utterance of the word sovereignty. This is not in the least to hint that Estonian politics is paranoid any more than in any other state but to illustrate the productive function of the sovereignty discourse.”

(Kuus, 2002: 408)

Estonia and Russia’s relationship over the years has been one of complexity, with relations largely ebbing and flowing since 1991. Similar to both Latvia and Lithuania, Estonia still holds close economic ties with Russia, both relying heavily on cross-border trade and energy imports/exports. Yet, due to its chequered history, and Estonia’s noticeable pivot West during the 1990s and early 2000s (see Chapter 4), relations have largely remained ambivalent, leading to a general mistrust and suspicion of one another. Frictions have mostly been political, congregating around a (still) unratified border (Aalto and Berg, 2002;

5 Such a view may be controversial but joins similar claims, such as the comments made by Russian security expert Sergei Oznobishchev, in suggesting that many in the Baltic states suffer from a “virtually genetic fear of the Soviet Union and now Russia” (Gidadhubli, 2004: 1885). This sits in interesting juxtaposition to Russia’s own security discourse and use of strategic narratives, where a politics of victimhood perennially depicts Russia against ‘the West’, thus morally justifying many of its own economic, security and military policies (see, Humphreys, 2015; Rühle, 2014; Ventsel et al., 2019).
Berg and Oras, 2000; Viktorova, 2006), and issues concerning citizenship and national identity (Berg, 2000; Feldman, 2001; Merritt, 2000; Smith, 1998).

In the immediate aftermath of restoring independence, accession to both NATO and the EU was a long-term strategic goal for Estonian leaders and was a clear indication that the country was intent on shaking off its post-Soviet legacy. Whilst membership to both held a promise of greater economic prosperity and security in a post-Cold War system, the gradual expansionism of both alliances towards Russia’s own sphere of influence would continue to unsettle relations.

During the 1990s, the Russian government had “vehemently rejected” (Kramer 2002: 731) the proposed accession of the Baltic states into NATO, while Western leaders were equally hesitant in antagonising Moscow – particularly during a period of renewed international cooperation following the collapse of the Soviet Union. Things did change in 2001, however, with all key stakeholders (NATO, Russia, and the Baltic states) all agreeing to modify their positions in “small but significant ways” (Kramer, 2002: 731), and by the following November all three Baltic states were invited to accession talks at the 2002 Prague summit. Newly elected President Vladimir Putin, acquiescent at the time, insisted that NATO accession was “no tragedy”, despite NATO’s eastern border now sitting some eighty-five miles from his hometown of St. Petersburg (Warren, 2002). Was this an attempt by Russia to strategically shift West itself, following nearly a decade of upheaval and economic decline following the collapse of the Soviet Union? (Nichols, 2002)

Without wishing to enter a huge discursive terrain regarding the strategic narratives and direction of Russia under the Putin presidency (see, for example, Gessen, 2012; Lucas, 2014; Pomerantsev, 2017; Sakwa, 2020; Walker, 2018; Wood, 2018), it is clear that such motivations did not last forever. Over the following decade or so, Russia’s relations with both NATO and the EU soured greatly: first, following a lengthy war with Chechnyan separatists (2000-2009), and then further following conflict with Georgia in 2008. By the time Russia had annexed Crimea in 2014 (see Section 5.2.2), it seemed that relations between Russia and the West were at their lowest since the Cold War. Within a matter of weeks, NATO Foreign Ministers had agreed to suspend all practical civilian and military cooperation with Russia, with a statement condemning “Russia’s illegal military intervention in Ukraine and Russia’s violation of Ukraine’s sovereignty and territorial integrity” (NATO, 2014a). This was followed up by strict international sanctions by the EU on Russian individuals and businesses (joining other international allies and strongly supported by the Estonian government), and some of which are still in force today.

---

6 Kuus notes how Estonia’s foreign policy objectives during this period – rapid international integration and the undivided sovereignty of the nation-state – were largely contradictory. Accession to the EU and NATO was, on the one hand, framed as “a guarantee for Estonia’s independence and sovereignty” from the Russian threat; whilst, on the other, integration to such alliances was also considered a threat to Estonia’s sovereignty and authority over its territory, “especially in matters of citizenship and minority rights” (2002: 394).
As the situation continued to unfold, discourse around the security and defence of the Baltic states would also ramp up. U.S. President Barack Obama, in an address to the Estonian nation during a visit to Tallinn in September 2014, stated unequivocally that NATO’s eastern members could rely on U.S. support in the event of an attack; also stating that the “defense of Tallinn and Riga and Vilnius is just as important as the defense of Berlin and Paris and London” (The White House, 2014). Former British Defence Secretary Sir Michael Fallon also suggested there was a “real and present danger” that Putin would attempt to test NATO’s resolve in light of the ongoing situation in Ukraine (Farmer, 2015). Geographically speaking, the Baltic states (and Estonia in particular) serve as the weakest point in NATO’s collective defence. Yet, as I unpack further in Section 5.2.3, any attempts by Russia to engage with the Baltic states militarily seems unlikely at present. Nonetheless, across NATO member states, I believe events in Crimea and Eastern Ukraine have contributed to a collectivised paranoia or anxiety over what Moscow may decide to do next – even leading to pleas from Baltic officials to strengthen NATO’s collective defence. Estonian President Toomas Hendrik Ilves was particularly vocal, calling for NATO to station more ‘boots on the ground’ as an active deterrence against an increase in antagonistic rhetoric and military performances across the Baltic Sea region (Blair, 2015).

Ilves’ calls for greater protection and deterrence across the region were soon answered. During its 2016 Warsaw summit, NATO members agreed to “enhance its presence” across its eastern flank with four multinational battlegroups stationed in Estonia, Latvia, Lithuania and Poland (NATO, 2019). In what can be regarded as a direct response to the annexation of Crimea and ongoing conflict in eastern Ukraine, NATO’s Enhanced Forward Presence (eFP) would mark the largest troop reinforcement of NATO’s collective defence in over a generation to members deemed most at risk from possible Russian interference. Russia has, unsurprisingly, seen the build-up of NATO presence across the Baltics (and Estonia in particular) as incredibly provocative, with Foreign Minister Sergei Lavrov reiterating that Russia will mirror any NATO reinforcement with its own adequate measures on its own western flank (Sharkov, 2016).

During the completion of this thesis, relations between Estonia and Russia have remained rocky, yet relatively non-confrontational. By virtue of its position within both NATO and the EU, Estonia has been afforded the relative security of both alliances’ unity and collective defence, in particular regarding Russia and its actions in its ‘near abroad’. This is not to say that Estonia has remained silent over the issue of Ukraine, or uncritical of Vladimir Putin’s apparent Soviet ‘nostalgia’ (Cassiday and Johnson, 2010). Indeed, as shown above, Estonian leaders and ministers have remained vocal in urging Western allies to remain alert and cognisant of the threat posed by Russia and what it believes to be fundamental violations of state sovereignty, human rights abuses and international law.

---

7 The total troop deployment across all four battlegroups was approximately five thousand – led by larger NATO member states (the UK, Canada, Germany and U.S.). The Estonian battalion battlegroup in Tapa (93km from Tallinn) has been led by a British deployment of over eight hundred troops, working with other NATO member personnel on a rotational basis (NATO, 2019).
Yet, it would be remiss to determine that such a deterioration in relations would be solely down to Russia, with diplomatic pressures and military exercises remaining largely tit-for-tat. In addition, Estonian attempts to reverse decades of ‘Russification’ as part of its restoration agenda during the 1990s have been equally antagonistic (Aalto, 2000), with the Russian government critical of the unfair treatment of Estonia’s Russian-speaking population, condemning its Estonian citizenship and language policies (Gorelov, 2020; Merritt, 2000).

5.2.2 Necessary wakeup calls
In this thesis, I have pointed to two critical junctures – the 2007 cyberattacks against Estonia and 2014 annexation of Crimea – as potential catalysts for the emergence of the Estonian Data Embassy. Not only are both events significant for their connection to the Russian state, but I also argue in this section that they served as a crucial and necessary wakeup call for the Estonian government with regards to possible threats to state sovereignty and vital functions of Estonia’s digital ecosystem. Here, I analyse their impact and affective responses they subsequently enacted.

It is fair to say that nobody foresaw the events that would unfold following the ‘Bronze Soldier’ incident of April 2007. After several days of civil unrest among large numbers of the country’s Russian-speaking minority on the streets of Tallinn, Estonia experienced what is widely labelled as the world’s ‘first’ state-sponsored cyberwar, with several waves of coordinated DDoS attacks succeeding in shutting down vital government and banking services (see Section 4.1.2 for a more detailed account of how events unfolded). While their intensity was far from exceptional, the extent, duration and overall coordination of the attacks against another state was unprecedented (Kaska et al., 2010: 44). It was the first time a country had experienced such a broad and sustained attack over the internet. Then President Toomas Hendrik Ilves would later reflect: “It was unheard of, and no one understood what was going on in the beginning” (Tamkin, 2017).

Coverage of the events that took place in 2007 has been well chronicled in both media and academic discourse (see, for example, Kaiser, 2015; McGuinness, 2017), with many describing it as a watershed moment, not just in Estonia but for the entire global community. Whilst the present dangers of a state-level cyberattack had already been prophesied across the cybersecurity community prior to this point, events in Estonia arguably brought cybersecurity into the mainstream and onto national security agendas. There was now a tangible case study to drive home the importance of cybersecurity awareness and defence to the not-yet-versed politician or policymaker:

---

8 After the restoration of independence, Estonian authorities automatically granted citizenship to anyone who resided in the country prior to 1940. Anyone who was unable to prove this, or arrived after 1940 (like many ethnic-Russians did during Soviet occupation), could only acquire citizenship with a proficiency in the Estonian language and knowledge of the country’s history. Many ethnic-Russians – unable to speak Estonian, and unable to hold dual citizenship (another Estonian government policy) – were made technically ‘stateless’, with approximately 80,000-90,000 finding themselves in a political and geographical grey zone. A majority of these were issued with grey ‘alien’ passports as a result.
“Because the biggest value from 2007 is not some kind of technical play or something like that, but the problem with that was the attitude towards cybersecurity. Before that, people were actually thinking that if you had a problem with your IT systems then actually it was because you didn’t know how to do IT. A lot of people knew that cyberattacks do exist, but Estonia and their politicians were the first that said loudly that ‘we are attacked’. What happened after that, those people who had actually seen this problem that they couldn’t really discuss before, they could now refer to that ‘Estonia has had this kind of problem’, and it opened the discussions.”

(interview 20 - 27/11/18)

The effects were felt no more strikingly than within the NATO community, insofar as highlighting the vulnerabilities and potential impact of an attack on state institutions and wider public. The prompt establishment of the Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE) in Tallinn the following year can conceivably be recognised as an attempt to allay such fears. Estonia had in fact proposed the formation of a dedicated Centre of Excellence prior to its accession in 2004 (Stewart, 2008) – perhaps already demonstrating their established expertise and an awareness of the threat posed in cyberspace. But it wouldn’t be until after 2007 - and Estonia’s effective response to the cyberattacks - that NATO leaders were finally convinced it was needed, with then Secretary-General "Jaap" de Hoop Scheffer committing his full support to the centre. During the next NATO summit in Bucharest (2008), NATO members would also approve a unified policy on cyber defence and a commitment to assist members during any future attacks10.

A number of key developments in Estonia domestically since 2007 also point to how the incident played a pivotal role in driving general awareness and better cybersecurity practices across government, industry and society more broadly. As I highlighted in Chapter 4, central to this was the development and creation of Estonia’s first National Cyber Security Strategy (2008-2013). Tasked with reducing the “inherent vulnerabilities” (MoD, 2008) faced in cyberspace, the document set the foundations from which Estonia

---

9 NATO Centres of Excellence (COE) do not form part of NATO’s official command structure, but do play a role in shaping alliance policy and providing training and education for leaders and specialists from NATO member and partner countries. The COE in Tallinn plays a pivotal role in research on cyber defence and legal norms, as well as cyber defence awareness and training.

10 At the time, this stopped short of equating to NATO’s Article 5 ‘collective defence commitment’, which would come during the 2014 Wales Summit. Here, it was agreed that cyberattacks reach a threshold that threatens “national and Euro-Atlantic” security and prosperity (comparable to that of a conventional attack), leading to cyber defence being recognised as part of NATO’s core collective defence (NATO, 2014b). Another positive outcome of the 2007 cyberattacks has been ongoing debates regarding the validity of international law in cyberspace, with the NATO CCDCOE publishing the Tallinn Manual (Schmitt, 2013; 2017), seen by many as an early canonical text in terms of cyberwarfare and international law (note: the Tallinn Manual is compiled by a group of leading experts and is not an official document representing NATO doctrine or the views of a particular state). In more recent developments, at the 2016 Warsaw Summit NATO officially recognised cyberspace as a domain of operations alongside land, sea and air (NATO, 2016).
was able to build its cybersecurity capabilities across areas of defence and industry. The strategy also played a crucial role in shaping cybersecurity as an interdisciplinary problem for society more broadly, while driving greater awareness in both a domestic and international setting. Often credited as one of the first cybersecurity strategies in the world, its subsequent iterations (2014-2017 and 2019-2022 – MoEAC, 2014; MoEAC, 2018) have sought to build on lessons learned since 2007 and spearhead innovative cybersecurity developments at both a public sector and industry level (Robinson and Hardy, 2021).

Another key development has been the continued drive and cooperation between the Estonian public and private sector on matters relating to cybersecurity. Many have pointed to how this played a vital role in the government’s response in 2007, with many private sector organisations (such as Swedbank, Estonia’s largest banking service) pooling resources and expertise to help cope after vital services were affected by the DDoS attacks. Such cooperation is still visible today and a number of interviewees pointed to the way in which this has had a positive impact upon the general maturity of cybersecurity across society:

“You got people thinking stuff. You got the story going. So you got investments – possibly more investments made based on that story. So, it was a good thing.”

(interview 28 - 17/07/19)

I also spoke to many Estonians who, in retrospect, regard the cyberattacks in 2007 as something of a blessing in disguise:

“Actually, we are very thankful for this cyberattack [laughs]. Because, due to that, we actually understand the importance of cybersecurity and we started to build our competence in cybersecurity, and we have started to think more about it. Thanks to that, we have here in Estonia the NATO Cyber Security Centre, and we have gained experience in cybersecurity.”

(interview 1 - 09/08/17 – see also Fig. 5.3)
This speaks to the widely held belief that significant lessons have been learnt from the events of 2007, the benefits of which are still being registered today. I also believe it points to something of an attitudinal shift at a state-level regarding attitudes to cybersecurity. For Jaan Priisalu and Rain Ottis, not only did it reveal how an overall dependency on its digital infrastructure meant that a return to old fashioned pen and paper was “next to impossible” (see Section 5.1), but also exposed a “digital fault line” in the way critical Estonian national information infrastructure and systems were “organized and made operational” (2017: 446-447).

Taking this one step further, I also wanted to ascertain whether this ‘digital fault line’ subsequently led to significant changes in how the Estonian state was beginning to think about how and where state information systems and data should be held and secured. In other words, to what extent did the 2007 cyberattacks serve as a pivotal moment from which a conversation around extraterritorially storing state data in the cloud could effectively emerge?

Some interviewees agreed with the plausibility of this argument, but a number of Estonian technical experts were reticent in recognising this link, instead pointing out how the DDoS attacks were an attack on the availability and reliability of Estonia’s critical infrastructure – “it was not about extracting new information” (interview 16 - 15/10/18). While it may be the case that the DDoS attacks were nothing more than an attempt to “flood the system” (interview 16 - 15/10/18) in order to choke government portals and services (not an attempt to extract critical data sets or state secrets), I believe a subsequent after-effect has been to stimulate greater conversation and a series of future ‘what ifs’ around the confidentiality and integrity of Estonia’s national information infrastructure (see Section 6.1.2). Nonetheless, there remains little explicit evidence that the 2007 cyberattacks had a direct impact on the emergence of the Data Embassy.
Over the course of completing this thesis, I also encountered a number of respondents who were critical of the general academic and media discourse around the nature (and subsequent impact) of the attack:

“There are loads of legends that the city was on the knees. The maximum damage was the largest bank was down for one hour and 20 minutes. That was maximum damage.”

(Taavi Kotka interview - 15/07/19)

Instead, I gained a sense of the more holistic impact the attacks had, becoming something of a symbolic awakening across the public and private sector in terms of the threats states now faced in cyberspace. Pointing to the benefit the attacks have had on the country’s ‘e-Estonia’ brand and international reputation as a cybersecurity pioneer (see Section 5.3), there was also a sense that without the events of 2007, a concept as ambitious as the Data Embassy may never have come to fruition: “Everything about e-Estonia is directly related to that event in 2007. So, it was a great impetus to make things more safe – to have backups.”

(interview 18 - 07/11/18)

If drawing a direct link between the events of 2007 and the establishment of the world’s first Data Embassy seems a little intractable, this certainly wasn’t the case following the annexation of Crimea in 2014. As highlighted at the beginning of this thesis (see Section 1.3), the events that unfolded over the course of 2014 served as a “warning bell” (Taavi Kotka interview - 15/07/19) for the Estonian government and harbinger for the Data Embassy to be subsequently established. Despite plans for the Data Embassy technically being conceived by Taavi Kotka in 2013 (see Section 4.2), it wasn’t until Russia’s decision to occupy and annex the Crimean Peninsula, and the conflict that followed in the Donbass region in eastern Ukraine, that momentum was able to build. Serving as yet another wakeup call for the Estonian government, Kotka hinted that the political situation meant he was able to sell the idea of the Data Embassy more easily than simply a ‘technical solution’:

“Politicians, they don’t understand those kinds of things, but they understand the fact that ‘okay, we don’t have a paper fall-back’. They understand that we might face the same challenges that we had in 1991 and ’92. Oh, fuck. Right? They understand those things.”

(Taavi Kotka interview - 15/07/19)

At the time, commentators felt that events in Crimea were also a tell-tale sign of the Russian government’s determination to “defend and consolidate” its sphere of influence in its ‘near abroad’ (Carpenter, 2014).
Most notable was Putin’s use of ethnic nationalist language (and calls to defend the political rights of all ethnic-Russians) as justification for his foreign policy motives; which, as Kimberley Marten (2015) notes, foreshadowed threats against many neighbouring states (including Estonia) with significant Russian-speaking populations of their own. Tactically, the Russian government adopted a highly sophisticated hybrid approach in Crimea and eastern Ukraine (utilising both military and non-military operations – see section below), whilst appealing to many native Russian’s geopolitical and historical imaginations around Crimea (Biersack and O’Lear, 2014). For an unsettled Estonian government, not certain on what *exactly* Putin’s “endgame” (Marten, 2015) might be, questions around national security and the commitment of the NATO Alliance were thrust into conversation. As Josh Rubin (2019) commented in *The Atlantic*, “The last thing the Estonian government wants is for Putin to claim to be the defender of Russian speakers in Narva, as he did in Crimea.”

**5.2.3 Hyperbole or necessary deterrence?**

Despite the purported Russian threat and its relation to the Data Embassy being played down by some (including the current Estonian President Kersti Kaljulaid), this section has so far shown that Russia continues to be framed as part of an everyday Estonian security discourse. For some, it has even become something of a preoccupation:

> “Any kind of security policy discussion in Estonia is always based around Russia, even if it is not named. So when people talk about things like environmental threats, what they are thinking about is pollution from Russia in the Baltic Sea. When they talk about migration, again there is a Russia angle to that. So everything is always focused on Russia.”

(interview 3 - 16/05/18)

It is of no surprise, therefore, that the majority of initial media discourse around the Data Embassy centred around Russia and the potential geostrategic goals of Vladimir Putin. This was further exacerbated by initial government rhetoric that contemplated Estonia’s territorial integrity and political independence once more (MoEAC, 2015). By way of concluding this section, I wish to question the efficacy of such rhetoric: first, exploring whether the Russian threat and its role in the development of the Data Embassy has been largely hyperbolic, before questioning whether the Data Embassy itself should be viewed as a rational response and effective deterrence mechanism against an antagonistic Russia.

As I have alluded to throughout this thesis, the purported Russian threat has played central to discourse around the Data Embassy. Whether it has been instigated by the Estonian government or not, this has largely concentrated on both Russia’s growing cyber capability (fearing a repeat of 2007) and its geopolitical and foreign policy objectives in its ‘near abroad’. Due to the latter, intensified in a post-Crimea landscape,
this has led to political commentators speculating on who ‘might be next’, with the Estonian city of Narva (situated along its north-eastern border with Russia) frequently the focus of its analysis. As David Trimbach and Shannon O’Lear (2015) observe, Narva and Crimea do share many similar characteristics (a predominately Russian-speaking population, proximity to Russian territory and a history of territorial disputes in the region) but, as I also argue in this thesis, a great deal of commentary and analysis has been a little conflated, imprudent and one-dimensional.

Nonetheless, a variation of the Crimean question was one that I kept returning to over the course of completing this thesis, asking specifically: what is the likelihood of Russia actually instigating some form of kinetic attack against Estonia? Furthermore, to what extent is such discourse hyperbolic? Or could Estonia experience a similar scenario to Crimea and lose its independence once more? Discussed on a number of occasions with interviewees, responses fluctuated and ranged from the dismissive to those who believed that Russia’s geostrategic goals in the Baltics were entirely plausible. For those who were more sceptical in making this link, they instead turned to criticising the role certain media have played in conflating and amplifying general hyperbolic discourse around Russia:

“And I believe that, for example, like when, in 2014, when Crimea was occupied by the Russians, then an anxiety started to show in the media more than it was among the people maybe.

Author NR: Because everyone would say Narva was under threat...?

Yeah, yeah. And what we saw was that foreign correspondents came to Estonia with a crew to make films in Narva and asking, like, where the tanks are. Wait, what now?!”

(interview 17 - 29/10/18)

From a more critical standpoint, it might be easier to argue that, due to Estonia’s position within NATO (and the relative security, deterrence and collective defence that membership affords), the likelihood of Russian intervention or use of military force against Estonia appears extremely unlikely (see, Ferris, 2018). But this is not to suggest that the threat from Russia is in no way legitimate, or that taking certain measures to safeguard Estonia’s digital ecosystem or territorial sovereignty is an irrational one. As one interviewee

11 As David Trimbach and Shannon O’Lear (2015) crucially point out, Narvans are not a monolithic community and thus should not be simplisticly characterised as a homogenous Russian population (see, also, Smith and Burch, 2011). Rather, the strong communities of Russian-speakers and ethnic Russians “comprise an array of political perceptions, citizenship statuses, and spatial identities” (2015: 500). I found this to be true during my own visit to Narva in 2017 (see Fig. 6.1), where, although a vast majority of political commentary likes to portray Narva as a small Russian enclave, its complex history and contemporary geopolitical landscape has led to intricate and nuanced understandings of identity, economics and culture.
elucidated, regardless of its position within NATO, Russia’s strategic aims and foreign policy goals still maintain a credible threat throughout the Baltics and wider Western NATO alliance:

“I do think that Russia would take opportunities to challenge the Western consensus about the state of the world. It has a grand strategic goal, but does not behave in a strategic way; it behaves in an opportunistic way. So if opportunities rise, then it will take them [...] And I think Russia's overall aim is to break the current global order and to restore a position where it had a serious say in international affairs, and particularly in affairs in what it considers to be its part of the world. This here is certainly part of its part of the world.”

(interview 3 - 16/05/18)

Such an argument chimes with a great deal of contemporary analysis on Russian geopolitics, illustrating Moscow’s ‘opportunistic’ yet ‘calculated’ foreign policy strategy, particularly in its ‘near abroad’ (see, Dyson and Parent, 2017; Lindley-French, 2014; Mankoff, 2014; Thomas, 2015). In compensating for its military, technological and economic inferiority, argues Reid Standish (2019), Putin’s Russia has instead employed a strategy based on much smaller, low-cost “calculated risks” that rely on “disinformation, political meddling, and subterfuge”. For a number of respondents, I spoke to, this was now of far greater concern than at what point tanks were expected to roll over the border, or whether ‘Little Green Men’ were going to pour into Narva overnight. Having taken note of Russia’s strategy in Ukraine (and to some extent, Georgia in 2008), there was a sense that if an attack was to occur, then it wouldn’t simply be a kinetic one. Adopting a hybridised approach that utilises more indirect, asymmetric tactics (such as reflexive control12), many believe that attempts to subvert democratic processes via misinformation or by unsettling large Russian-speaking demographics were far more likely. In truth, the Baltics have experienced both already to some degree, but there was a growing sense that if Moscow was to attempt to disrupt its own sphere of influence in Estonia, such subversive techniques were much more plausible:

“I would say that against the historical experience, [we] just have to think whether something like that is likely today, because any conflict that would happen here I don’t think that it will be the repetition of World War II - or any of the preludes to that. It would be different and even I would have to say, in this case it may not be occupational as such - that's why we should be really worried about this

12 Reflexive control can be defined in several ways, but has been a distinctive Russian tactic since the Soviet era. According to Timothy Thomas, reflexive control can be understood as “a means of conveying specially prepared information to a partner or an opponent to incline him to voluntarily make the predetermined decision desired by the initiator of the action.” (2015: 456) It is, in effect, a measure to control an adversary’s decision-making processes and was a tactic deployed extensively during Russia’s invasion of Ukraine in 2014 (Hosaka, 2019).
medalling with democratic processes. And, again, I think governments have to be preoccupied with actual moods and attitudes of their own people.”

(interview 9 - 28/05/18)

Finally, by framing the Russian threat as something known and intelligible, there was a belief among a number of participants that the Data Embassy could also be a vital and necessary deterrence against any form of Russian aggression (either via conventional means, or in cyberspace). In its broadest sense, the primary objective of conventional deterrence is to persuade “an opponent not to initiate a specific action because the perceived benefits do not justify the estimated costs and risks” (Mearsheimer, 1983: 14). Arguments here thus posit the Data Embassy as a deterrence method by ensuring that an attack on the state is less profitable for an adversary. This could be interpreted in two ways. First, the Data Embassy may serve as a vital deterrence by denial in cyberspace. As the aforementioned DDoS attacks in 2007 showed, critical institutions and services of the state were heavily disrupted and their availability was of paramount importance. Thus, having them effectively operate from a Data Embassy in Luxembourg (and perhaps a network of many more around the world in the future) will limit the likelihood of vital services and state infrastructure being shut down, increasing the cost for the adversary.

Second, in more conventional terms, some interviewees believed that the Data Embassy may also serve as a deterrence by “reducing the efficacy of territorial control” (interview 10 - 31/05/18) for an attacker – in this case Russia – meaning that an attempt to attack or seize Estonian territory and existing state institutions would be less beneficial. Effectively, this would mean that the state could protect (and potentially operate) its critical information systems and data extraterritorially from the Data Embassy. As one interviewee argued:

“You need to put yourself into the shoes of the planner in the military headquarters of the attacker. The things you must do, you must either suppress or take over existing institutions. And if you are actually continuing those institutions digitally or virtually you are simply making this attack planning more expensive […] so you are adding something into the calculation of the potential occupier, so basically it works like a deterrent in the end.”

(interview 20 - 27/11/18)

Although the Data Embassy, in truth, may not be the thing that stops Russia from invading if Moscow presented such a scenario, it might give you “leverage”, suggests one respondent, “and it changes the calculus, so why not?” (interview 10 - 31/05/18). This divergence from other prophetic visions of the Data
Embassy is interesting, for it posits that its form of deterrence may not become the silver bullet for a state facing existential threats in the future (whether conventional, cyber, or a hybrid of the two). Adopting a cautious approach instead, the above quote suggests that the Data Embassy may actually form an incredibly valuable part of a wider national security strategy and provide political leverage for states embroiled in an array of geopolitical scenarios or disputes (see Chapter 7 for a discussion on the Data Embassy’s wider utility).

This section has examined the narrativization of the purported Russian threat and its relationship to the development of the Data Embassy. Recognising that Russia has played a vital part in framing Estonia’s everyday security discourse (both historical and contemporary), it has explored how this has manifested itself in discourse around the Data Embassy. For many Estonians that I spoke to, significant events such as occupation, 2007’s cyberattacks, and the annexation of Crimea only perpetuate a sense that ‘it’ (meaning any of these previous events) ‘might happen again’; whilst many would speculate on the true motives of those inside the Kremlin, and whether the resolve of the Baltics and wider NATO alliance might be tested in the future. In the beginning, for Taavi Kotka, it was an opportune strategy to sell the Data Embassy to his ministerial colleagues, whilst also serving as a “sexy” topic for international journalists to write about and amplify this message (Taavi Kotka interview - 15/07/19). This message, however, still appeared to be at odds with many civil servants I spoke to, and the current strategy of an Estonian government seeking to distance itself from, and play down, the purported existential threat posed by Russia. This, as the remainder of this chapter explores, may be crucial for the government as it seeks to protect and develop its brand as a digital and cybersecurity pioneer even further.

5.3 Branding e-Estonia

“[In Estonia, clean and untouched nature co-exists with the world’s most digitally advanced society. It is a place for independent minds where bright ideas meet a can-do spirit.]”

(Brand Estonia, 2019)

Figure 5.4 – Recent branding used by the Estonian government for its e-Residency programme (source: www.brand.estonia.ee)

Joseph Nye (2011) recently proclaimed that, in an information age, the state with the best story will be the one that ‘wins’. In reference to the battles states now face with regards to the flow and control of information in a more interconnected world, Nye’s thesis speaks to a growing debate centring on the decline or crisis facing the modern state (Bauman and Bordoni, 2014; Owen, 2015). Increasingly, states are left grappling with the digital dominance and disruption of large tech companies that generate greater wealth
and influence on the global stage. Many have pointed to the rise of the ‘Gang of Four’ – Google, Amazon, Facebook and Apple (and occasionally Microsoft) – and their unprecedented accumulation of power, wealth and influence in ways that “existing regulatory and intellectual frameworks struggle to comprehend” (Moore and Tambini, 2018; see also Galloway, 2017).

In what seems to be a gradual erosion of sovereignty, power and influence, how should states react? In his book, *Disruptive Power* (2015), Taylor Owen suggests that states may have to adopt startup characteristics in order to survive and stay relevant in a digital era. Pointing to how the rise in digital technologies and more empowered digital actors has presented a crisis in state power, Owen calls on state-led institutions to reform and embrace ‘disruption’ in order to address the growing imbalance globally.

For Estonia, with a powerful brand – e-Estonia – and ‘story’ of its own, it could be argued that it has taken greater steps than most to address this imbalance. Through its embrace of disruptive technologies and innovative solutions within both its public and private sector, the country has been able to position itself as a “digital power” (Areng, 2014) whilst marketing itself as a “pathfinder” (Drechsler, 2018) in areas of emerging tech (e.g. Artificial Intelligence and blockchain), e-government and cybersecurity (see Chapter 4). The Estonian government also likes to profess that it functions like a startup, where radical projects such as e-Residency and the Data Embassy are first ‘sandboxed’ within the ‘living lab’ that is e-Estonia before being scaled up and subsequently replicated by other states across the world.

In this section, I examine Estonia’s nation branding strategy a little closer and question what role this may have played in the establishment of the Data Embassy. First, I trace the country’s efforts to rebrand itself post-independence as Estonia attempted to move beyond troubling post-Soviet imaginaries, before focusing on efforts to brand Estonia as the quintessential ‘e-state’ (Section 5.3.1). Here, I question whether the Data Embassy is simply another radical ‘crazy idea’ that helps to boost and capitalise upon Estonia’s reputation as a digital pioneer, before exploring whether nation branding has become a means for managing anxieties relating to the Russian threat. Second, I conclude with a critique of the Estonian government’s startup mentality, specifically with relation to the Data Embassy, exploring whether its ‘figuring it out as we go along’ approach could have potential adverse ramifications for both the project and Estonia’s digital society more broadly (Section 5.3.2).

### 5.3.1 Establishing a new identity: ‘Nordic With a Twist’ to digital ‘pathfinder’

Over the last few decades, states have increasingly turned to (and invested heavily in) nation branding programmes in an effort to reinvent their image and become more competitive on the global stage (see Section 2.3). ‘Branding the nation’ has, in many ways, become a vital practice and tool for states to fashion their own geopolitical narratives (or ‘myths’), thus projecting them to the wider world as forms of soft power (Browning and Ferraz de Oliveira, 2017). Following periods of political instability or transition, nation branding can provide an opportunity for a state to reboot its own image or national identity
Estonia’s own story has been well recounted throughout nation branding literature (see, for example, Aronczyk, 2013; Jansen, 2008, 2012; Jordan, 2014; Mäe, 2017; Saunders, 2017; Zeineddine, 2018; Tammpuu and Masso, 2018). Indeed, as the first former Soviet Republic to initiate its own extensive nation branding programme, it is viewed as one of the major success stories for its notable role in transforming Estonia’s image as it rapidly integrated into the global market post-independence. At that time, Estonia still faced enormous socio-economic challenges at home and, despite taking great strides with economic and political reforms during the 1990s (see Chapter 4), still considered itself ‘misunderstood’ and negatively portrayed by much of Europe and the rest of the world. With the long-term goal of joining the EU and NATO on the horizon, this transitional period was thus seen as a clean break and an ideal opportunity to rebrand the country (away from a perceived post-Soviet backwardness and deprivation) and for Estonia to reaffirm a sense of nationhood and cultural identity both domestically and abroad\(^\text{13}\).

Estonia’s initial branding efforts began in the early 2000s. Following the creation of Enterprise Estonia - a state-funded agency tasked with spearheading Estonia’s wider public diplomacy objectives - the Estonian government launched its inaugural Brand Estonia campaign, complete with the slogan: Welcome to Estonia: Positively Transforming. Officials were eager to capitalise on the country’s victory in 2001’s Eurovision Song Contest, and, in anticipation of hosting the competition the following year, to put “Estonia on the map” (Jansen, 2012: 85). To do so, they commissioned leading international branding consultancy Interbrand to work closely with the government and develop a series of narratives or ‘stories’ that would convey a particular core message and ‘image’ of Estonia to foreign audiences. Emphasis was placed on Estonian ingenuity and the radical, transformative journey taken since regaining independence, whilst also stressing the country’s European identity and ‘Nordic temperament’ towards an emergent tourist and investor market now on its doorstep (Dinnie, 2008; Jansen, 2012). Christening Estonia as Nordic with a Twist, the introduction of specific branding narratives was incredibly effective and were reinforced by a bespoke marketing campaign (costing €850,000) that included the use of branding books, promotional videos and the creation of a logo (see Fig. 5.5)\(^\text{14}\).

---

\(^{13}\) The occupation period oversaw attempts by the Soviet Union to ‘Russify’ Estonia, achieved namely through cultural repression, a large-scale programme of immigration from Russia, and the mass deportation of ethnic Estonians to Siberia (tens of thousands of Estonians - many women, children and elderly – were forcibly deported in 1941 and 1949). As I highlighted in Chapter 4, following the restoration of independence a period of ‘restorationist geopolitics’ ensued with extensive efforts to ‘de-Russify’ Estonia through invoking stringent citizenship laws and identity/cultural politics (see, Aalto, 2003; Berg, 2003). As Paul Jordan (2014) argues, Estonian nation branding was therefore as much a nation building exercise in its early years, and I would argue that that is very much still the case today.

\(^{14}\) Although the campaign has been widely considered a success, it hasn’t been without its detractors, with some criticising its ethno-nationalist discourse and approach (see Jordan, 2014; Saunders, 2017).
In 2008, Brand Estonia evolved into its second phase, *Introduce Estonia*. As Enterprise Estonia’s Brand Manager Leitti Mändmets explained:

“While Positively Transforming sent the world the message that Estonia was in transition and ready for positive change, Estonia has now left the transition phase behind and proved its existence as a small and strong country. It can be said that with its open thinking, innovation and development, Estonia has managed to continue positively surprising the world.”

(Mändmets, 2010: 73)

Now an established member of the EU and NATO, the rebrand was an opportunity for Estonians to convey a clearer, more harmonised message under a new mantra: *Positively Surprising*.  

It was also during this period that Estonia underwent its most significant period of digital transformation, with Estonians experiencing a ‘conveyor-belt period’ of technological progression (see Chapter 4). Many scholars have noted that, from a branding perspective, this presented the Estonian government with an opportunity to begin conceptualising and marketing itself as a ‘digital nation’ or ‘e-state’ (Mäe, 2017; Saunders, 2017; Tammpuu and Masso, 2018). Subsequently, the last decade or so has seen the emergence of the moniker ‘e-Estonia’, a “shorthand label widely used by national leaders, IT gurus, diplomats, and digital technology enthusiasts alike to evoke Estonia’s success of its public institutions through the implementation of particular e-solutions” (Mäe, 2017: 32). Described by journalist Nathan Heller (2017) as one of the most ambitious projects in technological statecraft, e-Estonia is often seen as a manifestation of Estonia’s success and transformation from post-Soviet transition state to today’s digital pioneer. So much so, the notion of e-Estonia has now acquired its own “powerful narrative dimension” (Mäe, 2017: 32) and can be seen as an extension of the state itself – where, at times, it carries an almost fairy-tale imaginary of a ‘digital Narnia’ or utopia (see, Drechsler, 2018; Vaarik, 2015).

---

15 Market research at the time had indicated that many first-time visitors to Estonia, often with low expectations, left ‘positively surprised’ (Mändmets, 2010: 74). Perhaps in an effort to move beyond earlier criticisms of being too stuck in the past, the campaign also focussed on Estonia as a progressive, rational country, intent on opening itself up to new emerging markets all over the world.
In many ways, the launch of the e-Residency programme in 2014 embodies this message the most, becoming e-Estonia’s flagship project and arguably the country’s greatest public diplomacy tool to date. Since its inception, the programme has garnered enormous international media attention (despite initial limited marketing), tapping into growing entrepreneurial trends around location independence and concerns over state bureaucracy – but also capitalising on seismic geopolitical events such as Brexit. Furthermore, on top of drawing greater attention to Estonia’s digital society, e-Residency has proved a successful soft power instrument, demonstrating the “exportability of Estonia’s digital solutions and the extendibility of ‘e-Estonia’ beyond the national borders of the country” (Tammpuu and Masso, 2017: 551).

During previous research on this topic I also became aware of a great deal of criticism being levelled at the programme, with many castigating e-Residency as a government-funded gimmick and PR exercise (Robinson, 2015). With the Data Embassy launching very much on the coattails of the e-Residency project (2014-2015), I started to question whether it could be similarly regarded. Was this another PR stunt by the Estonian government? How might the Data Embassy function as part of the country’s wider soft power efforts?

Given the overall media discourse surrounding the Data Embassy so far (see Chapter 3), it is clear that the project has played some form of positive branding role for e-Estonia – most notably in areas of cyber defence, e-governance and public-sector innovation. However, while a number of respondents admitted that the Data Embassy was not bad for state PR, they stopped short of denouncing the project as a branding exercise in itself:

“Well, we were aware of the fact that it wouldn’t be bad PR either, right? I certainly would not say it was a PR project, but there was an awareness involved that showed some thought leadership.”

(interview 10 - 31/05/18)

Instead, through the advent of ‘yet another’ novel technological solution (see the aforementioned ‘conveyor-belt’ – Chapter 4), I gained a sense of the Data Embassy’s function as part of e-Estonia’s overall

---

16 On the day after the Brexit vote, the e-Residency team established a landing page (www.howtostayin.eu) in order to capitalise on growing business uncertainty surrounding the UK’s decision to leave the EU. Since then, the number of applicants from the UK has grown nearly “six-fold”, totalling over 3000 (ERR, 2020a).

17 The accusation laid out by a number of critics was that e-Residency offered little in the way of concrete, tangible benefits for Estonian society (and for the e-Resident itself), and was instead more of a gimmick to boost the country’s profile. Whilst it would be difficult to deny that the project has served its purpose as an effective public diplomacy tool, it is important to note that e-Residency has served as a useful public utility for e-Residents, whilst generating an income boost for the state in the process. Recent figures have shown that the programme has earned the state €41 million (€31 million of which is generated in tax revenue) from over 15,000 businesses now operating digitally in Estonia (ERR, 2020b).
branding narrative. In many ways, it was the process of ‘coming up with something new’, and thus being recognised as a ‘pathfinder’, that was just as big a prize. As one Data Embassy insider put it:

“The other [thing] is that Estonia – you can’t underestimate the importance – you have to like sell your country somehow and Estonia has been this digital thing. But many of the solutions like ID card and e-services and so on, they are already old so you have to come up with something new. We have e-Residency now and these data embassies are getting attention now more and more. So doing something – one of a kind – with a government that is just as forward looking as we are - as Luxembourg is - it certainly seize the attention of journalists and other governments, politicians and so on. The selling argument can’t be underestimated as well.”

(interview 6 - 18/05/18)

The Guardian columnist Andrew Keen (2016) has noted how Estonia’s recent branding efforts, particularly in the technological sphere, have served to reinvent and sell the country as the “brightly lit antithesis of Russia”, where transparency and accountability are “baked” into a “new kind of digital civic operating system”. Yet, as this chapter has explored, the Data Embassy and its relationship to Russia has led to an uncomfortableness amongst some interviewees, with the government’s narrative around the project’s motivations also appearing to change over the course of completing this thesis. I believe this is a preferential strategy for the government, as the exacerbation of the supposed Russian threat in relation to the Data Embassy could, on a number of levels, prove “counter-productive” (interview 14 - 12/10/18). For instance, aggravating relations with Russia, whilst appearing alarmist towards EU and NATO allies, could have a detrimental effect on Estonia’s geopolitical/diplomatic relations. Furthermore, a number of respondents made it clear that there was an added economic risk involved in terms of driving away investment and the reputational impact this would ultimately have on the country:

“How do you get foreign direct investment if you say ‘OK, we are in danger that Russia will occupy us’? So, in that sense you have to say well this is a secure business environment and therefore there is no threat of invasion here.”

(interview 14 - 12/10/18)

This section has so far focussed on many of the positive impacts regarding Estonia’s nation branding strategy, and how these fit within a wider understanding of the Data Embassy. The country’s approach has not been without its detractors, however, with some critics questioning the authenticity of its branded
discourse. As Wolfgang Drechsler recently argued, “while e-Estonia’s achievements are significant, the numbers do not match the hype”\footnote{Drechsler points to the great deal of hyperbole surrounding Estonia’s digital success, arguing that although Estonia’s digital government is more advanced than most, not a single digital government indicator has Estonia as number one. For example, in a recent UN survey on e-government service provision, Estonia ranked 16\textsuperscript{th} behind Denmark (Huber, 2019).} (2018: 3). Such home-truths are rarely acknowledged in Estonia, with a great deal of propagandistic discourse around its digital society often going unchallenged (particularly in academic and media discourses)\footnote{I touched on this point in Chapter 3, with a focus on many of the hyperbolic statements around the Data Embassy after it was announced publicly. Wolfgang Drechsler (2018) has been openly critical of the similar hype written about Estonia’s digital society in international media, citing the \textit{New Yorker’s} piece on ‘Estonia, the Digital Republic’ and its standfirst which claimed “Its government is virtual, borderless, blockchained, and secure” (Heller, 2017). Of course, as Drechsler notes, none of these claims are bona fide and only go to augment Estonia’s image as some form of ‘digital Narnia’. As I have recognised in this elsewhere thesis (see Chapter 3), the claim that Estonia is somehow ‘borderless’ and ‘blockchained’ is incredibly misleading, but ultimately requires further analysis and critique.}. Nevertheless, I believe that a lot of e-Estonia’s marketable hyperbole may actually serve an additional purpose: becoming an effective defence mechanism and making the country (at least \textit{feel}) more resilient to the threat posed by its eastern neighbour. Such a theory conformed with the views of a number of critical respondents, with one noting how the e-Estonia brand and government’s proclivity for experimenting and pushing technological boundaries (see Section 5.3.2) may be representative of a desire for greater visibility and pertinency:

“Estonia also needs to outdo itself at all times to remain relevant in the global theatre of things […] we need people to look at us. And not only from a, ‘Ooh these are the funky guys in northeast Europe who are doing stranger danger things with IT.’”

\textit{(interview 28 - 17/07/19)}

In other words, I believe the e-Estonia brand not only offers the country strategic leverage and commercial potential, but also plays a crucial role for the state in managing its own existential anxieties (see Chapter 6), with the Data Embassy serving as yet another reminder to the world that the Republic is still alive (see Section 1.1). As former Managing Director of the e-Residency programme Kaspar Korjus rather bluntly put it:

“If more people can point to Estonia on a map then it’s harder to wipe us from it.”

(Korjus, 2018)

Prior to celebrating the country’s centenary and hosting the EU Presidency in 2018, Estonia launched its third and most comprehensive branding programme to date. Monolithic in comparison to its predecessors, it is a fascinating insight into some of the pervasive practices administered by twenty-first century nation
branders, with the Data Embassy a seemingly inconspicuous addition to its extensive toolkit\textsuperscript{20}. Nevertheless, whilst its wider messaging can sometimes border on the propagandistic, its often-glamourised story has unquestionably made Estonia the “darling of the e-community” (Drechsler, 2018: 11).

To conclude, it is clear that the Data Embassy has played a positive role in enhancing the e-Estonia brand, but to denounce it as a government vanity project would be imprudent. What is clearer, is that the Estonian government is reticent of the role the project plays in the state’s overall public diplomacy function, as well as managing its own anxieties, and thus believes that controlling its narrative is of great importance.

5.3.2 Starting-up and clouding over? Estonia as the world’s ‘living lab’

“You know, [in] 2014 we introduced the e-residency, so we have always done new things. Part of our agenda is to explore, innovate, try new things and if you fail it is OK, it’s fine. Just start over and do something again.”

\textit{(interview 12 - 01/06/18)}

In this thesis I have explored how the Estonian government is keen to profess that it functions like a startup company (e-Estonia, 2016). An unofficial policy of sorts, it conveys a culture whereby innovation is encouraged through the development of novel, disruptive technological solutions with little burden on their expenditure or success rates\textsuperscript{21}. Instilling a degree of freedom within what are traditionally bureaucratic forms of public administration, ministers and civil servants are believed to be able to take more risks on novel ideas or proof-of-concepts (without fear of retribution), whilst Estonia has been able to fashion itself as a technological ‘pathfinder’ in the process. Arguably the antithesis to the approach taken by many states, as government CIO Siim Sikkut posits, “It’s about allowing safe spaces for experimentation…and allowing for the possibility of small but controlled failures in some of those areas” (Huber, 2019).

Conceivably, such a philosophy can be dated back to many of Estonia’s technological advances during the late 1990s/early 2000s, where efforts to introduce a paperless cabinet and internet voting were radical, untested steps into the unknown (see Chapter 4). Growing academic excellence in areas of IT, mechatronics and public administration, coupled alongside a strong R&D push and burgeoning startup community, effectively enabled close collaborative relationships to form between the public and private sector. Over time, this not only allowed for a confluence of ideas and people to flow, but also enabled the

\textsuperscript{20} Estonia’s branding toolkit today is complete with its own ‘story’ and visual design that enables Estonians to communicate clear and concise messaging through marketing (e.g. across both the public and private sector), public speeches (e.g. by civil servants and/or notable politicians such as the president) and diplomacy (e.g. international conferences and the UN Security Council campaign). The reader may wish to visit brand.estonia.ee in order to gain an insight into the government’s current core messaging and branding strategy/output.

\textsuperscript{21} It is possible to draw similarities to Israel and its framing as a ‘Startup Nation’ – where existential anxieties are also correlated to elements of the digital/cyber that are rooted in the country’s past (see, Bone, 2020; Fraiberg, 2017; Getzoff, 2020).
government/state “to move like a startup, and startups to think big like a government[/state]” (Burke, 2018). The e-Residency programme has perhaps embodied this philosophy more than any other government initiative: first launching as an archetypal startup “in beta mode”, before growing demand led to a ‘scaling up’ of operations as it became a “normal part of how the state functions” (Korjus, 2018).

In this thesis, I argue that the Data Embassy is another form of government/state startup. Formed as a novel, innovative addition to Estonia’s digital ecosystem, the project embodies its professed startup mentality whilst also adopting a number of startup characteristics (see Table 4). At the time of writing this thesis, the Data Embassy is still in its own formative ‘beta phase’ – the Data Embassy in Luxembourg is widely considered a pilot project – with the intention of scaling up as and when is necessary. Like a startup, however, there is also an acceptance that the Data Embassy concept may cease altogether before its full potential is realised22 (see Section 3.4).

<table>
<thead>
<tr>
<th>Innovation/Disruption</th>
<th>Startup</th>
<th>Data Embassy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Startups are normally required to be innovative in order to differentiate from competition. With a high growth potential, many also look to ‘disrupt’ an existing market in order to create new value and overtake an existing competitor (e.g. Uber and Airbnb).</td>
<td>The Data Embassy can be considered a novel innovation, particularly with regards to traditional state backup methods (see Section 4.2). It may also be considered a ‘disruptor’, by way of reconfiguring the way states potentially approach national security and the preservation of state records in the future (see Chapter 7).</td>
<td></td>
</tr>
</tbody>
</table>

| Product | A startup traditionally focusses on a single product/service, central to its brand or USP. | The Data Embassy can be considered a unique state-led ‘product’ or service, but ultimately plays a larger role in the overall e-Estonia brand. |

| Structure/Team | A startup may initially lack in structure/hierarchy, and will comprise of a small team. | Although the Data Embassy project didn’t lack a hierarchical structure, it comprised of an incredibly small team (including engineers, security architects and lawyers). |

| Resources/Partnerships | Startups traditionally lack in economic and human resources; relying on investors (e.g. venture capital) and third-party support. | The Estonian government also partnered with Microsoft in early pilot projects (see Section 4.2). |

| Volatility | Startups can face many financial/political/market uncertainties, and are high-risk/prone to failure. Startups are thus expected to be adaptable and dynamic. | The Data Embassy has faced a number of political hurdles to date, and can ultimately be seen as a huge risk/gamble for the Estonian government (see below – also, see Section 3.4). |

Table 4 – A comparison of startup and Data Embassy characteristics

Whilst such an approach may be lauded for its creativity, resourcefulness and adaptability, it does, conversely, raise some important questions, not least around the efficacy and longevity of such projects.

---

22 As one Data Embassy insider told me: “We will see how the Luxembourg project is going and we will see how to expand, and do we need to expand. Or maybe the project doesn’t meet its goals, and the Data Embassy project is not meant to be [laughs].” (interview 09/08/17)
For example, what does the next phase look like after the Luxembourg pilot? What specific technological solutions or security architecture will be used for ensuring there is a worldwide network of Estonian Data Embassies in the future? What was characteristically clear from my time researching the Data Embassy, was that no clear or official roadmap was apparent for future steps, and there was a sense of not really knowing what was around the corner. More often than not, such questions were met with a great deal of ambiguity, particularly from Data Embassy insiders, who would simply reiterate:

“So we haven’t discussed this properly through just yet”

(interview 1 - 09/08/17)

“We are in a place where we even ourselves don’t know what we can tell you yet, because it is not set in stone what will be.”

(interview 5 - 17/05/18)23

By way of concluding, I wish to critique this approach, asking whether a startup mentality in this context may actually present more challenges for the Data Embassy and Estonia’s digital society more broadly. To me, and a number of sceptical interviewees I spoke to, it felt that the Estonian government was largely ‘figuring it out’24 as they were going along (arguably a startup characteristic itself). As one respondent noted of the wider e-Estonia approach, “You do the marketing first, then you start doing the plans, then you start thinking, but actually then you start building it” (interview 28 - 17/07/19). Building on Kattel and Mergel’s ‘hiding hand’ principle from the previous chapter, I argue that the approach taken with regards to the Data Embassy is symptomatic of a well-established public-sector culture in Estonia that pushes “visionary changes without anticipating all the challenges and risks involved upfront” (2018). Whilst this has proved a successful tactic for Estonian policymakers and e-government visionaries (such as Linnar Viik and Taavi Kotka) in the past, I would argue that such an approach is riskier for a Data Embassy project that is closely aligned with matters of national security policy and security/preservation of state archives.

23 I accept that some of these muted responses may also be a result of government officials purposefully remaining coy over such developments towards a researcher – particularly on such matters which may constitute Estonia’s national security – but it became increasingly clear during my time researching the Data Embassy that its startup approach meant that many of the next steps were yet to be decided. During these conversations, respondents would often refer to the fact that the project was still in its ‘first phase’, and that once “we have this first phase done then probably people will sit down again and look at how we have done it so far, and decide if we move forward or what happens.” (interview 4 - 17/05/18)

24 Recently, when discussing Estonia’s overall digital governance model, government CIO Siim Sikkut posited that ministers are often “figuring it out as we go along” (Trendall, 2019). In many ways, I believe such an expression also reflects the approach taken towards the Data Embassy.
Although one respondent admitted that a number of unique circumstances means that Estonia can “dare to be more startup-y” *(interview 21 - 28/11/18)*, they did, however, warn that Estonia may not always be the beneficiary:

“This idea that ‘we don’t run a pilot, we don’t do focus groups, we don’t do interviews, we just do it’. This may actually be bad for Estonia, but for everyone else it’s great. Because Estonia is the living lab of e-governance for the rest of the world.”

*(interview 21 - 28/11/18)*

In short, although Estonia’s doctrine of operating like a startup may prove beneficial in terms of boosting the e-Estonia brand and positioning the country as a ‘pathfinder’ for other countries, it does herald a number of potential risks and consequences for major government projects such as the Data Embassy. In many ways, it is one unenviable PR disaster away (such as a major data breach or collapse in diplomatic relations) from unpicking years of progress. For now, however, it appears that is a risk that Estonia is willing to take.

In this section, I have examined the role of Estonia’s nation branding strategy in relation to the Data Embassy. Whilst the main motivation for the Data Embassy was not to embellish its already highly regarded e-Estonia brand and story, it is clear that the project has played a vital function in the country’s overall public diplomacy narrative. By way of critiquing the state’s overall branding approach and startup mentality, I have also examined its relationship to the purported Russian threat, arguing that the Data Embassy may be another strategy for keeping Estonia ‘on the map’ and in the mind of its allies.

Nonetheless, what is clear from the analysis above, is that the story (and arguably some of the associated myths) surrounding the Data Embassy and e-Estonia are of the utmost importance to the state:

“Stories are what drive things forward. Stories inspire, stories get people to strive toward better results. Stories inspire politicians, government officials, chancellors, vice chancellors, advisors, aids, all these folks.”

*(interview 28 - 17/07/19)*

If, as Joseph Nye suggests, the state with the best story will be the one that wins in a digital age, then it may be prudent to suggest that Estonia’s is one that is well on its way to being written. By way of caution, however, it is important to remain cognisant of the great deal of hyperbole surrounding the e-Estonia story.
– one that is often propagated by national leaders, diplomats and journalists. In this section, I have instead attempted to present a more critical, nuanced portrayal of Estonia’s digital society (of which the Data Embassy is now a significant part of), in order to highlight some of the frailties and imperfections that are often clouded by Estonia’s powerful narrative as a digital pioneer. “Unfortunately,” as Wolfgang Drechsler warns us, “if a story sounds too good to be true, then it is probably because it is” (2018: 16).

5.4 Conclusion: Ensuring the (Digital) Continuity of Estonia

This chapter has explored the somewhat cloudy motivations behind the Estonian government’s decision to begin extraterritorially storing its data and information systems outside of its own borders. Highlighting a temporal shift in government discourse, from initial concerns over territorial integrity to a more recently espoused business case, I have captured a clear tension that exists in relation to the Data Embassy. In particular, this has centred around the Estonian government appearing reticent in either playing up or playing down the threat Estonia faces regarding Russia. Walking something of a geopolitical tightrope – partly in relation to an ongoing situation in Ukraine, but also in how Estonia wishes to be perceived on a global stage – this quandary was perfectly articulated during one interview:

“I would certainly say that…for the way the government communicates to the world, in general with its view on things, it’s always a dilemma on how you communicate the geopolitics. Because on the one hand, you don’t wanna downplay the risks, right? Both…purely for the self-interesting reason that some realistic risk perception is necessary to get your allies engaged. Look, we have been saying for quite some time that Russia is a real problem, and they’ve got aggressive designs in general on their neighbours […]

[…] Until 2014, many Western European countries called us ‘alarmist’, right? And unfortunately, events in Ukraine showed that we weren’t being alarmist. Our risk profile is very similar to Ukraine, compared to other EU members, but our point was not that Estonia is about to be invaded, but in general this is a problem.”

(interview 10 - 31/05/18)

Ultimately, this has led to a fine balancing act being played by those in government, crafting a carefully balanced narrative around the Data Embassy: first, in a way that could be ‘sold’ to other ministers, and ‘sexy’ enough for international journalists to write about (Taavi Kotka interview - 15/07/19); yet, second, in a way that maintains a degree of geopolitical, diplomatic and economic sensibility with regards to Estonia’s image and relationship with the wider world. Early ‘alarmist’ discourse around the purported threats facing Estonia should be seen as a success - post-Crimea, support was garnered across government, whilst
international attention would only go to bolster Estonia’s image as a pioneer and leader in areas of
e-government and cybersecurity.

Over time, however, this discourse has shifted with the Estonian government appearing to adopt a more
cautious approach, instead professing the Data Embassy’s practical/pragmatic importance for Estonian
society. In Section 5.1, I explored the Data Embassy’s business case in more detail, illuminating historical
concerns over archival preservation and storage, and the degree of logicality it provided for a country that
is so heavily dependent on the functioning of its digital infrastructure and e-services. I argue that there are
two significant reasons for this shift. The first is perhaps reflected in changes within Estonia’s political
system, with Taavi Kotka no longer leading the project as government CIO and the election of Kersti
Kaljulaid as Estonia’s president. For Kotka, with whom much of the initial discourse around territory loss
and sovereignty was directed from, it is clear that such a change in narrative occurred after he left for the
private sector in 2017. For his successor Siim Sikkut, a greater focus was then placed on the project’s
practicalities – whilst, during early interviews in 2017, government officials also wanted to stress to me that
the Data Embassy wasn’t “because of [a] fear of Russia” (interview 1 - 09/08/17). As I highlighted at the
beginning of the chapter, newly elected President Kersti Kaljulaid has also played down the role of Russia
with regards to the Data Embassy – but this may be symptomatic of her overall Russia strategy as
president.

The second reason can be understood in terms of state-level damage limitation, as any exacerbation of the
purported Russian threat could ultimately prove counter-productive (geopolitically, diplomatically and
economically) and detrimental for the country’s powerful nation branding strategy. In Section 5.3, I
examined the role of the e-Estonia brand and Data Embassy as part of the state’s overall public diplomacy
function, arguing that both may play a significant role in making Estonia more resilient to the Russian threat
by making the state more visible to its allies.

Shifts such as these are not to say that the Estonian government no longer perceives threats to its territorial
integrity and political independence as significant. In Section 5.2, I examined how the Russian threat still
plays a vital part in framing Estonia’s everyday security discourse and how this now appears to be manifest
in discussions around the Data Embassy. Focussing on both historical and contemporary crises – Soviet
occupation, 2007’s cyberattacks and 2014’s annexation of Crimea – I argue how such experiences have
come to frame perceptions of a Russian threat in relation to the Data Embassy and thus may be justification
for its establishment. For some, this everyday security discourse perpetuated a belief that ‘it might happen

---

25 President Kaljulaid has been clear that open dialogue and cooperation with Russia is vital if relations are to improve in the coming
years. In April 2019, Kaljulaid visited Moscow and met with Vladimir Putin in an official state visit (the first in almost a decade),
whilst attending the reopening of the Estonian embassy in the capital. She was heavily criticised by Estonia’s Baltic allies, but
brushed off the criticism by suggesting “Talking to all neighbours is only natural, and it’s a bit unnatural that I have to explain it”.
It remains to be seen if the president’s attempts at reigniting diplomacy with Russia will be a success, but when asked if Baltic
security was discussed without other leaders present, Kaljulaid retorted, “I don’t want to be on the menu, I want to be at the table.”
(Walker, 2019).
again’, whilst others challenged the use of such ‘alarmist’ rhetoric. Nevertheless, by examining the general hyperbole surrounding the Russian threat in relation to the Data Embassy, I suggest that it may be a little naïve to determine that it is front and centre of the government’s decision to establish an extraterritorial Data Embassy. Questioning Russia’s territorial ambitions in Estonia, and the Baltics more broadly, I instead point to the more subversive threats posed through disinformation and political interference of which the Data Embassy may do little to negate.

Despite the overall message and motivations behind the Data Embassy appearing somewhat inconsistent, the Estonian government has remained resolute in upholding one of its main goals: to ensure the *digital continuity* of Estonia (see Section 1.3). First entering Estonian public discourse in 2014, its stated aim is to maintain the core functions of the state’s digital infrastructure. Whether this is through the availability of government services or preservation of critical information systems, digital continuity (once a goal of the archivist or CTO of a major corporation) can now be seen as part of the country’s wider national security strategy with the specified goal of ensuring the state can continue to function in the event of a crisis or contemporary emergency.

As I have highlighted a number of times throughout this thesis, it is clear that the preservation and continuation of Estonia’s digital ecosystem is of utmost importance. However, particularly through the use of government rhetoric around territory loss, it is evident that the Data Embassy and digital continuity are closely intertwined with an overall state continuity project. As this chapter has explored (and is explored further in the next), such discourse around the Data Embassy appears to mimic past efforts where struggles around the state’s existence have come to the fore (from independence in 1918, to a legal continuity doctrine throughout Soviet occupation, and a further restoration geopolitics after regaining independence in 1991). Digital continuity, as Lorraine Kaljund argues, can therefore be considered “both a technical and ideological project” (2018: 9) and thus an extension of state continuity efforts that appear rooted in Estonia’s collective memory.

This chapter has attempted to uncover what motives are behind the Estonian government’s decision to form the world’s first Data Embassy. Although I have highlighted some of the tensions and inconsistencies in its approach, I don’t believe this is an attempt by the government to purposefully obfuscate. Rather, I believe it points to attempts to control the Data Embassy’s overall narrative in order to manage many of the everyday anxieties the state faces – from the archival to the geopolitical – as I explore in the following chapter.
“Stood atop Hermann Castle, I looked out across the fast-moving Narva River towards the city of Ivangorod and its equivalent city fortress. I saw Russian tourists waving from its parapets, with Estonian tourists waving back. Below us was the ‘Friendship Bridge’, which marked the border crossing between Estonia and Russia, although its barbed wire exterior was less than ‘friendly’. Despite the constant hum of passengers and pedestrians crossing the bridge, I was reminded by the heavily securitised checkpoints that I was stood not only at the edge of Estonian territory, but also the Eastern frontier of NATO and the EU.

I’d heard (and read) a lot of stories about Narva. A Russian enclave. Nobody speaks English (unlike Tallinn). Locals were disillusioned with life in Estonia and the EU. Some yearned to return to Russia. International ‘commentators’ would often tip Narva as ‘next’ in Putin’s sights. A few closer Estonian friends had told me this was simply hyperbole, and that I needed to experience the city for myself.

As I left Narva later that evening, I reflected on these various stories and narratives surrounding the city and its purported wider geopolitical importance. In truth, the reality on the ground was different. Narva showed itself to be a deeply fascinating and complex place, where a mixture of cultures, identities and socio-political realities collide. A city that, yes, had deep inequalities and was fairly excluded from the rest of Estonian society, but one that was incredibly misunderstood and misrepresented nonetheless.”

(August 2017)
Chapter 6 – Estonia’s Anxiety

So far in this thesis, I have been interested in understanding what motivations underpin the Estonian government’s decision to begin extraterritorially backing up its state data and information systems outside of its own borders (see Chapter 5). Whilst these motivations may appear inconsistent, I have argued that they reveal far more about the state itself, from its performative archival practices (in both analogue and digital form) to an everyday security discourse that centres around Russia and emphasises Estonia’s own existential concerns. Despite the government’s well-argued business case (see Section 5.1), it is clear that the Data Embassy is, in fact, entwined with a much deeper Estonian continuity project that appears to be rooted not just in the psyche and collective memory of many Estonians today, but also manifest in the everyday practices and performances of the state.

To take this argument further, this chapter considers whether such practices and performances are indicative of a state-wide collective anxiety. From everyday concerns over the fragility of its digital ecosystem and preservation of critical databases and archives, to more existential concerns over territorial integrity and political independence, I argue that the Data Embassy’s emergence cannot simply be understood in the context of Estonia’s ‘everyday geopolitical fears’ (Pain and Smith, 2008). Rather, in this thesis, I use the term anxiety because it captures better the various complexities and nuances at play in the Estonian government’s decision to establish a Data Embassy outside of its own borders.

As noted in Chapter 2, anxiety has now become one of the defining characteristics of our modern age (see Section 2.4). Andreja Zevnik (2017) notes how this also reflects a wider discursive shift that has taken place in society whereby anxiety has seemingly replaced fear in our everyday political lexicon, and is now commonly used to describe a whole host of affective phenomena and as a tool for understanding modern political reality. Zevnik goes on to highlight the differences between the two terms:

“If fear or the experience of fear is something comprehensible, identifiable and in turn (possibly) easily removable from or manageable in everyday social and political realities, anxiety, in contrast, suggests the experience of something that is more porous, liquid, unidentifiable, unknown and perhaps even absent.”

(Zevnik, 2017: 236)

Building on a Freudian understanding of the term, anxiety is marked by a “quality of indefiniteness and lack of object” (Stonebridge, 1998: 174) that reflects a more generalised state and can lead to a sense of uncertainty and lack of control, whereas an emotion like fear has a definite ‘object’ and is more directed to a specific entity or threat (Birch et al., 2017; Haldrup et al., 2008). In the context of this research, I believe these characteristics of anxiety best describes how the Estonian state feels and expresses itself ontologically,
and how it also seeks to manage some of the existential threats its faces today (often correlated to those experienced in its past). In relation to many of the threats outlined throughout this thesis, I differentiate them from being ‘fears’, but instead as anxieties that are often unknown and unidentifiable, and that are undulatory in frequency and circulatory in character. Indeed, many of the threats Estonia experiences today could well be characterised as unidentifiable or absent (e.g. do not present a clear and present danger to the state). For example, in terms of the Russian threat, it could be argued that there is no perceived imminent threat against the state and that an attack against the country seems unlikely at present (see Chapter 5).

Regarding the everyday risks posed to Estonia’s archives and digital ecosystem, it is also difficult to pinpoint where such a threat may originate and when it may occur. Nevertheless, despite their ambiguity, they are threats that are still deemed plausible by the state – often borne out of historical experience – and thus require a state-level, anticipatory response to them.

In this chapter, I suggest that this dynamic - one of feeling constantly under threat, yet an uncertainty around if or when something may happen - is emblematic of a collective anxiety that is experienced at the heart of the Estonian state. The way this anxiety makes itself felt is a first order dilemma for the Estonian state: in order to be ontologically secure (in this case, the existing socio-territorial order) the government in power is forced to territorially back-up the very thing (the digital infrastructure of the Estonian state) that is designed to generate a sense of security within the existing borders of the nation-state. Such an anxiety, as Lyndsey Stonebridge (1998) suggests, also has a “distinct temporality” as it looks both forwards and backwards, meaning it congregates and sticks to particular political moments and histories (e.g. periods of occupation, [re]gaining political independence, accession to NATO/EU, 2007s cyberattacks and Crimea in 2014). As such, I argue that Estonia’s anxiety is pervasive (for it is enduring and extends throughout the state’s apparatus), undulatory (as it often comes and goes in waves), and paradoxical (as it is seemingly everywhere, but nowhere in particular).

To date, there has been surprisingly little work on state’s collectively experiencing emotions and affective phenomena such as fear, paranoia and anxiety; although there is a growing body of work that has considered the role of elites and moral panic (see, Bonn, 2010; Clarke and Chess, 2008) and other emotions/affects at a state level in world politics (see, Mercer, 2014; Nugent, 2019; Toal, 2017). Drawing on this existing work, the overarching aim of this chapter is to identify Estonia’s state-level anxiety and how it manifests. Building on Marek Tamm’s (2008; 2013) influential work on Estonian collective memory - which seeks to understand how Estonians remember their past and how memories that make up the Estonian nation are both conveyed and sustained over time – I examine how this anxiety is felt and experienced through expressions of Estonia’s collective memory, wider public discourse, various social and political practices, diplomacy and infrastructures.

In this chapter, I argue that Estonia’s anxiety manifests at a state-level in three particular ways:
1) Estonia’s ‘data futures’ (**Section 6.1**);  
2) Estonia’s everyday affective geopolitics (**Section 6.2**); and  
3) Estonia’s productive anxiety (**Section 6.3**)

In Section 6.1, I identify Estonia’s anxiety through the lens of the archive and the state’s own ‘data futures’ (Pink et al., 2018). First, through an examination of Estonia’s archival history and archival practices today, it is noted how such an anxiety is rooted in the material archive and a post-Soviet collective memory. Second, I examine how this anxiety is also underpinned by state-level concerns over its ‘unknowable’ future. Reflecting on anxieties over data loss and an inoperative state, I suggest that the perpetual uncertainty the Estonia faces is central to understanding how the anxiety is experienced by the state and its elite.

In Section 6.2, I explore how Estonia’s anxiety is lived and felt through an everyday affective geopolitics. First, I examine how this anxiety is often rooted in Estonia’s collective memory, and how certain historical events, such as the downing of the passenger plane Kaleva and Soviet occupation, linger and remain not only in the collective psyche of many Estonians today, but also in the practices of the state. Second, I examine how Estonia’s anxiety is lived and felt today through an everyday affective geopolitics. Examined through the lens of events such as the 2007 cyberattacks and the 2014 annexation of Crimea, I highlight the embodied and emotional qualities of Estonian statecraft and how this anxiety is conveyed through the state’s own security discourse, and diplomatic and geopolitical culture.

Finally, in Section 6.3, I change tack slightly by considering whether Estonia’s anxiety may actually serve a productive function, particularly in the context of the Data Embassy. Contesting the way in which anxiety is often viewed through a negative lens, is there, in contradiction, a potential upside to anxiety? In doing so, I examine how Estonia’s anxiety may be being ‘put to work’ productively by the state in order to manage many of the ontological insecurities it faces today – from pervasive anxieties over its national archives to the enduring spectre of the Russian threat.

### 6.1 Estonia’s ‘data futures’

In the previous chapter, I outlined the Estonian government’s purported ‘business case’ for establishing the world’s first Data Embassy (see Section 5.1). Highlighting the state’s growing dependency on its digital infrastructure, it posits a degree of logicality and pragmatism behind the decision to begin extraterritorially storing critical databases outside of Estonia’s borders. Reflecting on many of the ‘archival realities’ (Yale, 2015) Estonia faces – from concerns over data loss, to the availability of state e-services and the threat of having to ‘return to paper’ in the event of a crisis – I also examined how such realities are managed: i) first through the periodical ‘backing up’ of state archives to Estonian embassies (a practice that has been

---

1 I address the notion of ‘data futures’ in more detail in the following section (see Section 6.1.2).
occurring for over fifteen years), and now ii) through the use of Data Embassies. In this chapter, it is posited that such performative practices are illustrative of a collective state-level anxiety, of which efforts to preserve its state archives (both analogue and digital) appear rooted in Estonia’s quest for ontological security (by regulating its collective memory and relationship to a Soviet past).

In this section, I examine the way in which this anxiety has manifested itself through the materiality of the archive and the state’s ‘data futures’ (Pink et al., 2018). First, through an exploration of Estonia’s own distinctive archival history, I suggest that its anxiety can be identified through its relationship with the material archive (Section 6.1.1). Despite efforts to digitise many of its archival practices, I argue that Estonia’s move towards ‘backing up the state’ to the cloud is still grounded in a material, archival anxiety, that is captured in the notion and threat of having to ‘return to paper’ in the event of an emergency. Second, drawing on state-level apprehensions regarding the future possibility of data loss, technological obsolescence, and an inoperative ‘e-state’, I argue that Estonia’s anxiety is also manifest in the enduring uncertainties the state faces over its ‘unknown’ future (Section 6.1.2). Referring to a number of legitimate concerns regarding potential conflicts with Russia, outdated technology or ‘insider threats’, I argue that Estonia’s anxiety can be better understood through an understanding of its own ‘data futures’.

6.1.1 A ‘return to paper’: Estonia’s material, archival anxiety
This thesis has reflected on how Estonia’s digital society has become simultaneously infallible yet fragile – how, despite its many advances and purported benefits for the everyday Estonian (security, privacy, accessibility), there is still a foreboding sense that something bad is potentially around the corner. In many ways, this anxiety is hardwired into the establishment of the Data Embassy itself, where visceral concerns over the preservation of its archives – or potential incapacitation of its digital infrastructure and ‘e-state’ - are central to Estonia’s geopolitical culture and ontological security. As Taavi Kotka and Innar Liiv outlined in their early working paper on the concept, scenarios whereby “digital signatures do not work for days at a time, or the data in the Land Register is corrupted, are not acceptable to Estonian society” (2015: 161). This, as many respondents told me, means that the state would be unlikely to function effectively if it were forced to ‘return to paper’ in the event of a crisis:

“It is important to note that Estonia is uniquely – in the year 2018 – reliant on e-governance. The ability for Estonian citizens to get in contact with either a local or state government, or any agency, is [done] via electronic means.”

NR: Almost that there is a vulnerability in a sense because everything is digital?

“Yes. Estonia cannot function without that. You cannot function without a functioning internet. I mean if there is no electricity no modern society can function very well. But here, [there] is an added layer of complication because,
really, pretty much everything is done via electronic means. So basically, nothing will happen in terms of a government serving the citizens or banking or anything of that sort. Nowadays you even don’t have a physical redundancy system in a way to go back to.”

NR: That’s the paranoia in a sense, that there is no paper to go back to?

“Of course. And there are instances where there are no paper anymore. Even on very specific and important aspects – the Land Registry – which is not on paper at all anymore. Nothing. So this is…you cannot go back to archives […] And then of course, there is always a possibility - looking at Estonian history – we are a small country, next to a big one, which has historically been unfriendly - to say it in a very mild manner. You basically need to look at, say, your data, which is of citizens and government combination. So, from a geopolitical upheaval […] it can be ranging from man-made problems relating to business continuity of Estonian e-government, starting from cyberattacks or terrorist attacks, ranging to war […] you will have data, not just citizens, that you have to restart.

Even without the menace of the Russian Federation next door, it does make sense to have data embassies […] bearing in mind that the country today is not just carried by its citizens but by its data.”

(interview 15 - 12/10/18)

The notion or belief that Estonia could not ‘go back’ to operating with pen and paper, or rely solely on an analogue system of governance, is something that was encountered repeatedly whilst researching the Data Embassy2. As the quote above shows, the state’s growing dependency on its digital infrastructure has meant that relying on paper-based archives in the event of an emergency is no longer realistic, and that the Estonian state today is underpinned as much by its technological infrastructure and data as it is its citizenry and sense of national identity. In this section, I argue that this is indicative of a state-level anxiety in Estonia that is rooted in the archive and a post-Soviet collective memory.

---

2 Broadly, these conversations would centre around the lack of a paper trail and the dependency this created on Estonia’s contemporary digital society: “our data is not mostly backed up on paper anymore – it used to be” (interview 18 - 07/11/18); “What we learned is that we have to be so dependent, we can’t go back on paper” (Taavi Kotka interview - 15/07/19). But I also encountered a similar narrative whilst discussing other significant political moments in Estonia’s recent history. For example, following the 2007 cyberattacks, one cybersecurity expert told me, “Between the customers and electronic banking. Everybody was not ready to go back to paper” (interview 20 - 27/11/18) - whilst another civil servant identified similar concerns following the recent ID card crisis (interview 13 - 03/10/18 – see section 4.2.1).
The past two decades or so have seen an explosion of interest, not just from archivists and historians, in the notion of the archive (see, for example, Manoff, 2004; Schwartz and Cook, 2002). For centuries, the archive – understood as a “collection or ensemble of material that documents the past” (Mills, 2013: 703) – has enabled states to accumulate vast quantities of historical knowledge and information, whilst facilitating the governance of a given territory or population in the process (see, Derrida, 1995; Foucault, 1972). Moreover, the growth/development of national archives has also played a foundational role in the legitimation of states, and are thus considered crucial sites in the formation of national memory and identity (Featherstone, 2006; Manoff, 2004; Ogborn, 2003; Yale, 2015). Consequently, archivists and historians no longer view the archive as a “neutral, transparent site of record” (Merewether, 2006), but instead as a contested subject and site of analysis itself. Thus, the archive has become a crucial site of inquiry for a wide range of scholars, not only in an attempt to unlock the archive’s many historical and sociopolitical testimonies, but also in providing “a window onto current debates and common concerns in many academic fields” (Manoff, 2004: 9). As such, the archive is now recognised for its inherent political dimensions, with a number of studies demonstrating an array of colonial/imperialist (Craggs, 2008; Duncan, 1999; Richards, 1993), institutional (Davies, 2000; Mills, 2013) and even personal (Burton, 2003; Ashmore et al., 2012) archival histories.

In the context of this research, I am particularly interested in the role the archive plays in state formation and how archival histories play a significant part in the collective memory of the state today (see, Brown, 2013; Josias, 2011; Peters and Besley, 2019). Elizabeth Yale’s (2015) writings on the archive open up some of the tensions that exist, particularly for states, between the ‘archival ambitions’ of information mastery and impartiality (see Richards, 1993), and the ‘archival realities’ of partiality, anxiety and failure to access (see Pink et al., 2018). This tension – between the desire for complete conformity and control of the digital state, and the archival realities of historical data loss and potential future inaccessibility (see Section 6.1.2) – is central to understanding Estonia’s anxiety in relation to the Data Embassy.

In order to understand Estonia’s archival anxieties a little better and how they are manifest in state practices today, it is worth reflecting on the country’s own archival history and its trajectory taken from analogue to digital archival practices over the last century. After independence was gained in 1918, Estonia had made significant progress in its own archival practices, but this “natural development” was interrupted by Soviet occupation in 1940 with the archives of all three Baltic states “forced into a Soviet framework with Stalinistic methods and communist ideology” (Pillak, 1990: 577 – see, also, Grimstead, 1981). Significant reforms to Estonian archives in the late 1980s – driven, in part, by Mikhail Gorbachev’s Perestroika movement at the time – did lead to the restructuring and declassification of a number of state repositories (Pillak, 1990), but this period of ‘glasnost’ in the archives’ (Grimstead, 1989) still did not account for the

---

3 This also speaks to a growing body of research across geography that engages with the archive (see, Featherstone, 2006; Gagen et al., 2007; Kurtz, 2001; Mills, 2013; Withers, 2002).
substantial damages/losses incurred during the occupation period. Many Estonians have referred to this period generally as ‘lost time’ (see Section 4.1), but it is also worth considering the objects, documents, or records that were ‘lost’ during that period and how their material absences are felt today as part of the country’s collective memory (see, Naylor, 2020; Tamm, 2013). As noted in Chapter 5, a number of interviewees have reflected on how, in the aftermath of independence, anxieties were manifest in the material absence of certain archival records:

“When we restored our independence in 1991, it was like “how to know who is Estonian?”, “how to give them citizenship?”, “how to know what land is owned by who?”, and they looked towards old church books and records from the Old Republic to see who were the descendants and so on.”

(interview 6 - 18/05/18)

In an attempt to allay some of the archival realities faced regarding Estonian citizenship and land redistribution, one of the first steps taken by the restored Republic was to establish a Population Register (Riigikogu, 1991) and Land Register (Riigikogu, 1993). Both databases were deemed critical in the aftermath of independence, facilitating the governance of “territory and population through accumulated information” and data (Featherstone, 2006: 591). But their establishment can also be viewed as a notable precursor to the digitalisation of state infrastructure and public services that began to accelerate during the late 1990s and early 2000s, as Estonia rapidly transitioned towards becoming a self-proessed digital society or ‘e-state’ (see Chapter 4). In a similar vein to the adoption of a ‘paperless’ governance policy in 2000, steps were taken to convert many of the state’s critical databases and registries to existing only in digital form. For example, the database for the Population Register was the first to become wholly digital in 2000 (Riigikogu, 2000), while all Estonian healthcare records were digitised in 2009, and both would soon connect to other critical databases and information systems via X-Road infrastructure. As Chapter 4 considered, however, it is this distinct lack of a paper trail - and the evidential value each respective register or database holds – that is a great source of anxiety for the state, and one that is predicated on the establishment of the Data Embassy itself.

For public officials (many of whom had grown up under a totalitarian system of governance as part of the Soviet Union), the rapid digitisation of infrastructure and public services presented many novel challenges.

---

4 As Estonian archivist Peep Pillak has acknowledged, many Estonian archives had suffered from “pointless and excessive restrictions that had obstructed the development of historical studies and hindered the[ir] arrangement” (1990: 578 – see, also, Kuubben, 2003). Reflecting on the spatial history of the archive, Mike Featherstone notes how (particularly in a post-colonial context) archives were often destroyed, stolen, purchased and relocated, meaning that for “formerly subjected peoples […] constructing the national memory from the archive was often problematic as the archives had generally been shipped to the European imperial centres” (2006: 592). Anton Weiss-Wendt points to a similar problem and history in an Estonian context, noting how “the KGB evacuated a large number of documents from the archives of the Communist Part of Estonia (now a brand of the Estonian State Archives) to Moscow in 1991” (1998: 308).
What would happen if the state’s critical databases and registries – now only existing in digital form – suddenly became compromised or no longer operational? An even worse scenario for many to comprehend: what would happen in the event of Estonia losing its political independence once more?

“One should be as serious about how well do we protect our own databases, so that any foreign government wouldn’t get their hands around the Estonian national registry or something like that.”

(interview 9 - 28/05/18)

Since the late 1990s, Estonian archivists and policymakers have been cognisant of the risks posed towards their national databases and archives, with concerted efforts being made to introduce systematised disaster recovery processes (Kuuben, 2003; Tiidor, 2003). But, as the country began to transition towards adopting a system of wholly digital databases and archives, there was a heightened recognition of the threat this posed to the function and legitimacy of the state. By way of stressing the intrinsic value and indispensability of Estonia’s digital databases and archives, § 103 of the Population Register Act (2000) states: “If there is any danger that, in the case of a state of emergency or state of war, the population register becomes a threat to the security of persons or national security, the use of the population register shall be suspended by an order of the Government of the Republic or by the chief processor” and that “the chief processor is required to take measures to preserve and protect or destroy the data in the population register” (Riigikogu, 2000). In other words, as Jason Thompson suggests, the data held on the registry is considered “so vital to the functioning and legitimacy of the Estonian state that it must be protected at all cost[s]” (2019: 18).

The inherent security risks and challenges associated with a shift towards digital archiving practices have also been recognised in wider literature, with scholars becoming increasingly attentive to the spatiality and function of the digital archive (Beer and Burrows, 2013; Featherstone, 2006; Peters and Besley, 2019). For Mike Featherstone, the digital archive signifies a step away from the archive’s traditional physical confines (the national museum, library or centralised state repository) and its associated “bureaucratic forms of control and surveillance” (2006: 595). Rather, building on a Foucauldian and Derridean understanding of the archive, the “decentralized digital archive takes the form of a database in which, depending on the access coding, knowledge becomes freer to flow through decentred networks” (2006: 595), thus providing a “fluid, processual, dynamic archive, in which the topology of documents can be reconfigured again and

---

5 Indrek Kuuben notes how the opening of Estonian archives, after living under a totalitarian system for a prolonged period, occurred quite rapidly, and thus caused some instability “because new norms have not been established yet and old norms are not valid anymore” (2003: 19).

This section has so far illustrated Estonia’s own distinctive archival history that I believe has shaped the emergence of the Data Embassy over the last decade. In doing so, I have also examined a transformational shift in state practice over the past twenty years or so – from analogue to digital – that has seen the proliferation of digital technologies and practices across society. But, as the conversation at the beginning of this section illustrated, such a shift has also accentuated many of the ‘archival realities’ Estonia now faces, as the country becomes more and more dependent on its technological infrastructure and the security/preservation of its digital archives. Such a dynamic has ultimately served as a catalyst for the Data Embassy, as the state has been impelled to consider ‘futureproofing’ the state’s archives and information systems, ensuring what it calls ‘digital continuity’, against an increasingly dependent and fragile digital ecosystem.

Before we see the Data Embassy materialise, however, yet another fascinating archival practice emerges, as the state began taking steps to safeguard its critical digital databases and archives by periodically backing them up to Estonian embassies around the world (see Section 5.1). Although this practice would prove to be a forerunner to the Data Embassy itself, what struck me most were the novel processes involved here and what this may inform us about Estonia’s material, archival anxiety. The process itself – ‘backing up’ critical databases and archives to magnetic tapes, and physically transporting overseas via the diplomatic bag – is representative of the state reconnecting to its traditional archival practices, at a time when Estonia seemed intent on moving towards its vision of a ‘digital utopia’ (*The Guardian*, 2016). In other words, in facing up to a number of perceived existential threats and archival anxieties, the state in effect *returned* to the purported safety of the material archive and its associated forms (in this instance, the magnetic tape, diplomatic bag, and the diplomatic immunity afforded by the foreign embassy in another territory).

The subsequent emergence of the Data Embassy in 2018, then, represents the latest development in Estonia’s compelling archival history. Seen as the pragmatic and logical ‘thing to do’ in light of transformational shifts in state practices, as well as a growing dependency on the state’s digital infrastructure and information systems, the Data Embassy can be seen as a major step forward in attempts to tackle many

---

6 Featherstone also touches upon some of the inherent dangers regarding wider shifts towards the digital archive, noting the “accumulation of transnational information” and the problems “digital flows beyond the nation-state” now pose (speaking to relevant debates around data sovereignty and extraterritoriality – see Section 2.1). He also goes on to discuss the dangers of a ‘cancer culture’ developing in the digital archive, due to “unperceived degradation” (2006: 595). I make a similar argument in the following section (6.1.2) as I discuss state-level anxieties regarding technological advancements, such as the advent of quantum computing, and the threats this poses to existing cryptographic algorithms and information systems.

7 This shift by the Estonian government, recognising its increasing dependence and necessity for ensuring digital continuity, also speaks to a growing body of academic work and policy discourse in Estonia around the practice digital archiving and preservation of digital records (see, Karberg, 2014; Oliver and Konsa, 2012; Pappel et al., 2017).
of the state’s archival realities faced since first gaining independence in 1918. But in doing so, the emergence of the Data Embassy also demonstrates that the state and its archival practices cannot be easily separated from its material, Soviet past. As this section has shown, and as evidenced in the archival practices and concerns over being able to ‘return to paper’ in the event of an emergency, Estonia’s anxiety is rooted in a post-Soviet geopolitics and collective memory that is inherently bound to the material archive.

6.1.2 Wiping the state clean: Estonia’s paranoid yet anticipatory future

During a number of interviews with Estonian respondents, it was not uncommon to experience a direct sense of apprehension over the future state of Estonia’s digital society:

“What if you need some information that was there in 2018 or 19 [...] and [it] doesn't exist on paper anymore?”

(Taavi Kotka interview - 15/07/19)

Similar feelings have been expressed across government discourse on the Data Embassy (MoEAC, 2015; 2016), where, brought together, the possibility of future data loss, technological obsolescence or an inoperative digital society all provide a persistent source of anxiety for the state. Whilst the previous section considered an anxiety that could be identified through the material archive and Estonia’s Soviet past, in this section the focus turns to the enduring uncertainties the state faces over its ‘unknown’ future, arguing that Estonia’s anxiety and ontological insecurity can be understood through its own ‘data futures’.

The term ‘data futures’ is derived from Sarah Pink, Debora Lantzeni and Heather Horst’s (2018) work on the everyday anxieties citizens face in relation to data. For Pink et al., living in an increasingly ‘datafied society’ (Schäfer and van Es, 2017) – whilst offering many purported benefits - can mean living with perpetual anxiety: from the realities of the ‘messiness’ (Dourish and Bell, 2011) of data in our everyday lives, to the uncertainties associated with how data might be (mis)used or accessed, and anticipation around its loss (Pink et al., 2018: 2). They go on to suggest that we also live in age where people increasingly feel that their data is no longer secure, and could be “lost, stolen or somehow compromised” (Pink et al., 2018: 12). As such, a general malaise exists over our so-called ‘data futures’, where “living with data means living in a world of uncertainty” (ibid). Often, it is this uncertainty – or impossibility of not knowing our future – that leads to what psychoanalyst Rollo May refers to as “a perpetual condition of tension and worry” (May, 1977: 14), where data anxieties now appear part of our everyday lived experience.

Of course, data anxieties are not solely consigned to individual experiences. In an age of ubiquitous computing, internet-connected devices and large-scale data sharing, cybercrime and corporate data breaches are now an enduring fixture in our everyday lives. As such, businesses and governments, too, find
themselves in a perpetual condition of anxiety with regards to data and the security of critical infrastructure/information systems. I adopt the term ‘data futures’, in the context of this research, to refer to the collective state-level anxieties Estonia faces with regards to the possible future threat of data loss, technological obsolescence and incapacitation of the state. Building on the archival realities outlined in the previous section, I suggest that, despite Estonian authorities taking great pride in their many technological advancements and role as ‘digital pioneer’ (see Section 5.3), the “lingering future possibility” (Pink et al., 2018: 4) of threats facing Estonia is indicative of an anxiety I believe the state is experiencing.

The angst and uncertainty around Estonia’s ‘data futures’ can be understood in three specific contexts. The first relates to the everyday geopolitical risks Estonia faces, and how concerns over future cyberattacks and military escalation present significant threats to the security and preservation of the state’s information systems and digital archives, as well as the function and legitimacy of the state itself. Drawing on Estonia’s everyday geopolitics (see Section 6.2), such anxieties can be understood in the context of both historical and present events (e.g. prior Soviet occupation, 2007’s cyberattacks and the ongoing conflict in Ukraine and annexation of Crimea in 2014), and can be evidenced through Estonia’s everyday security discourse, geopolitical culture and notion that ‘it might happen again’ (see Section 5.2).

The second concerns the technological risks that threaten the functionality of Estonia’s digital society both today and in the future. In the previous chapter (see Section 5.1), I outlined the dangers that archivists (and, by association, states) face in the future as digital archives risk becoming inaccessible, illegible or obsolete “by the pace of innovation in information technology” (MacLean and Davis, 1999: 11). In the context of this research, I extend this beyond the archive to include vulnerabilities pertaining to Estonian information systems and technological infrastructure. Such anxieties are not only predicated in the establishment of the Data Embassy itself – as a means of safeguarding or ‘futureproofing’ critical information systems and infrastructure – but are also manifest in key government policies, such as the ‘no-legacy’ principle which mandates that all public sector IT systems and technology should be replaced after thirteen years (see Section 4.1). Furthermore, this speaks to wider concerns throughout the information security community regarding the pace of technological development, such as the advent of large-scale quantum computing, and the risk this poses to cryptographic algorithms deployed today8 (see Smith III, 2020).

---

8 The worry for many cryptographers and information security experts (and, by association, states and their security services) is that as technology improves, cryptographic algorithms that are used to secure data today could be ‘broken’ in the future. This is an obvious anxiety for the Estonian government too, with the risk that data that are secured in critical databases (such as the Population Register) could be ‘breakable’ in ‘x’ number of years. Public-key cryptography, which Estonia relies heavily on, is a particular vulnerability here, with the understanding that popular cryptographic schemes – such as RSA and Elliptic Curve Cryptography – “will easily be broken by a quantum computer” in the future (ETSI, 2020). This has obvious repercussions for global information infrastructures, compromising the confidentiality and integrity of data and information over the internet and modern forms of storage (such as the cloud). Although it is unclear as to when large-scale quantum computers will be ready, there is now extensive work taking place in the information security community (led by NIST, the eminent international standardisation authority) to develop quantum-resistant public-key algorithms that enable systems are secure if and when that time comes (see, NIST, 2017).
The third and final context concerns human risk. As Estonian archivist Indrek Kuuben has argued, risks threatening archival premises and archival records can emerge from “both technical and human factors” (2003: 19), and thus it is prudent to expect that Estonia’s digital society is not impervious to the threat of human error - more so given the inherent complexity (and dependency) of its critical infrastructure. Whilst human errors can often be managed or mitigated against, a considerable threat remains in the form of deliberate sabotage and the danger of critical information systems/archives being damaged, corrupted or destroyed by an ‘insider threat’. The fear of a potential powerful insider is grounded in a post-Soviet geopolitics and is intrinsically linked to an Estonian geopolitical culture and everyday security discourse that has an inherent suspicion of espionage against state institutions. Although it could be argued that the likelihood of this occurring is relatively low-risk, I contend that the notion of an ‘insider threat’ still contributes to a paranoia and anxiety that is embedded in the collective memory of many Estonians, and thus the decision-making practices of the state and its elite, today.

6.2 Estonia’s everyday affective geopolitics

Whilst the previous section explored how Estonia’s anxiety is manifest in the materiality of the archive and Estonia’s ‘data futures’, the following section examines how this anxiety is also formed as part of an everyday affective geopolitics. Focussing in on some of the everyday practices and rituals of the state and its elite – both historical and contemporary – my aim is to identify how Estonia’s anxiety is lived and felt, through both the collective memory of the Estonian elite and the state itself, and an ‘everyday geopolitics’ that continues to be shaped by the Russian threat and the state’s own ontological insecurities. In doing so, I recognise the different temporalities to Estonia’s state-level anxiety, and how it is shaped by (and intensifies around) particular historical ‘moments’ and geopolitical events, forming part of a post-Soviet collective memory in the process.

First, I explore how anxieties around the preservation of Estonian archives and the continuity of the Republic are lived and felt through particular moments of country’s collective memory and Soviet past (Section 6.2.1). Building on the work of Marek Tamm (2008), I examine how certain events or political moments from the past are often foregrounded and linger in the collective conscience today, and question what role this may play in the establishment of the Data Embassy. Second, drawing on Gerard Toal’s reading of an affective geopolitics and interest in the forcefulness of affect and emotions in world politics, I explore how Estonia’s anxiety is experienced and felt today (Section 6.2.2). Grounded in contemporary

---

9 In an information security context, human error can refer to the unintentional actions – or inaction – of an employee that could lead to a security incident (such as a data breach, or system failure). For example, IBM’s ‘2014 Cyber Security Intelligence Index’ found that 95% of all security incidents involve some form of human error (Pham, 2014).

10 The notion of ‘insider threat’ could take many forms. For example, an informant may wish to simply cause significant damage to Estonian information systems on behalf of a foreign power. Or, an informant may also attempt to perform a form of ‘data dump’ (in the style of U.S. whistle-blower Edward Snowden) in order to expose vast swathes of private citizens’ or intelligence data.

11 Since the collapse of the Soviet Union in 1991, there have been numerous cases of Russian espionage being conducted in Estonia – some even reaching the higher echelons of power in government. By virtue of the country’s history and demographics, inevitably ‘sleeper agents’ from the Soviet-era were found to be recruited by Estonia’s security services – since 2009, twenty individuals have been convicted of working for Russian intelligence agencies, such as the Russian FSB (see, Juurvee and Perling, 2019; Weiss, 2019).
political discourse and the actions of the Estonian state and its elite, I argue how this anxiety is often found to intensify and ‘stick’ to significant political moments in Estonia’s contemporary history, and how these influence the practices of the state today.

6.2.1 ‘It is still in the back of the head of our people’

On 14 June 1940, the Finnish passenger plane Kaleva (see Fig. 6.2), en route from Tallinn to Helsinki, was shot down by two Soviet Ilyushin DB-3 bombers shortly after take-off from Ülemiste Airport. Badly damaged, the Kaleva plummeted into the Gulf of Finland, a few kilometres northeast of the Estonian island of Keri, killing all nine passengers and crew on board. Among the dead were a number of diplomatic personnel (including two French diplomatic couriers and U.S. diplomat and code expert Henry W. Antheil Jr) carrying 227kg of diplomatic post (see, Johnson and Hermann, 2007; Rislakki, 2014).

Figure 6.2 – An image of Kaleva, the civilian passenger and transport plane that was shot down while en route from Tallinn to Helsinki on 14 June 1940 (source: Helsingin Sanomat Oy/HS Arkisto)

With the Soviet Union denying any involvement and an official Finnish inquiry into the incident remaining somewhat ambiguous, several conspiratorial theories surround the downing of the Kaleva. Timing would appear crucial. That day, the Soviet Union had enforced an air and naval blockade on the Baltics that ultimately served as a prelude to their annexation just three days later (see Section 1.1). Because of this, there are many Estonian legends that believe the plane was being used to transport the country’s remaining gold deposits to either Helsinki or Stockholm, whilst other theories posit that Joseph Stalin himself directly ordered the Kaleva flight to be shot down, after being convinced that Estonian President Konstantin Päts was onboard and attempting to flee into exile (interview 6 - 18/05/18 – see, Johnson and Hermann, 2007). Given the impending Soviet blockade, however, the most plausible theory remaining today is that the plane was downed to prevent any key diplomatic correspondence from leaving the Baltic states and reaching

---

12 At the time, the Finnish commission investigating the crash were cryptic in their explanation of the crash, concluding that “the explosion […] was caused by an external factor that the commission has not been able to ascertain” (Rislakki, 2014: 608). Historians have questioned whether this reticence from the Finnish government was an effort to allay any tensions with the Soviet Union following a peace pact signed a few months prior – although they would later go on to release full details of the crash and fully implicate the Soviet Union in the incident (Van Hare, 2013).
Despite these conflicting narratives, for many Estonians it is the story and mythology surrounding incidents such as the downing of *Kaleva* that still serve a very certain purpose. As this short vignette aims to demonstrate, anxieties around the preservation of Estonian archives (or in this case, diplomatic post and gold) and the continuity of the Republic can often be traced back through particular moments of the country’s collective memory and Soviet past. Estonian historian Marek Tamm (2008) notes the importance that narratives and their (re)construction play in the process of memory work. “Every community, including the nation,” writes Tamm, “is based on ‘stories we live by’, on narrative templates which give coherence to a community’s past” (2008: 510). And, as I found in conversations pertaining to Estonia’s political independence (see Section 5.2.1), the use of such narratives can similarly feed into sensibilities expressed today. Recounting the *Kaleva* incident, and how such events can help to shape perceptions vis-à-vis the Data Embassy and Russia, one interviewee posited, “I think it is still in the back of the head of our people” (interview 6 - 18/05/18).

The notion that incidents such as *Kaleva* still remain ‘in the back of the head’ of many Estonians today is something that plays central to my understanding of Estonia’s anxiety and its relationship to the Data Embassy. Specifically, it points to anxiety’s “quality of indefiniteness” (Stonebridge, 1998) and spatial temporality (Zevnik, 2017) as it ‘sticks’ to certain political moments both historical and present. To help unpack this, if we consider one of the more dominant narratives that has so far shaped the Data Embassy – Estonia’s everyday security discourse and relationship to Russia (see Section 5.2) – then this is not to signal that there is any kind of imminent threat against Estonia and its state institutions. Nor is it to suggest that there is a widespread (and somewhat irrational) fear amongst the Estonian population that Vladimir Putin and a revanchist Russia has ‘blueprints’ over its ‘next move’ in the Baltics (although it is likely that such fears certainly do exist). Instead, I believe it points to a recognition of, or an alertness to, a threat/danger that could conceivably happen in the future – one that is often based on historical experience - but with no real indication of when.

This is not to claim that Estonia’s threat perception, and thus its judgement relating to the creation of a Data Embassy, is somehow irrational or misguided (see Section 6.3). Rather, anxiety is a useful analytic for making sense of how the looming presence of Russia and other anxieties around data and the archive seemingly linger in the background – rarely dissipating or disappearing completely – only to intensify/foreground once more around particular political moments or collective memories (such as Soviet occupation, the 2007 cyberattacks or Russia’s annexation of Crimea in 2014). In relation to Russia, the

---

13 For other studies that focus on Estonian or Baltic collective memory in a post-Soviet context, see: Hackmann, 2008; Onken, 2010; Perchoc, 2019.
Estonia-based academic Wolfgang Drechsler perfectly articulates how such an anxiety is able to manifest itself in Estonian public life today: “Perhaps, one can say that in regards to the Russian danger, the off-chance that something might happen, is just big enough in Estonia that one can never neglect it” (Drechsler, 2018: 13). In many ways, it is this ‘off-chance’ or sense that ‘it might happen again’ (see Section 5.2) that is central to an understanding of Estonia’s anxiety, and how it shapes the ontological security of Estonia today.

However, in this thesis I am also interested in how Estonia’s anxiety operates beyond an individual level and the disposition of the ‘everyday Estonian’ (indeed, such a task would prove complex and require further research, ultimately beyond the scope of this thesis). Rather, the aim is to demonstrate how this anxiety is felt and experienced collectively in Estonia, and how it is most prominently felt at a state level, where an everyday affective geopolitics (that is often fixated on Russia and Estonia’s ontological insecurity) can lead to anticipatory security logics, such as the Data Embassy, to take form. In the following section, I take a closer look at Estonia’s everyday affective geopolitics, examining what impact this may have on the development of the Data Embassy and the state’s ontological (in)security.

6.2.2 Affective investments: from everyday security theatre to the reassurance of the Data Embassy

On 23 June 2014, Estonian President Toomas Hendrik Ilves delivered a speech to the country celebrating Võidupüha (or Victory Day), a day which commemorates the defeat of German forces in 1919 during the Estonian War of Independence (see Fig. 6.3). Each year, the Victory Day speech provides a platform for the Estonian president to reaffirm the state’s defence capabilities, and broader security commitments of its allies, to members of the Estonian Defence League (the country’s voluntary paramilitary armed forces) and wider public. This annual rehearsal of statecraft, with its customary rousing rhetoric regarding the security and defence of the Republic, is in many ways a means of providing reassurances and ontological security to the Estonian people14, whilst there may be some critics who simply denounce it as nothing more than ‘security theatre’. In 2014, however, Ilves’ speech was delivered under more testing circumstances than years gone by, amidst the backdrop of increasing geopolitical tensions following the annexation of Crimea:

“Let us not live in illusions. The foundations of the security architecture on which we, along with our allies, relied for 23 years, are gone. We’ve been constantly soothed by people who insisted that no more territories would be annexed in Europe; no more countries would be militarily attacked.

---

14 For example, in her 2019 Võidupüha speech, President Kersti Kaljulaid stated that “Estonian security begins with every person’s own sense of security” (President.ee, 2019). In his 2007 speech, President Ilves stated “Security also means that Estonians need not fear for their country or themselves [...] Let us call the absence of such fears the psychological defence of our fellow citizens” (President.ee, 2007).
Yet, it turns out that countries are still attacked, territories are still occupied and annexed […]

What we see in Eastern Ukraine today, we saw in Estonia in 1940 and 1919. We cannot, and often don’t even want to imagine how fragile the wellbeing that we’ve got used to really is; how fragile is the peace around us, our independence and our freedom. Just like no one could imagine it in the cafés of Tartu or the farms of Valgamaa in 1938.

Now we know how costly this illusory sense of security soon turned out to be.”

(President.ee, 2014b)

Such pointed rhetoric, particularly at a period of intense unrest within the Baltics, was anticipated, sending a clear message to the Estonian people and its allies that the foundations upon which Western freedoms and security rest are fragile and increasingly under threat. Yet, it is through the these (sometimes rehearsed, sometimes more improvised or even banal) everyday practices and performances of the state, that I argue that Estonia’s anxiety is perhaps most embodied, visible and present today.

To that end, in the remainder of this section I examine how Estonia’s anxiety is manifest in the everyday practices and performances of the state and its elite. In doing so, I highlight the embodied and emotional qualities of Estonian statecraft, and how Estonia’s anxiety is lived and felt through an affective geopolitics that, in turn, is conveyed through the state’s own security discourse, and diplomatic and geopolitical culture. For Gerard Toal, affective geopolitics concerns the forcefulness of affect and emotions in world politics, and how certain events or political moments can trigger “powerful emotions” and “moments of ritualized enactment” that are “automatic and unconscious, below or barely at the level of consciousness” (2017: 12-13). Again, drawing on key events and political moments in Estonia’s recent history – such as the 2007 cyberattacks and Russia’s annexation of Crimea - this section explores how this everyday affective geopolitics contributes to the anxiety that is at the heart of the state, and how this may have also played a role in the development of the Data Embassy. As I go on to show, not only does this everyday affective geopolitics centre largely around Estonia’s relationship to Russia, but also concerns the country’s
geopolitical culture and how it sees itself in the world (for example, Estonia as the plucky survivor; the post-Soviet transitional success; the new (and law-abiding) kid on the bloc in NATO and the EU; and now, the digital pioneer).

As stated in the previous chapter, the 2014 annexation of Crimea played a significant role in the establishment of the world’s first Data Embassy (see Section 5.2). Indeed, not only did events in the Donbas region of eastern Ukraine lead to arguably one of the worst geopolitical crises in Europe since the Second World War, but, for many Estonians, it perpetuated a belief that ‘it might happen again’ and that Estonia’s political independence could once more be under threat. It is at this moment, when the annexation and subsequent conflict served as the most prominent “warning bell” (Taavi Kotka interview - 15/07/19) for its politicians and policymakers, that I explicated how those in the Estonian elite were most convinced by the Data Embassy and the idea of ‘backing up’ the state (see Section 5.2.2). Reflecting Estonia’s everyday security discourse at the time - where the Russian threat was perceivably at its most heightened since the regaining of independence - it is also the moment where I believe Estonia’s anxiety/ontological insecurity was at its most salient, epitomised by the state’s overarching decision-making culture, as well as the wider political discourse and diplomatic culture of its elite, at the time.

On top of the decision to establish the Data Embassy, Estonia’s growing anxieties were made manifest in an everyday affective geopolitics – centred largely around Russia and the state’s own ontological insecurities – that was embedded in, and amplified by, the political discourse and geopolitical culture that was being curated and framed by the Estonian elite during this period. Whether this was through the use of powerful, “affectively loaded” (Koschut, 2017: 483) political rhetoric in speeches and interviews (as shown by President Ilves above), calculated social media posts online, or the role of media sensationalisation and headlines both in national and international press (see Chapter 3), Estonia’s anxiety was lived and felt through many of the everyday practices and performances of the state and its elite. Similarly, in 2007, in the aftermath of the Bronze Solider incident and the subsequent cyberattacks against the state, comparable powerful political discourse was utilised by the state, whilst it could be argued that Estonia’s security discourse (including its approach to defence and cyber) changed overnight (see Section 5.2.2). Speaking just months after the incident, once again during Victory Day celebrations, an affronted President Ilves outlined the severity of the attacks upon which the country had just faced:

“The recent months have shown that Estonia’s independence is not to everyone’s liking. Our democratic order, rule of law, freedom of speech, tolerance, and the Estonians’ desire to live our lives our own way seem, for some, to be something that is to be undermined and weakened. For this purpose, devices have been used which, in the Western notion, are not part of the conventions of civilisation.
This spring, Estonia was hit by a serious onslaught. True, no howitzers were used and we could track no traces of Polonium. But our Embassy and our diplomats were attacked, and thus also the principles of the Vienna Convention ignored.

Worse still, our IT-infrastructure, which aspires to be on the top of the world, was assaulted in such a manner that NATO deemed it necessary to send its leading experts over to support our own top team and learn from their experience. Estonia was attacked with a weapon and in a manner whose full significance is just beginning to dawn on the whole world in the 21st century. Our banks, our newspapers, our public institutions were under attack. Those attacks were directed against Estonia, paying no heed to the nationality, political values or mother tongue of our inhabitants.”

(President.ee, 2007)

Despite proving difficult to attribute, Estonian political discourse at the time was clear and resolute in asseverating Russia’s responsibility for the attacks (see Section 4.1.2), whether through the rhetoric of political figures like Ilves or wider (inter)national media narratives. For instance, after facing a series of protests and attacks outside of the Estonian embassy in Moscow during the Bronze Soldier incident, Estonian Ambassador to Russia, Marina Kaljurand, told a press conference that she believed the protests and subsequent cyberattacks were likely orchestrated by the Kremlin (Yasmann, 2007) – a line that has been reiterated by other Estonian politicians and diplomats since. Estonia’s anxiety also evidenced itself in other everyday practices and performances of statecraft and diplomacy at the time, such as the development of the country’s first national cybersecurity strategy and the opening of the NATO CCDCOE in Tallinn, whilst regularly calling on allies in both NATO and the EU to offer their support and reassurances to the Baltic states. It is in the increased performativity of the state and its elite in these moments, that the anxiety reveals itself to be all-pervasive (as it registers across areas of the state’s apparatus and in the actions of its elite) and undulatory (as it recasts itself and ‘sticks’ to particular political moments and collective memories, doing so in a series of affective waves).

Such anxiety, therefore, speaks to a number of different temporalities that seemingly push and pull against one another. Taken in the context of 2007 and 2014, a crucial point to make is that both events were not unimaginable for the state and the everyday Estonian – rather, they were part of an already lived experience and collective memory. Indeed, these were not simply irrational fears regarding a perceived aggressive and hostile neighbour, but were instead part of an everyday affective geopolitics that is lived and felt by the
state and its elite. Yet, what makes this anxiety so interesting, not least to our understanding of how emotions and affects operate at a state-level in world politics, is again its “quality of indefiniteness” (Stonebridge, 1998) and the degree of ambiguity that exists around the ontological security of the state and the threats it currently faces. For instance, whilst it may seem that the state deems the Russian threat as something known and intelligible, it is also true that many of Estonia’s ontological insecurities are marked by unknowns and perpetual uncertainties regarding threats faced in either the physical or virtual domain. Whether it is a lack of clear evidence regarding the risks facing Estonia and the wider Baltic region vis-à-vis a purported ‘revanchist’ Russia under Putin (see Section 5.2.3), or the enduring uncertainties the state faces over its ‘unknowable’ future and its archives (see Section 6.1.2), the question of if or when a national crisis or some form of attack occurs (and by whom) is emblematic of the anxiety that sits at the centre of the state and its overarching decision-making culture of its elite.

Exacerbated by Estonia’s role as a small state, and the perceived fragility of its digital ecosystem and own political independence, there is a sense that the state and its elite have very little control over the existential threats it may face, which again leads to what May refers to as “a perpetual condition of tension and worry” (May, 1977: 14). Indeed, the eminent French philosopher Jean-Paul Sartre once proclaimed that anxiety exists when there is not a fear of anything in particular, rather a “pervasive unease about oneself and one’s existence” (Bakewell, 2016: 154). So, to take from Sartre in the context of this everyday affective geopolitics, is the anxiety Estonia is experiencing embodied by the state’s own ‘pervasive unease’ over its own functionality and existence? It is here, where that tension and foreboding sense of uncertainty is at its strongest, that I argue that the decision to develop exceptional and anticipatory measures such as the Data Embassy are most desired and necessitated. As the following section will go on to show, such measures also point to attempts by the state to manage and control the anxiety it experiences regarding its own ontological insecurities (see Section 6.3).

To briefly conclude, what does the arrival of the Data Embassy tell us about Estonia’s state-level anxiety and wider everyday security discourse? Principally, it reminds us that small states like Estonia are actively involved in the construction and framing of their own geopolitical melodramas. Seeking greater ontological security post-2007 and 2014, the state and its elite have been intent on reassuring its citizens against any existential threats it faces, whether through the powerful rhetoric of political speeches or a number of ritualised/rehearsed state performances. Whether these are simply forms of security theatre, or the effective methods of managing and controlling the anxiety it faces, the Data Embassy appears to offer something different: a way of displacing the state (and its critical information systems and data) in order to protect and preserve it in the future. In doing so, there is an affective investment in the Data Embassy from the state, its elite and citizens that again speaks to the different temporalities of Estonia’s everyday affective geopolities – one that is forward-looking (as a means of protecting the state, and anticipating the next crisis
or attack) and, at the same time, backward-looking (cognizant of its past traumas and resolute on never repeating them).

6.3 Estonia’s productive-anxiety
So far, this chapter has examined state-level anxieties in the context of the archive, data (in)security and Estonia’s everyday affective geopolitics. In doing so, however, it is fair to say that this anxiety has been framed through a fairly negative lens - first, as a means of reconciling past conflict/trauma and, second, as a means of ‘coping’ with the number of uncertainties and future unknowns the state faces today. This negative portrayal of anxiety presented a challenge for me empirically as I often found discussions with respondents on this topic quite challenging, particularly for those working for/close to the state:

“I wouldn't call it an anxiety, I would say that it's kind of a self-preservation instinct, because, in every few decades, we've been invaded in some way or another.”

(interview 11 - 01/06/18)

Did this point to a misunderstanding of anxiety, or its use in this particular context? Or was admitting being anxious, for some respondents, perhaps an admission that the state was somehow weak or woefully inadequate to defend itself?

This has led me to think more critically about the way in which anxiety and other emotions are understood and experienced across different spatial temporalities and contexts. Psychoanalyst Rollo May (1977) writes of how anxiety is frequently portrayed through a negative and ‘destructive’ lens, in a way that can often accentuate its many downsides. Yet rarely do we acknowledge any of anxiety’s positive characteristics, nor its function as a potentially productive affect. In certain contexts, anxiety can be extremely beneficial and constructive – a ‘signal’ with “representational charge” (Stonebridge, 1998) – enabling an individual to be extra alert and responsive to any imminent threat or danger, whilst allowing for additional precautionary measures to be taken in the process (Miloyan et al., 2019). To that end, this final section considers the role of anxiety in relation to the Data Embassy and its interpretation in an Estonian context. In asking ‘is there a potential upside to anxiety?’, I reflect on how my use of anxiety as an analytical register in an Estonian context was contentious for some respondents, before examining how anxiety may be being put to work productively by the state and its elite in order to place-brand and manage Estonia’s own ontological insecurities.

6.3.1 Ärevus: translating emotions in different cultures/contexts
During the completion of this research, a number of interviewees disputed the claim that Estonia was experiencing some form of state-level anxiety with regards to the Data Embassy:
“I think most people in the Estonian government would argue, you know, they would admit the claim that people in Estonia have anxiety, but our attitudes are actually pretty cold and rational.

You know, we don’t run around screaming that the sky is falling, because it’s not constructive and we don’t have the luxury of doing that.”

(interview 10 - 31/05/18)

This struck me, at the time, as an intriguing claim worthy of further investigation. On the one hand, it implied a contextual misunderstanding of the question as to whether Estonia was experiencing a collective, state-level anxiety. On the other, it pointed to a sense of uncomfortableness with the term’s attribution to an Estonian context, and how admitting that Estonia was experiencing an anxiety could be construed as being somehow weak, irrational and/or incessantly fearful of the threat posed by Russia. As the previous respondent continued:

“We do a lot of rationally calculated things…things that are rationally calculated to prepare for, deter, dissuade general Russian aggression. And of course, if it were to occur, to improve our ability to react to it. And, you know, I think the Data Embassy stuff…if its only business argument were of Russia, then maybe it wouldn’t quite justify it. But it’s not!”

(interview 10 - 31/05/18)

Responses such as these raise interesting issues and tensions about how anxiety is identified and understood across different temporalities and sociopolitical contexts.

Initially, I pondered whether the use of anxiety (translation: ärevus in Estonian) in this context was, for some respondents, an issue of misinterpretation. As noted in Chapter 3, political scientist Simon Koschut has written about the lexical and semantic variations of certain terms in different languages, cultures and contexts, suggesting how some emotions can become “lost in translation” (2017: 483). In terms of my own research, perhaps the use of anxiety in a political (and thus non-medical/theoretical) context was unfamiliar to some respondents, and how its usage was potentially being misconstrued as a form of mass diagnosis upon individual Estonians, or that Estonians were thinking irrationally with regards to the purported

---

15 In the quote above, for example, the respondent accepted that some individuals in Estonia may ‘have’ anxiety, but as Estonians are ‘pretty cold and rational’ beings more generally, how could Estonia possibly be characterised as anxious? This was at least my own interpretation of the situation, but it did reflect other conversations I had during my time in Estonia.
Russian threat. In response, a number of respondents instead emphasised the state’s ‘rationality’ with regards to the Data Embassy (see quote above), whilst one interviewee simply felt that another term was better suited:

“I don’t know if anxiety is exactly the right word. There is a similar word…just a feeling of understanding that there is a possible threat. Anxiety is perhaps…like being anxious about it, it’s not the same, it is a rational response to a perceived threat.”

(interview 18 - 07/11/18)

Ultimately, however, it felt that there was an inherent suspicion or scepticism around my use of the term (albeit by a small number of respondents who had direct connections to the state). Whilst this was felt, on the one hand, as an attribution of the state as being fundamentally irrational and illogical with regards to the Data Embassy (something that some respondents were keen to dispel), I also gained a sense that the use of anxiety also brought with it an uncomfortable association with the term’s negative connotations (as highlighted at the beginning of this section).

With this in mind, I want to finish this section (and chapter) by examining the way in which Estonia’s anxiety may actually serve as a productive affect, and how it may be being administered by the state as means of managing its own ontological insecurities, self-identity and position in the world. In the previous chapter, I reflected on how Estonia’s everyday security discourse played a central role in the government’s motivations behind establishing a Data Embassy (see Section 5.2). For Merje Kuus, Estonia’s security/sovereignty dichotomy – particularly around the framing of the Russian threat – has long held a crucial “productive function” (2002: 408) with regards to Estonia’s own ontological security, allowing for the state to continue on its path of rapid international integration whilst framing the Russian threat as something ‘known’ and ‘intelligible’. In the context of this research, I argue that Estonia’s anxiety serves a similar function with regards to the Data Embassy, allowing the state to continue to frame Russia and its other everyday insecurities clearly and unambiguously to its allies and wider international community. To be “productively paranoid” (interview 16 - 15/10/18), as one interviewee put it, also means that the state remains extra-vigilant of any potential risks/threats to its sovereignty and territorial integrity, whilst also allowing the government to implement certain anticipatory logics (such as the Data Embassy) into its policymaking and everyday functioning of the state. One interviewee went further and argued how Estonia’s anxiety also functions advantageously for the country’s position as a small state and how it wishes to place brand itself globally (see Section 5.3):

16 The irony of this quote being that ‘a feeling of understanding that there is a possible threat’ inadvertently describes the notion of anxiety that I have theorised throughout this chapter.
“We need to be visible, we need to show that we are there so that our political allies and military allies would still read about us. It’s like marketing […] So we need to do it at all times. That’s probably one of the sources of anxiety.”

(interview 28 - 17/07/19)

Whilst there are undoubtedly individuals that wish to suppress the state-level anxieties that are currently experienced in Estonia (as the quotes at the beginning of this section show), the state is in effect managing (and maybe even commodifying) its anxiety as a means of addressing the ontological insecurities it faces. To expand on this further, I draw on Rosanna White’s (2019) doctoral research on performing sovereignty in the Canadian Arctic. Writing about the anxieties the state faces over its authority and sovereignty claims in the region, White’s work examines how successive Canadian governments have engaged in highly visible and performative practices of sovereignty in the Arctic, and how these are constantly “evolving and adapting as the region continues to change politically, environmentally, economically and culturally” (2019: 20). White terms many of these performances as forms of ‘affective sovereignty-anxiety management’, as they attempt to reassure the Canadian population that the government is committed to securing and protecting the Canadian Arctic. In the context of this research, the performative practice of establishing a Data Embassy and ‘backing up’ the state to the cloud constitutes a form of affective sovereignty-anxiety management in and of itself, as the Estonian government takes the necessary steps to address many of its ontological insecurities it faces today (from the archive to the ever-present Russian threat). The arrival of the Data Embassy, alongside other examples of state practice and performativity, can therefore be considered a novel form of collective mood management – or affect engineering par excellence – as the state seeks to reassure and assuage the anxieties both its elites and wider public face regarding the future continuity of the Republic.

6.4 Conclusion: A Government-in-anticipation-of-Exile?
In this chapter I have argued that the decision to begin extraterritorially backing up state data and information systems outside of its own borders speaks to a collective anxiety that is found at the heart of the Estonian state. By revealing some of the everyday concerns over the fragility of the state’s archives and overarching digital ecosystem, or more existential concerns regarding Estonia’s political independence, I have shown that the arrival of the Data Embassy points to a growing anxiety that is lived, felt and embodied through the various practices and performances of the state and its elite. Recognising that the Data Embassy is part of a much deeper Estonian continuity project that is rooted in the collective memory of the state (as well as its people), I have argued that Estonia’s anxiety is one that is pervasive, undulatory and paradoxical. I have used the notion of anxiety – rather than fear – as I believe it best represents the various nuances and complexities at play in the decision to establish a Data Embassy, better describing the indefiniteness and distinct temporalities that characterise the threats and ontological insecurities Estonia faces today.
Throughout the chapter, I outlined three particular ways this anxiety has manifest itself. First, I identified Estonia’s anxiety through two distinct lenses – the archive and the state’s own ‘data futures’ – arguing that state-level anxieties are rooted not only in the archive and a post-Soviet collective memory, but in the “lingering future possibility” (Pink et al., 2018) of data loss and inoperable digital ecosystem (Section 6.1). Second, I explored how this anxiety is lived and felt through an everyday affective geopolitics, and how this is subsequently enacted by the various practices and performances of the state and its elite, particularly around the purported threat of Russia (Section 6.2). Third, I considered how anxiety is conceptualised and made manifest across different spatial temporalities and contexts, arguing that Estonia’s anxiety should be recognised beyond its negative connotations, and instead as an extremely productive affect that is being enrolled and managed by the state in order to address its ontological insecurities (Section 6.3).

In doing so, this chapter has contributed to our understanding of how different emotions and affects operate at a state-level in world politics in a number of ways. First, in capturing the different temporalities of Estonia’s anxiety, I have shown that emotions and affects can embody certain characteristics and qualities when considered across particular histories, contemporary moments or futures. In the case of Estonia and the spatial temporality of the Data Embassy, this is captured in attempts to make a future that manages the day-to-day anxieties the state faces – securing its past through the material archive, and securing its ‘unknowable’ future through its digital equivalent in an extraterritorial data centre. Consequently, the digital and non-digital are constantly informing one another - and how this anxiety is experienced by the state and its elite - with the process of digitisation not only helping to preserve the past but also manufacture more anxieties around a ‘unknowable’ future. Second, in capturing the various complexities and nuances to Estonia’s anxiety and how it operates at a state-level, we are reminded that emotions and affects can be culture and context-specific, and how these may be experienced entirely differently at either an individual or collective level. Furthermore, Estonia’s anxiety and journey towards establishing a Data Embassy shows us that states can experience and embody a patchwork of different emotive/affective states, as the state-level anxiety identified in this chapter was often found intertwining with feelings of confidence, trepidation, anger, confusion, or even fear itself.

In many ways, Estonia’s anxiety reminds us that there is an element of looking backwards to enable the state to be able to move forwards. But, as this chapter has shown, the temporal quality of Estonia’s anxiety has revealed that it is equally forward-looking in how the state seeks to manage and govern its everyday anxieties. Thus, by way of concluding, I want to consider how the Data Embassy allows us to think about the ways in which particular futures are calculated, imagined and performed by states, and how state-level emotions/affects like anxiety can be mobilised in an attempt to make specific futures known and actionable. In his work on anticipatory action, Ben Anderson (2010) argues that futures are anticipated and acted on through the assembling of different styles, practices and logics. Whilst practices consist of acts that make
specific futures present, logics are interventions that involve actions that aim to “prevent, mitigate, adapt to, prepare for or pre-empt specific futures” (Anderson, 2010: 779). Thus, the Data Embassy is a specific intervention and anticipatory logic that seeks to prevent, pre-empt and prepare for a future emergency or crisis. As such, the practice of backing up the state to the cloud can itself be considered a productive anticipatory logic for the state that is proactively taking measures to combat anxieties around the archive, data and the purported Russian threat.

Bringing these anticipatory logics into conversation with Fiona McConnell’s work on alternative forms of statehood and Governments-in-Exile (2009; 2016; Jeffrey et al., 2015), I argue that Estonia’s anxiety has mobilised the state in such a way that points to a Government-in-anticipation-of-Exile. Building on the collective memory, trauma and historical experience of past Governments-in-Exile during the Soviet period of occupation (see Section 1.1), I believe this enduring anxiety has forced the state and its elite to act creatively in a way that seeks to mitigate the ontological insecurities it faces and avoid returning to a past where Estonia’s political independence was once again under threat. States, particularly those facing existential threats from political conflict, economic crises or climate change, could stand to benefit from operating within and managing their collective anxious futures. Whilst the use of creative, anticipatory interventions like the Data Embassy can help states move closer towards living with a future that is known and actionable, rather than unknown and uncertain.
Figure 7.1 – The Tallinn TV tower - located just outside of capital. Built in time for the 1980 Moscow Olympics, the tower is a symbolic, material reminder of Estonia’s Soviet past (author’s own image)
Chapter 7 - The Data Embassy and Geopolitics and in a Digital Era

So far, this thesis has performed an extensive analysis of the Estonian Data Embassy, with a detailed focus on the case study of Estonia’s first Data Embassy, located in Betzdorf, Luxembourg. Not only has this analysis recognised some of the complex arrangements behind the Data Embassy’s primary motivations (see Chapter 5), and its role as a state anxiety management tool (Chapter 6), but has also outlined its potential utility for the Estonian state in the future. Yet, as this case study has been unpacked in greater detail, it is also clear that the Data Embassy’s utility extends far beyond the scope of Estonian geopolitics and its future statecraft. Indeed, as I have argued throughout this thesis, the Data Embassy has already evoked a number of distinct geopolitical possibilities and futures, whilst the utility and function of the state have also been called into question as we consider the number of potential permutations and wider impact of a future network of Data Embassies around the world in the future.

In this chapter, I consider the role the Data Embassy plays in reconfiguring many of our traditional conceptualisations of geopolitics, diplomacy and international law. By viewing the Data Embassy through the lens of what Jeffrey et al. (2015) term as anomalous geopolitical spaces – sites that embody “unrecognised, contested or alternative forms of geopolitics from that of a sovereign state” (2015: 177) – my aim is to highlight how the Data Embassy speaks to other forms of statehood and statecraft that deviate from international norms; but also recognise how the state is both imagined and performed within the unique space of the extraterritorial data centre. Building upon and drawing together some of the key themes addressed so far in this thesis – from state-level anxieties to novel forms of diplomacy – this chapter also aims to sketch out new directions of research in this area, as well as outlining possible future policy recommendations as the Data Embassy continues to elicit interest from other state (and non-state) actors.

In order to further examine the Data Embassy and the specific futures it may engender, this chapter is divided into two parts. First, I examine how the Data Embassy has opened up new debates regarding statehood, sovereignty and legitimacy in a digital age (Section 7.1). To do so, I analyse the practicalities of ‘hibernating’ the state and assess whether the Data Embassy would serve a useful function in the event of an emergency (such as the Estonian government being forced into exile), before then going on to explore how the Data Embassy has been reimagined in a number of different geopolitical contexts and futures.

Second, I examine what impact the Data Embassy could have on the practice of diplomacy in the future (Section 7.2). With a focus on the Estonian Data Embassy in Luxembourg, I explore what impact the concept may have on future diplomatic relations. In particular, I examine to what extent both Estonia and Luxembourg may utilise the Data Embassy strategically in the future, and what impact this would have on their standing and prestige on the world stage. Next, given the potential advent of more Data Embassies in the future, I go on to explore the changing nature of the embassy, questioning whether its definition should
be extended to reflect changes within diplomatic practice today; before then going on to critique the Vienna Convention in the context of the Data Embassy, and consider whether it is fit for purpose in a digital age.

7.1 The Data Embassy and the future of the state
In the opening chapter of this thesis, I discussed the hypothetical scenario whereby the Estonian state could effectively be backed up to the cloud – or put into ‘hibernation’ (Hammersley, 2015) – in the event of an emergency, only to then be ‘rebooted’ or restored once it was safe or suitable to do so. For states facing a number of existential anxieties, from natural disasters to armed conflict and cyberwarfare, backing up the state to an extraterritorial Data Embassy may be an appealing anticipatory logic (Anderson, 2010) in an increasingly uncertain world. Utilising such a practice may also provide ontological security for smaller states, similar to Estonia, affording greater perceived security and political legitimacy from the cloud. In just a few years, the Data Embassy has already helped to evoke a number of distinct geopolitical imaginaries around the future function and survivability of the state. In this section I examine these imaginaries in more detail, whilst also reflecting on the way in which the Data Embassy may be opening up new debates around statehood, sovereignty and legitimacy in a digital age.

Estonia is an opportune case study to explore these themes, as over the last two decades it has taken steps to experiment and ‘improvise’ (Jeffrey, 2013) with the state through the use of new digital technologies and services – from the use of digital identities (eIDs) to internet voting and e-Residency. As I noted in Chapters 4 and 5, Estonia is a country that is continually trying to reimagine itself virtually, beyond its own physical limitations, and how it now sees itself today as the quintessential ‘digital nation’ and ‘e-state’. In this section, I examine how the Data Embassy can be considered as yet another form of state improvisation by the Estonian government, asking whether its emergence may also recalibrate many long-held assumptions over twenty-first century statehood. First, I examine the practice of ‘hibernating’ the state, grounding this largely within Estonia’s own uncomfortable relationship with statehood, before then going on to consider the Data Embassy’s wider functionality in the context of an emergency (Section 7.1.1). Second, I explore how the Data Embassy has been reimagined in an array of geopolitical contexts, from mitigating the threat of rising sea-levels to the potential utility for state/non-state actors that lack international recognition or constituted territory, analysing the concept’s effectiveness within a conventional state system and how statehood may be constituted in a digital age (Section 7.1.2).

7.1.1 Hibernating the state: highly innovative or highly impractical?
Estonia-Estonians’ relationship with the state has, for a long time, been an uncomfortable one. From the initial birth pangs of statehood experienced after the Estonian War of Independence (1918-1920) to the unabating fifty-one years spent under occupation from the Soviet Union and Nazi Germany (1940-1991), it could be argued that there has been a perpetual sense of unease with regards to the state’s functionality and existence. This apprehensive relationship to (and with) the state continued following the restoration of independence in 1991, first during a period of ‘restoration geopolitics’ and early territorial/border disputes
with Russia in the 1990s (Aalto, 2003; Berg and Oras, 2000), and then secondly as Estonia joined the EU and NATO, with many at the time seeing this as a direct threat to Estonian state sovereignty (Kuus, 2002). Because of this considerable historical uncertainty (and, as some scholars point out, that the modern Estonian state has only existed in any free and meaningful sense for just over a century now – Drechsler, 2018), for many Estonians the idea that the state is somehow ‘fixed’ or permanent is not widely acknowledged. As one interviewee expanded:

“There is something in the Estonian disposition – and this is a very complicated semiotic argument going back to historical things – that Estonians have an uneasy relation even with their own state. And they can gamble with it because Estonians focus on their own society – the Estonian people that live here – so Estonians see their own state as only a vehicle to maintain the struggle in society, which they wouldn’t call society but the Estonian people. Therefore, Estonians can gamble with state institutions, rather than ‘well, we need to preserve them’, because for them if the state goes that’s not so important. What’s so important is that the people stay.”

(interview 21 - 28/11/18)

Today, this view of the state is largely manifest in Estonia’s geopolitical culture and vision as a digital society, and how it very much sees itself as a pioneering ‘digital nation’ or ‘e-state’. Wolfgang Drechsler (2018; forthcoming) has written about this and perhaps why it is that Estonians feel comfortable with the notion of the state operating like a startup (despite them often failing), and why this approach is deemed appropriate and acceptable for the country today (see Section 5.3):

“This is because the current official message from Estonia - the international government message, one that was used as the key note in the literal sense during the EU presidency in 2017 - is that the (nation) state, the Western [state], our state is dying.”

(Drechsler, 2018: 11)

Such a view of the state can also be traced through recent government discourse, particularly around the notion of Estonia moving towards a ‘country without borders’ or ‘country without territory’ (see Chapters 4 and 5). What these (I would argue, largely hyperbolic) slogans show, is that there are many of those in the Estonian elite that are keen to experiment and improvise with the notion of statehood – from the idea of digital nomads conducting business remotely across its purported porous, virtual borders (e-Residency), to the belief that the state does not have to be tied to its geography in the event of an emergency and can be operated from the cloud (Data Embassy). Whilst this view of the state not only helps to play into
Estonia’s geopolitical culture and image as a technological pioneer – as well as the idea that it is a country that is willing to push the boundaries of contemporary statehood - but I also believe it plays a significant role in managing the many existential anxieties it faces today, particularly around the Russian threat (see Chapter 6). This latter point is one that is shared by Drechsler, who suggests that the “original […] virtuality of Estonia as a Nation State, its continued perceived precariousness, and the continued potential threat by another, very successful Nation State (the old Colonial power), are the reasons why Estonia can so easily (and even wants to) abandon the idea of the classic Nation State” (Drechsler, 2018: 14).

Departing slightly from Drechsler’s argument here, I don’t believe that Estonia’s current view of statehood is anti-statist, or that its elite wishes to abandon the state altogether. Rather, I believe it points to a recognition and understanding that the classical notion of the state is increasingly unfit for purpose in a digital age, and that states may well have to adapt and adopt anomalous forms in order to function and secure themselves against existential threats in the future. Thus, because of these prevailing paradigms on statehood and state transformation (from historical uncertainties to its functionality within today’s digital world), I argue that the notion of the state not being tied to its geography has greater purchase in an Estonian context, where the Data Embassy’s emergence signifies an important and intentional disruption to the classic Westphalian notion of statehood.

Furthermore, due to this unsettled relationship with the state, it is also of little surprise that the imaginary of ‘backing up’ or ‘hibernating’ the state carries a degree of necessity and political capital from those within the Estonian elite at present. Indeed, not only is the process of state hibernation about the anticipatory logics of preparedness and self-preservation (Anderson, 2010) – practices that appear to be manifest in Estonia’s geopolitical culture and the collective memory of the state – but hibernation also serves as a mechanism for the state to recover and repurpose. Within such an imaginary, hibernation allows the state to enter a state of animated suspension – where the state’s critical databases and archives are preserved in perpetuity in the cloud – with the aim of restoring itself to its original status and functionality when it is prudent to do so. Throughout this period, the Data Embassy would in effect provide a degree of serviceability and nourishment to the apparatus of the state whilst in absentia, enabling key databases and digital services to continue to function in a form of abstracted state-level ‘safe mode’.

---

1 Estonia’s uneasy relationship with the state does of course sit paradoxically to the notion that Estonians today are generally more trusting in their state, especially in the realm of digital governance and the state/citizen relationship to data (see Chapter 4). As mentioned earlier in this thesis, further research into this relationship is required, but one rudimentary explanation may be that whilst Estonians may well be more trusting in its institutions today, there still exists a relative uncertainty over the state’s permanence and its role/efficacy for a twenty-first century digital Estonia.

2 When a computer or device is hit by a system-critical issue (such as a bug or corrupted hard drive), it is normally entered into ‘safe mode’. Whilst in safe mode, the operating system has reduced functionality, and this allows the operating system to diagnose and isolate any problems on that operating system, and for the user to troubleshoot any potential solutions. I’ve used the term safe mode here in the context of the Data Embassy, as I believe it usefully describes the process whereby the state is effectively put into hibernation (with reduced functionality) in order protect and preserve itself from a threat, whilst potential safeguarding solutions are found.
In the context of this research, I also argue that the practice of hibernation is a form of state improvisation (Jeffrey, 2013), and how this performative act could also be acknowledged as an attempt at conveying political legitimacy in the event of an emergency (see Section 7.1.2). For instance, in the event of a country being struck by a natural disaster or crippling cyberattack, or if a government was forced into exile, the Data Embassy would serve as an extraterritorial backup and fail-safe of the state’s most critical databases and digital services. In effect, this would allow for a government to continue to operate and function from anywhere in the world, with its extraterritorial Data Embassy providing the technological infrastructure necessary to ensure the availability of key databases and services from the cloud. From an everyday perspective, Nikolai Rice (2019) speculates on how this could work in the event of a future occupation of Estonian territory:

“Though territorially-occupied, Estonia’s international legitimacy, ingrained through its place in the United Nations, NATO, and the European Union, would likely provide it with ample international political space to operate either out of a series of embassies or even an office-in-exile, akin to the occupied Allies in London during WWII. Connected to its e-governance cloud infrastructure, the Estonian government could actively and routinely support its citizens by continuing to use the exact same modes and means of governance it has been developing over the last decade. Estonians abroad, or perhaps even still in Estonia, could connect with their government in the same virtual manner to which they have become accustomed.”

(Rice, 2019)

Whilst this portrayal offers a fascinating insight into how a country may look to utilise a Data Embassy in the event of an emergency, to what extent is the Data Embassy’s overall utility overstated here? Indeed, despite the notion of state hibernation being an incredibly evocative imaginary for considering how a Data Embassy and ‘virtual state’ might function in practice in the future (see Section 7.1.2), questions do still remain with regards to the concept’s overall utility in the event of an emergency. This was a recurrent conversation that I had during a number of interviews, where the practicalities of the Data Embassy in the event of an occupation were called into question. As one interviewee reflected:

“This is my question, like, in my head this whole Data Embassy serves as what Ernst Jaakson did for 50 years. He kept records, he kept Estonia going. He went to the receptions, he kept Estonia on the picture. So if we have that data and something happens – you know, for the sake of an argument, the same thing as before and Estonia gets occupied and independence gets restored again - we get
that data and we start building up a country. So, essentially it is pretty much similar to what happened, and that is basically the continuity. So, maybe from a strictly legal point of view, it serves a purpose, but it would not serve the Estonian population when they are occupied or hit by an actual disaster. Would it do anything to actually benefit them? I'm not seeing that it would, at this point.”

(interview 19 - 21/11/18)

A similar point was made by another interviewee, who reflected on the legal implications of such a scenario and whether the state would continue to exist under such exceptional circumstances:

“And if we all started to prepare for the potential annexation or whatever by creating virtual embassies, again we have to eventually ask what’s the utility of those embassies, because the main question still becomes: is the country able to defend itself? Or, like, is the country able to survive as a country? And if the answer to that question is no, then it comes with at least part of the international community’s conclusion that that country does not legally exist anymore; and under the current international law, it comes with the conclusion that even if in our mind it exists, it has no real legal capacity or, at least to say, no practical capacity to act as a country.”

(interview 9 - 28/05/18)

What both of the quotes above reveal, is that while the Data Embassy concept is one that is highly innovative and potentially transformational, it may, in certain circumstances, also be incredibly impractical for a government in terms of serving its citizens from the cloud. Similar questions could also be raised should Estonia fall victim to a freak natural disaster or another crippling national cyberattack. Hypothetically speaking, if any of these events were to severely disrupt the connectivity of Estonia’s critical national infrastructure and Internet (in effect, knocking the country ‘offline’ and blocking it off from the outside world), then to what extent would the Data Embassy serve a purpose for the everyday Estonian? Of course, the country could still rely on data backups, but the purported ‘end-goal’ of a fully mirrored system of Estonia’s digital ecosystem that operates from the extraterritorial Data Embassy would be of little use in a number of contexts (see Section 4.2.3). For example, in the event of a mass-scale cyberattack (both larger and longer than 2007s attacks against various state institutions), the Data Embassy may well keep the state’s digital services running extraterritorially from the cloud, but of what use would they be to Estonian citizens on the ground, with little-to-no access to those services?
Indeed, one popularised story and narrative from the 2007 cyberattacks – suggesting that the ‘plug was pulled’ on Estonia’s Internet in order to disrupt and protect the country from the effects of the coordinated DDoS attacks (Grassegger and Krogerus, 2017) – would arguably do little to negate the damage caused to Estonia’s information systems, nor support the citizens of which they are designed to benefit and secure. If such an attack was prolonged and incredibly disruptive to Estonia’s entire digital ecosystem, then citizens would be unlikely to access important daily digital services such as banking, business portals or ordering healthcare prescriptions. As alluded to in previous chapters, the notion of ‘returning to paper’ or analogue forms of governance in such times are considered unviable in many circumstances.

Nevertheless, debates such as these are fascinating (and in need of further scrutiny) as we begin to consider the Data Embassy’s utility and function for states other than Estonia in the future. Speaking to Alex Jeffrey’s work on state improvisation and the production of political legitimacy (Jeffrey 2013; Jeffrey et al., 2015), issues such as these show that forms of improvisation may not always have a positive outcome. Instead, they remind us that the state can come into being through a series of acts and performances that require constant work and care – even in moments of hibernated suspension. To briefly conclude, although the Data Embassy and practice of hibernation could be characterised as a form of state improvisation, it is not yet clear as to what impact this could have on claims to political legitimacy (explored further in Section 7.1.2). Furthermore, analysing the Data Embassy’s utility across a number of different scenarios and contexts, I suggest that the Data Embassy may be inefficacious for the everyday functionality of the state (and thus everyday citizen) should it face a national crisis such as an occupation, cyberattack or natural disaster. Therefore, at present, it appears that the Data Embassy’s backup function serves its greatest utility for a state in the event of an emergency, allowing the state to recover and repurpose whilst in absenta of its normal everyday functionality.

7.1.2 Reimagining the state: emergencies, exile and ISIS

Whilst the business case for the Data Embassy has been signalled as logical and necessary for Estonia’s highly digitised society (see Section 5.1), the concept has also been positioned by many (including interviewees and senior politicians) as an ideal model and strategy for other states around the world. Facing a plethora of modern-day threats and uncertainties – from natural disasters such as earthquakes or floods, to acts of terrorism and military intervention – states may look to adopt the Data Embassy as a valuable deterrence and resilience mechanism, forming part of a much wider national security strategy. As Estonian President Kersti Kaljulaid has professed, “It’s a normal security measure that I think every country nowadays should take” (POLITICO, 2018 – see Chapter 5).

In just a few years, alternative imaginaries around the concept have already begun to form and will continue to flourish as the Data Embassy gains more analytical attention. During many conversations held over the course of completing this thesis (some more informal than others), the reimagined role of the Data Embassy in other contexts would lead to many fascinating use-cases. For example, in light of the devastating
2011 Tōhoku earthquake and subsequent Fukushima nuclear power plant disaster, how might the Japanese government benefit from backing up state data and information systems overseas? Amidst the recent Catalan independence movement (where former President Carles Puigdemont was forced into exile in 2017), one Catalan friend discussed with me the potential benefits of operating the proposed Catalan Republic from the cloud – if only for its political symbolism and potential serviceability - should it be forced into exile in the future.

Primarily, however, the Data Embassy still evokes geopolitical imaginaries around the mitigation of the Russian threat. In a recent report for the Council on Foreign Relations on reducing tensions between Russia and NATO, Kimberly Marten set out a number of key deterrence measures for the Trump administration, believing President Trump and Pentagon officials should push for the establishment of “NATO-country cyber embassies on foreign soil to enhance deterrence through denial” (2017: 31). By doing so, Marten believes that cyberattacks and land seizures in the Baltics and other states on NATO’s ‘eastern flank’ (e.g. Poland) would be “less profitable for Russia” (ibid).

Other discussions regarding future iterations of the Data Embassy have centred around legal validity. Following a conversation on the difficulties faced by the Kuwaitis and their missing archives (see Section 5.1), one interviewee pointed to the efficacy of the Data Embassy from a legal perspective in the event of independence being lost:

“So it’s the idea of keeping your backups outside of the country actually, in my mind, becomes really vital also in cases where you need to have a backup later on if you want to go to court to prove something. For example, the case which is in Crimea at this point of time, you have most likely heard about the problems there with the land registry and so on. So definitely the backups are done for this reason, for outside of the country, that if something changes, you can still have a backup.”

(interview 17 - 29/10/18)

Referring to the ongoing situation in Crimea, the Data Embassy is posited here as almost a legal guarantor during any potential threat to a state’s sovereignty, legitimacy and independence. It remains to be seen whether such data or information held by a state in a similar scenario could be used in an international

---

3 There is certainly a case to be made that the Data Embassy concept makes an attack on a state less profitable (see section 5.2.3), but Marten’s recommendations are unfortunately lacking in any further detailed analysis. Undoubtedly more research within a Baltic/NATO context is required as all three Baltic states (and Poland) have differing geopolitical circumstances, meaning that such a solution may not be advantageous for neighbouring states other than Estonia. For example, after a brief discussion with a government minister from one of the aforementioned states, it was made clear that the idea of replicating Estonia’s Data Embassy concept did not sound appealing to them.
court of law in defence of state sovereignty, but it is interesting to see how the Data Embassy is already being reimagined as a potential solution to future territorial disputes.

Taken to a more theoretical conclusion, I wish to point to the way in which such imaginaries around the Data Embassy allow us to think more critically (and creatively) about the evolving role of the state and the way in which it may operate in the future under different scenarios. With increasing concern over the current global climate crisis, states are having to think of novel ways to implement archival resilience and disaster recovery strategies in the event of a natural disaster (such as earthquakes, hurricanes, fires and floods). As the Japanese example at the start of section illustrated, we may begin to see the Data Embassy being posited as a solution to a catastrophic disaster by backing up vital components of state infrastructure abroad. Jason Thompson (2019) has taken this one step further by asking whether the Data Embassy could serve as a future solution for states facing existential sea level rises and climate catastrophes. Thompson’s reimagining of the concept, in the context of the fictitious island of ‘Bakati’ in the Pacific Ocean, games through a number of in-depth scenarios within which the island is forced into climate-exile and thus imagined as a non-territorial ‘e-state’. Thompson’s research offers us a useful tool for imagining how the state could operate in the event of an emergency, but equally how states may be able to survive (and even continue to ‘influence’ diplomatically) in the event of territory loss.

For journalists, like Nathan Heller from the New York Times, the Data Embassy can also evoke such dramatic geopolitical imaginaries around the logics of occupation and exile, that the utility of the concept reads like a pitch for a Hollywood movie:

“In the event of a sudden invasion, Estonia’s elected leaders might scatter as necessary. Then, from cars leaving the capital, from hotel rooms, from seat 3A at thirty thousand feet, they will open their laptops, log into Luxembourg, and—with digital signatures to execute orders and a suite of tamper-resistant services linking global citizens to their government—continue running their country, with no interruption, from the cloud.”

(Heller, 2017)

Continuing this theme, the idea of being able to ‘backup’ or ‘hibernate’ the state and operate your country from the cloud will continue to elicit interest with its potential usage in an array of differing scenarios – from small states facing similar anxieties to Estonia, to state/non-state actors with limited recognition or political legitimacy. As Ben Hammersley ideates:
“Countries in waiting – Palestine, for example – could start to configure their own systems, building a whole state on a server, and run it all from the mobile browser. Insurgent states-within-states, like Hezbollah in Lebanon, could compete with the mainstream governments with better infrastructure, faster updates and more responsive bug fixing. Cities could institute entirely digital infrastructure and market themselves as providing a more convenient front end to their slower mother nation.”

(Hammersley, 2015)

Speaking to a growing body of work in political geography that explores alternative sites of political legitimacy and anomalous geopolitical spaces (see, Jeffrey et al., 2015; McConnell, 2016), I believe there is scope for further research in this area that considers the Data Embassy’s utility for state and non-state actors in the wider international political system. For instance, for states that are unrecognised, disputed, exiled or de facto in status – such as Tibet, Palestine or Somaliland – the premise of extraterritorial data storage may be particularly alluring. In some cases, the actual improvisatory performance of opening a Data Embassy in another part of the world could well contribute to efforts at constituting recognition, sovereignty and political legitimacy within the wider international state system (see Section 7.2.1).

The Data Embassy has also been reimagined for use in more nefarious ways. In particular, how may insurgent groups or terrorist organisations such as ISIS or Boko Haram utilise similar technologies in order to operate their caliphate from the cloud? Writing for WIRED, Carl Miller suggests that this could already be happening, with the recent discovery of a vast cache of documents online appearing to belong to ISIS, in what seems to be a deliberate attempt to “store, protect, and treasure the collective memory of a state that [doesn’t] exist anymore” (see, also, Ayad, 2020). Since 2017, ISIS has gradually been swept from its territorial strongholds in Mosul, Raqqa and Baghouz, and, in the process of having its territorial extent severely curtailed, it appears that the former unrecognised quasi-state has taken steps to begin ‘backing up’ its most vital documents and archives using the open-source software, Nextcloud (a cloud-based service that allows users to backup data and synchronise files in a way that avoids centralised hosting and control). Whilst being nowhere near as sophisticated as Estonia’s digital Data Embassy, it is important to note that it is still providing a critical function for the caliphate by continuing to offer its ‘services’ to its ‘citizens’ in the form of propaganda, networking tools and tutorial videos⁴ (Ayad, 2020; Miller, 2020). Despite the cache being nothing more than a storage drive at present (similar to a file saved on Dropbox), it remains a crucial

---

⁴ It has been widely recognised that at the height of its power, ISIS had advanced cyber capabilities and took advantage of digital technologies and social media to spread propaganda, recruit sympathisers and evade spying intelligence agencies (see, Atwan, 2016; Ayad, 2020). I would argue, however, that the likelihood of a future ISIS-style Data Embassy is negligible, given that it would likely have to seek support from a state that is both sympathetic to its cause and able to support it at a technological level. Therefore, it would be unlikely to establish something as robust, sophisticated and effective as the Estonian Data Embassy initiative.
digital repository and tool that aims to keep ISIS alive, blending “the unique horrors and brutalities of that
collapsed regime with the dry, folder-based nature of an archive” (Miller, 2020).

Despite the many different use-cases and Data Embassy imaginaries addressed in this section, questions
remain regarding the effectiveness of such practices within a conventional state system. As I hinted at in
Section 7.1.1 with regards to the Estonian Data Embassy in Luxembourg, whilst the notion of operating
components of a state or disputed territory from the cloud may be technically feasible, the very idea and
utility of an entire virtual state seems unlikely given the criteria for statehood in a current Westphalian
system. As stated by the declarative theory of statehood under the Montevideo Convention (1933), a state
is defined as a person in international law if it meets the following criteria:

1) A defined territory
2) A permanent population
3) A government, and
4) A capacity to enter into relations with other states

Clearly, a Data Embassy or any form of virtualised state fails to meet these criteria at present. Although it
may be possible that some states could recognise Estonia as a fully functioning sovereign state operating
from the cloud in the event of an emergency (which would fall under the constitutive theory of statehood),
it remains to be seen that the extraterritorial Data Embassy would be deemed a legitimate political entity
under international law. As Jeffrey et al. note, from an international law perspective, “legitimacy is thus
approached through a lens of institutional recognition: that is whether or not a polity is recognised by other
sovereign states as having met the international criteria for legitimate statehood” (2015: 179). Thus, just as
Carl Miller (2020) argues that a storage drive is unlikely to constitute statehood for ISIS, it is clear that the
Data Embassy would be unlikely to do the same in the event of Estonia being hit by a large-scale cyberattack
or forced into exile. Nevertheless, Estonia’s plan to build a Data Embassy and the idea of the state not
being tied to its geography will continue to draw interest and, as Lorraine Kaljund notes, to be “explicitly
celebrated and marketed as a disruption of this Westphalian paradigm” (2018: 6).

7.2 The Data Embassy and the future of diplomacy
The Data Embassy has emerged at a time where the boundaries of diplomacy and diplomatic practice are
continually shifting around the world. In particular, the utilisation of digital technologies in diplomacy has
become an increasingly widespread and global phenomenon (Manor, 2018a). From the embassy’s
newfound role as a social media outpost, communicating an array of news, views and consular services - often referred to as ‘Twiplomacy’, and sometimes to the detriment of diplomatic relations - to the emergence of the world’s first ‘digital ambassador’ in Denmark to serve as a fulcrum between state and Silicon Valley (Klymge et al., 2020), diplomacy has had to adapt quickly in order to compete with its new digital terrain (Fletcher, 2016). As a result, diplomacy is increasingly being recognised as no longer flowing solely from diplomat to diplomat, state to state, but as a practice that is increasingly conducted from the phone or tweet-deck (Robinson and Miltner, 2018) and by alternative actors that operate at the margins of the international political system (McConnell et al., 2012).

In this section, I examine what impact the Data Embassy could have on the practice of diplomacy in the future. First, I consider to what extent the Data Embassy may impact on inter-state relations with the advent of more Data Embassies, exploring how Estonia and Luxembourg may already be utilising/leveraging the Data Embassy for their own strategic benefit (Section 7.2.1). Second, I turn to the embassy itself and examine whether its definition should be extended following the advent of both virtual embassies and the Data Embassy (Section 7.2.2). Finally, building on previous research that explored the Data Embassy’s applicability to the Vienna Convention (Robinson et al., 2019), I consider whether the Data Embassy has set an influential legal precedent regarding extraterritorial data storage, and question whether the Vienna Convention is in need of updating to reflect changes in the practice of diplomacy in the twenty-first century (Section 7.2.3).

### 7.2.1 Data Embassy diplomacy

On 20 June 2017, the world’s first Data Embassy was established after the Republic of Estonia and Grand Duchy of Luxembourg signed a bilateral agreement regarding the hosting of Estonian data and information systems within a government-operated data centre in Luxembourg. The historic agreement, which was signed by Prime Ministers Jüri Ratas and Xavier Bettel (see Fig. 7.3), serves as a reinterpretation of the Vienna Convention that, in effect, binds both countries to fulfil specific obligations and similar diplomatic protections and immunities to that of a traditional embassy (Robinson et al., 2019). Notably, it was the first time two states had ever agreed to provide these kinds of protections and immunities outside of a diplomatic mission.
Beyond the highly ritualised and rehearsed performances that took place that day (the signing, the hand-shake, the photo op and the formal celebrations later that evening – see Section 4.2.3), I have also been incredibly interested in what this particular moment symbolised in diplomatic terms. For Estonia and Luxembourg, it signified a new kind of diplomatic relationship between the two countries, one that is grounded through the extraterritorial hosting and storage of state data. If more countries decide to follow Estonia and Luxembourg’s lead moving forward, then I believe this also raises key questions with regards to how diplomacy may be exercised and performed in the future. For instance, will other states form new kinds of diplomatic relationships through the creation of Data Embassies? If so, how will states begin to respect the integrity of other states’ data in the cloud? Furthermore, will states such as Luxembourg leverage their existing superior data centre infrastructure as a means of repositioning itself on the world stage as a powerful twenty-first century data haven or refuge? Whilst questions such as these have been relatively unexplored until now, I believe they warrant attention in this thesis as I contend that the Data Embassy formalises a new kind of ‘alternative’ diplomacy that takes place within the ‘unusual’ space of the extraterritorial data centre (see McConnell et al., 2012). To help unpack these questions a little further, in this section I focus on three specific areas that emphasise the Data Embassy’s relevance to the future practice of diplomacy.

First, drawing on the Luxembourg case study explored in this thesis, I argue that the Data Embassy may be utilised as an effective tool by states to improve or foster better diplomatic relations on the international stage. For small states that may have limited budgets, resources and influence in the diplomatic field, establishing a Data Embassy partnership could be seen as a fairly direct and inexpensive option for enhancing diplomatic relations with another country. For states that are unrecognised, disputed, exiled or de facto in status, the performative process of opening a Data Embassy and establishing diplomatic relations via the extraterritorial data centre could also have tangible benefits with regards to constituting
greater recognition, sovereignty and political legitimacy within the wider international system (see Section 7.1.2).

In the case of Estonia and Luxembourg, I believe the decision to establish a Data Embassy played both a symbolic and practical role in enhancing relations between the two states. At the time, Xavier Bettel hailed the agreement for being built upon a degree of “trust” and “friendship” (Digital Luxembourg, 2017); whilst I have also argued that the decision combined a digitally informed leadership and shared economic and security values between the two countries (see Section 4.2.3). Since that point, I have observed a marked difference in the way that Estonian and Luxembourgian politicians communicate and perform this relationship to the wider public – whether this is through the Estonian President Kersti Kaljulaid offering a glowing review of Luxembourg’s compatibility during a podcast interview at Davos (POLITICO, 2018) or through the promotion of their burgeoning bilateral relations via Xavier Bettel’s twitter account (see Fig. 7.4). This is not to say that both countries have established diplomatic relations from scratch however (indeed, both are active members of NATO and the EU and have long-standing relations with one another), but it is clear that the decision to establish a Data Embassy in Luxembourg has played a significant role in improving diplomatic relations between the two countries.

Figure 7.4 – Luxembourg Prime Minister Xavier Bettel tweeting following a visit from Estonian President Kersti Kaljulaid – a sign of greater diplomatic cooperation between the two countries? (source: www.twitter.com)

---

5 Interestingly, one interviewee revealed that pre-existing relations between both countries were, in fact, a major stimulus in getting negotiations regarding the Data Embassy off the ground: “So it was a bit easier since it was between Estonia and Luxembourg, Luxembourg also being a small country, and their Prime Minister being a friend of Estonia, being able to nudge things on his behalf” (interview 12 - 01/06/18).
Building on from the first, my second point considers whether Estonia (or other states in the future) may look to locate Data Embassies strategically as a means of enhancing their diplomatic standing around the world. As mentioned above, for smaller states, such an approach may be beneficial in terms of boosting a country’s fairly limited diplomatic reach, and for new partnerships to be forged via the cloud and extraterritorial data storage. The question of whether a Data Embassy may be located advantageously was one that was discussed with a number of respondents as we ruminated on where Estonia may look to situate a Data Embassy next. As highlighted in Chapter 3, I would often turn to my Data Embassy network map (see Fig. 3.3) as a prompt and discussion point on potential locations, which elicited a number of interesting responses and geopolitical imaginaries over a hypothetical global network of Data Embassies in the future. Whilst a number of respondents working close to the project remained coy on where they believed any future Data Embassies may be located, I found that other respondents (i.e. Data Embassy ‘outsiders’) were more open and interested in speculating on how Estonia may wish to plot its next move – some joked how Russia and China were perhaps not the best suitors (interview 1 - 09/08/17), whilst others pointed to how agreements with Japan, South Korea or those within the Five Eyes intelligence alliance (Australia, Canada, New Zealand, UK and U.S.) could benefit Estonia both diplomatically and in terms of bolstering national security (interview 20 - 27/11/18; interview 14 - 12/10/18).

One common denominator throughout these discussions was the belief that the next Data Embassy should be located outside of the EU. Not only would this be a fundamental step in testing the geographical distribution and technological redundancy of any potential future Data Embassy network, but it would also help assess how other non-EU (and maybe even non-NATO) states would align with Estonia in terms of the legal obligations and diplomatic protections that are required to be exercised within their territory (see Section 7.2.3). Canada was one country that was frequently discussed as a potential future location. Not only do both countries have strong connections in areas of digital governance⁶, but Canada also has a strong Estonian diaspora as a result of many families fleeing to North America during the Soviet occupations⁷. Thus, in the same way that Canada became a sanctuary for many thousands of Estonians fleeing the persecutions of Soviet rule during the twentieth century, might the Data Embassy symbolise a twenty-first century equivalent for its data and information systems?

---

⁶ Back in May 2018, Estonian Prime Minister Jüri Ratas visited Canada as part of his country’s centenary celebrations, meeting with his Canadian counterpart Justin Trudeau in Ottawa. As well as reaffirming shared commitments on issues of security and stability in Central and Eastern Europe, both leaders signed an MoU that committed deeper cooperation on areas of digital government and the digital economy, allowing both countries to collaborate on joint projects and share best practice around digital governance (Prime Minister of Canada, 2018). It is likely that this digital cooperation started a few years prior, when Canada’s Deputy Minister Alex Benay visited Tallinn on a government-led emissary to learn about Estonia’s digital government. Benay is reported to have returned back to Canada with one message, “I want what they have, let’s make it happen” (Tuulas, 2020).

⁷ Prior to Soviet occupation in 1944, approximately 72,000 Estonian political refugees fled to Sweden and Germany. Of this number, nearly 14,000 Estonians immigrated to Canada between 1946 and 1955, with many travelling on so-called ‘Viking’ boats (such as the SS Walnut) from Sweden, posing a significant challenge for Canada’s post-war immigration policy (Aun, 1985; The Canadian Encyclopedia, 2008). According to latest census figures, there are more than 24,000 Estonian-Canadians in Canada today (Statistics Canada, 2017), with Toronto being the city with the largest population of Estonians outside of Estonia.
Furthermore, I was also struck by the fact that the Estonian government has stipulated that any future Data Embassies would be located in countries that are ‘friendly’ to Estonia (Kotka and Liv, 2015; MoEAC, 2015). Whilst this was not terribly surprising – would it, for example, be beneficial for the Estonian government to locate a Data Embassy in a potentially hostile country? – it did lead me to reflect on what basis would Estonia characterise a state as ‘friendly’, and to what extent this status was fixed and regularly evaluated. As one Data Embassy insider revealed to me: “Yeah, it’s friendly, but friendly means that they share the same values and belong to the same international community” (interview 6 - 18/05/18). But what if those values of a once friendly partner were to change? Or if they were suddenly compromised (politically or financially) by an adversary? As such, the same interviewee went on to detail how there were other important components to consider, including whether or not the data centre was government-operated or not:

“[I]t should have its own government-owned security certified data centres - and that was a bit of a problem with Britain as well, that their data centres are owned by the private sector. And that would be a threat, because those can be sold, they can be sold to those unfriendly countries, those can be sold to whoever. This is why the second very important part [is] that [we use] government-owned data centres – or partly government-owned – and the 3rd parties have to share the same values and to give the same diplomatic immunities and privileges, and be willing to sign the declaration/bilateral agreement not only that we want the Data Embassy, but going into the essence and really giving the protection to…not to an embassy room but to a data centre or dedicated data centre space.”

(interview 6 - 18/05/18)

I found this quote to be incredibly revealing, for it not only refers, albeit indirectly, to the threat that many Estonians believe is posed by Russian foreign investment⁸, but also picks up on how these are manifest in an everyday security discourse and many of the ontological insecurities Estonia face today (highlighted in Chapters 5 and 6). In essence, I believe this also points to some of the state-level anxieties that are currently experienced and exhibited by those in the Estonian elite, and how this potentially impacts upon who they wish to enter close diplomatic relations with, who they wish to conduct business with, and also effect where future Data Embassies may be located.

My final point speaks to an interesting development that has taken place during the course of completing this thesis, recognising the wider utility of the Data Embassy outside of an Estonian context.

⁸ From this quote, I believe the suggestion is that Russia may wish to strategically invest in foreign data centre infrastructure in the future, and thus potentially compromise the technological security of Estonian data held outside of its borders. Such a claim is by no means unique to Estonian political discourse, and also speaks to wider anxieties, particularly in the West, around Russian and Chinese financial investment in infrastructure, real-estate and commerce (see, Moran, 2012; Weiner, 2006).
(see Section 7.1.2). As I acknowledged in Chapter 4, due to the country’s excellent telecommunications infrastructure and high concentration of Tier IV data centres, Luxembourg has started to position itself as a ‘hub’ for other states to begin hosting and storing their data within its borders. This development was disclosed to me during my first interview back in 2017:

“There know already that Luxembourg has made a contract with us, and they have actually also mentioned some other parties who are interested in Luxembourg’s services…so basically, whilst Luxembourg is doing the project with us, they would like to have a reference, and afterwards become a ‘data embassy service provider’. For them, it’s very good. They have good location in the middle of Europe, and they have very good data centre facilities there.”

(interview 1 - 09/08/17)

I am interested in this development as it suggests that Luxembourg may stand to benefit diplomatically from the Data Embassy concept. For instance, the country may wish to leverage its favourable geography and existing data centre infrastructure in order to foster new diplomatic relations through the extraterritorial hosting and storage of state data. In doing so, I believe Luxembourg may also be able to powerfully reposition itself on the world stage, serving as a twenty-first century data ‘haven’ or ‘refuge’ for other states around the world that may be facing similar anxieties to Estonia9. The recent announcement that Monaco will be looking to open a similar Data Embassy in Luxembourg offers credence to this view (see Section 4.2), despite it perhaps not fitting the profile of a state that is particularly vulnerable nor digitally dependent.

One interviewee told me how Luxembourg’s other characteristics also meant that it would make an exemplar Data Embassy ‘hub’ in the future:

“Luxembourg is very business-minded as a government. Their banking system, they want to sell. I don’t know, their government has like satellite factories, so it really shows that they want to position themselves in the world as having some kind of business cases and offering the services to others. And of course, Data Embassies are one of a kind. Data Embassies are definitely for them a business case, and definitely, like Estonia being the first client is quite a good selling argument as well [laughs].”

9 As cultural anthropologist Alix Johnson points out, Iceland has previously been posited as a data or ‘information haven’ as it is considered “an attractive place to store the data of the world” (Fish, 2014). This is due, in part, to Iceland’s information-friendly legislation that favours free speech and data privacy – in 2014, Icelandic politician Birgitta Jónsdóttir remarked: “Iceland should become for information what Switzerland is for money” (Gaedtke, 2014) – but also, like Luxembourg, Iceland possesses superior data centre infrastructure (as well as ideal geology/climate) that makes it an ideal location to store data.
The notion that Estonia would be a good selling point was repeated by another respondent, who posited: “And if you have Estonia, who is poster boy for cyber and IT or e-government services…let’s put it this way, hosting its data in your government, it is also a mark of quality” (interview 11 - 01/06/18). Bringing both of these points together, I believe they raise some interesting qualities regarding the Data Embassy and its function as a diplomatic tool for small states such as Estonia and Luxembourg. First, it recognises that a Data Embassy could offer an effective soft power function, enabling host states to provide an alternative business case and national security function, that in turn bolsters its reputation and standing in world (as Luxembourg has already achieved in the world of financial services, for example). Second, and building on the first, the Data Embassy has something of a symbiotic quality for states wishing to enter into diplomatic cooperation with one another – in this example, Estonia is able to boost its image as a digital pioneer, whilst Luxembourg has enabled itself to be positioned as a Data Embassy ‘hub’ for other states – which suggests that both ‘host’ and ‘sending’ state may stand to benefit diplomatically from the establishment of diplomatic relations via an extraterritorial Data Embassy. So far, this section has outlined the ways in which a new form of Data Embassy diplomacy may be emerging. In the following sub-sections, I explore how this has also manifest in debates surrounding the future of the embassy and international diplomatic treaties such as the Vienna Convention.

7.2.2 Digital Embassies

On 4 December 2007, the Estonian government took the unusual step of opening a ‘virtual embassy’ in the popular online world Second Life (see Fig. 7.5). Situated in the Diplomatic Quarter of Diplomacy Island, the embassy joined the Maldives and Swedish virtual representations that were officially inaugurated a few months earlier. For governments experimenting with new forms of digital diplomacy, Diplomacy Island promised new possibilities for diplomatic representation and interaction, with visitors able to explore these new virtual spaces and talk to virtual diplomats about visas, trade and other consular-related matters. For governments with fairly limited budgets and human resources, virtual embassies would also assist small and developing countries that have “limited diplomatic outreach” in the ‘real’ world (Diplo, 2007).

---

10 *Second Life* is a free, virtual, online world where users (known as ‘residents’) can create their own avatars and interact with other users from across the globe. *Second Life* users are able to connect with one another, participate in various activities, and are able to build, shop and trade virtual property using the platforms own currency, Linden Dollar, which is exchangeable with real world currency (Pathak, 2017). Launched in 2003, the platform steadily grew in popularity, with around one million monthly users by 2013 (Linden Lab, 2013), although this has since decreased.

11 Despite Sweden initially announcing the concept, the Republic of Maldives controversially jumped ahead and opened its virtual embassy a few days before on 22 May 2007. Swedish Foreign Minister Carl Bildt attended the opening of the Swedish embassy, albeit in the form of an avatar. ‘Diplomacy Island’ soon grew in size as Estonia, Serbia, Macedonia, Albania, Colombia and the Philippines all opened their own virtual embassies in the virtual world.
According to the Ministry of Foreign Affairs (MoFA, 2007), the Estonian virtual embassy had three basic functions. First, the virtual embassy would allow the government to explore and take advantage of new and complex online worlds, using them for disseminating information to a wider public/audience. The second was to organise “high-level meetings, lectures and seminars” (ibid) for diplomatic experts and players to experience virtually. The third was to introduce the players of Second Life to Estonian culture and the latest developments and innovations in e-government. Stepping into the ‘technology room’ of the embassy, players were introduced to e-Estonia with three digital sculptures representing Estonia’s pioneering use of internet-voting, the future of communication and the threat of cyberwar\textsuperscript{12}. Stina Bengtsson (2012) has argued how the virtual embassy in Second Life played a crucial role in the production and expansion of Estonian national space, whilst also assisting in the country’s wider nation branding practices (see Section 5.3).

Unfortunately, despite initial fanfare and promise, virtual embassies in Second Life were not as successful as first envisaged, with the vast majority closing and becoming ‘digital ruins’ (Miller and Garcia, 2019) within a matter of years\textsuperscript{13}. Nonetheless, their emergence not only speaks to recent innovations in the practice of public diplomacy (see Section 2.3), but also points to a shift in how the embassy is conceptualised and imagined in a digital age. In this thesis, I argue that the Data Embassy should be considered another such example, and consider whether its emergence may allow us to reconceptualise the embassy beyond its

\textsuperscript{12} Today, Estonia has its own physical manifestation of the ‘technology room’ in the form of the e-Estonia showroom (or ‘Briefing Centre’) based in Ulemiste City, Tallinn (see Section 3.3.3).

\textsuperscript{13} Sweden’s virtual embassy closed in 2013, whilst a similar fate befell the Estonian virtual embassy sometime after this. Although there is no publicly available information as to why this happened, Ilan Manor (2018b) has reflected on how digital diplomacy initiatives such as these are incredibly resource intensive, and it is likely that the large financial running costs, and disappointing lack of visitors (Bengtsson, 2012) were a factor in the Estonian virtual embassy’s demise.
traditional confines. Throughout the process of conducting this research, the question of whether the Data Embassy constituted a new form of embassy or not would continue to cause debate with academic peers and interviewees. Indeed, during initial plans to utilise existing space within embassy buildings for data backups (see section 4.2), the Data Embassy could well be envisioned as the traditional embassy’s digital equivalent - merely affording the data and information systems stored on its server racks inside the embassy the same diplomatic protections. However, once it became apparent that this method would not be possible – and the Estonian government opted to utilise existing data centre space outside the confines of a traditional embassy – the notion that a Data Embassy could be considered an ‘embassy’ at all was called into question.

Initially, there was a degree of scepticism over terminology usage, with the Data Embassy being criticised for being unclear and potentially misleading. For some critics, the name was nothing more than a marketing ploy to help raise the international profile of both the project and Estonia itself14 (a criticism that was also levelled at the e-Residency programme, for it was initially understood by some as a future avenue for actual permanent residency or citizenship). Given that the term is something of a misnomer, one interviewee highlighted early concerns around how the Data Embassy could be misinterpreted more widely:

“The main reason why we haven’t wanted to use the word embassy is simply because people would too broadly make the connection with the Vienna Convention meaning of the word embassy. If the world in general could understand that there could be several types of embassies – which perhaps don’t have the same rights – then it would be fine to use that word.”

NR: So do you think it could be conflated – potentially misused in that sense?

“Perhaps not. Not like meaningfully in a bad sense. But simply because people don’t know the difference and it can lead to misconceptions, definitely.”

(interview 18 - 07/11/18)

Consequently, during the early stages of the project there was a great deal of uncertainty and pushback regarding the conceptualisation of the Data Embassy in a legal context, with a number of experts highlighting concerns over legal semantics and interpretation: “Because if you speak to lawyers they all say ‘oh, no no no…this is not an embassy. We don’t want to hear about data embassies’” (interview 1 - 09/08/17). One interviewee revealed that this may have also played a factor in talks stalling with the UK over its proposed Data Embassy (see Section 4.2), as the British FCO “didn’t buy or didn’t

14 This was an impression I encountered during a number of personal ‘off-the-record’ encounters researching the Data Embassy.
share the understanding of the international legal framework…and for them it was ‘we have our Vienna Convention’, ‘we have our traditional embassies’, ‘you can’t say something digital with [server] racks is an embassy’, an embassy is something very traditional in international law” (interview 6 - 18/05/18). As a result, the term ‘embassy’ was not used in the bilateral agreement that was signed between the Republic of Estonia and Grand Duchy of Luxembourg and was instead termed as “an agreement […] on the hosting of data and information systems” (Riigi Teataja, 2017).

Moreover, some respondents were keen to point out that the Data Embassy goes against the overall purpose of the Vienna Convention, and could thus not be considered an embassy under international law: “It is only established as an embassy within the framework between Estonia and Luxembourg” (interview 19 - 21/11/18). One government legal expert expanded on this further:

“It is not a traditional diplomatic mission. First of all, it doesn’t have any personnel. Perhaps there is a policeman. I’m not sure, that would be a technical question. But I’m pretty sure that there isn’t any state officials there, beside the policeman. But if you are looking at the Vienna Convention, then I mean an embassy – a diplomatic representation – is mainly about people. The physical room is mentioned as premises [in the bilateral agreement]. So right now, we couldn’t have a diplomatic representation without actual people. I’m just guessing, but it should be something like that. So, this is the main reason it could not be a diplomatic mission.” (interview 18 - 07/11/18)

With the notion of a Data Embassy becoming something of a misnomer, then, does this mean that its wider use (as well as its use in the context of this research) is somehow problematic? Perhaps, as one interviewee admitted, the term “data storehouse” (interview 1 - 09/08/17) or ‘warehouse’ would be more felicitous? In this section, I contest that the term is problematic for the following reasons. First, there is no escaping the fact that the Data Embassy has worked incredibly well as a marketing tool for the state (see Section 5.3). Thus, after it was decided that existing embassy locations would no longer be used, I would argue that it made little sense for the Estonian government to change the name of the project as it was gaining in prominence in both media and political discourse. Second, and perhaps more importantly, the aforementioned bilateral agreement that was signed between Estonia and Luxembourg has actually set a

---

15 The interviewee went on to argue that the Vienna Convention also stipulates that you cannot have two premises for one diplomatic mission, meaning that Estonia could not locate Data Embassies in countries that already host one embassy: “You can have one embassy within one country – you can have consulates and all that, but consulates do not have the same kind of inviolability that embassies have, so they cannot be as secure, definitely. And if we had an embassy, it would be an additional thing, so it wouldn’t be as secure.” (interview 18 - 07/11/18). Interestingly, there is no permanent diplomatic mission in Luxembourg, only a consulate.
legal precedent regarding the inviolability of data and information systems, meaning that embassy-like provisions have been afforded outside the context of a traditional diplomatic mission. As I highlighted in Section 7.2.1, this is the first time two states have agreed to provide this kind of inviolability – with Luxembourg providing similar diplomatic privileges and immunities to that of a traditional embassy, while Estonia is extending its ability to exercise its powers of jurisdiction within a small, demarcated server room inside a Tier IV data centre outside of its own borders.

Whilst it is clear that this small space within the data centre is not recognised as an embassy under international law, I believe that the exceptional embassy-like provisions that have been afforded in this context raise important and yet-to-be explored questions regarding the conceptualisation of an embassy in a digital age. To that end, I wish to consider how the Data Embassy may allow us to extend the definition of an embassy outside of the traditional confines of a physical diplomatic mission. Drawing on the growing interest and utilisation of ‘virtual embassies’, and the potential utility of Data Embassies moving forward, in this thesis I conceptualise the notion of a digital embassy. A digital embassy can first be understood as a virtual representation of a traditional diplomatic mission. As the example of the Estonian virtual embassy on Second Life and others online diplomatic representations around the world have shown (see Section 2.3), not only do they function as an extension of national space (Bengtsson, 2012), but they also provide crucial diplomatic/consular services to citizens and foreign publics abroad. Second, as the Data Embassy shows, a digital embassy may also be conceptualised as a crucial state mechanism for hosting and securing critical state data databases and information systems outside of its own borders. Bringing both of these forms together, I argue that by engaging with the notion of the digital embassy, scholars and practitioners will better understand and conceptualise novel forms of diplomatic practice in a digital era, whilst also being able to attend to the various alternative diplomatic sites and spaces (such as the MFA website or data centre) that adopt similar functions and characteristics to that of a traditional diplomatic mission.

There were some respondents who agreed with the general sentiment that an embassy could be conceptualised in a digital form: “It wouldn’t be the first institution in international law that would change in time” (interview 18 - 07/11/18). However, some remained a little more cautious, admitting that “I am not so sure if we should redefine embassies, because it is like redefining home or something like that. But I think that we should redefine services in a diplomatic context” (interview 11 - 01/06/18) – referring to the role the private sector may play in providing some diplomatic services in the future. When I asked former British Diplomat Tom Fletcher a similar question during a seminar in London in 2017, he expressed how in a digital age we should maybe think of an embassy as more of ‘an idea, not just the building’.

In the context of this research, I argue that the idea of the Data Embassy being an embassy and not simply a data ‘storehouse’ or ‘warehouse’ really matters. As David Malone (2012) has argued, the embassy is a
symbol of sovereignty. “Indeed, it is true that many embassies in important capitals seem to serve a sole function, to signal that their state exists, by flying the flag and sometimes by doing little else” (Malone, 2012: 236). Therefore, in this thesis, I argue that the extraterritorial Data Embassy does a similar job for the Estonian state, by giving it ontological status and legitimacy within the space of a data centre. A means of mitigating many of its everyday anxieties and insecurities (see Chapter 6), the Data Embassy is thus a mechanism manufactured by the Estonian government to constitute a form of recognition, sovereignty and legitimacy – it allows it to feel like a state (Mercer, 2014).

7.2.3 Vienna Convention 2.0?
The Vienna Convention on Diplomatic Relations (VCDR, 1961) is widely regarded as the cornerstone of modern diplomacy (Denza, 2009). Since its conception in 1961, it has achieved near-universal participation and compliance by states, bringing clarity and uniformity to modern diplomatic practice. Its counterpart, the Vienna Convention on Consular Relations (VCCR, 1963), soon followed, codifying certain rights and obligations with regards to the conduct of consular relations. Although both have fallen victim to violations and controversy over the years (see, Epps, 2011; Simpson, 2020), their high degree of observance and influence upon international relations, diplomacy and law cannot be undervalued. Yet, as I have argued in this thesis, recent technological advances have led to significant shifts in the practice of modern diplomacy - from the increasing utilisation of digital technologies and social media by states, MFAs and politicians to communicate with foreign publics, to the use of ‘virtual embassies’ as digital representations of diplomatic missions in cyberspace (see Section 2.3). The arrival of the Data Embassy, I have argued in this section, signifies yet another shift, with embassy-like protections being afforded to Estonian data and information systems within a Luxembourgian data centre.

However, as previous research on this topic has identified, the Vienna Convention is not deemed presently suitable for the protection and inviolability of data and information systems outside of the traditional diplomatic mission (Robinson et al., 2019). Thus, in the case of the Estonian Data Embassy in Luxembourg, a bilateral agreement was introduced, serving as a reinterpretation of the VCDR and providing an extra-legal layer that ensures both states fulfil specific obligations and provide similar diplomatic protections to that of a traditional embassy. As a blog for Microsoft recently commented, by doing so the Estonian government may be setting an influential precedent regarding extraterritorial data storage in a world where “international legal frameworks predate the digital age” (Microsoft, 2017). With the potential advent of more Data Embassies in the future (see Section 7.2.1), I conclude this section by considering: to what extent is the Vienna Convention fit for purpose in the twenty-first century?

In order to get closer to answering this question, it is first worth considering how the Vienna Convention has been embroiled in previous scholarly debates regarding the scope and efficacy of the VCDR and other
diplomatic protocols (see, Aceves, 1998; Epps, 2011; Ross, 2011; Sieh, 1990; Subramanian, 2017). As former Indian diplomat Kishan Rana observes:

“A few scholars and practitioners hold VCDR to be outdated, and would like to see its provisions concerning immunity to be modified; some wish to bring activities directed at non-state actors, including public diplomacy, under some regulation. But there is little appetite among states for starting a revision process, and even less prospect for crafting new consensus over a revised framework.”

(Rana, 2016: 150)

Nevertheless, it is also the case that there has so far been little conversation and debate around the role and efficacy of the Vienna Conventions in light of recent technological advancements (for an exception, see Parkhill, 1998), of which this research aims to open up in the context of the Data Embassy.

Noted above, the Vienna Convention is an international legal framework and treaty that predates today’s digital age. Codified and adopted in the 1960s, Rana (2016: 150) notes how the VCDR is very much a “child” of the Cold War and is rooted in the “ethos” of that period. As such, there may be substance to the claim that the convention and framework is fundamentally outdated in today’s digital world. How, for example, does the Vienna Convention keep up with advances in telecommunications and state surveillance capabilities? Eileen Denza (2016) has argued that the archives and documents of a diplomatic mission are inviolable in whatever form they are and wherever they may be (and it is thus interpreted to include modern forms of information storage – such as external storage devices). But in an age of increasingly complex communication networks and data flows, do the same principles and interpretation of diplomatic law apply? Does, for example, the VCDR cover the protection of diplomatic communications in digital form if it were intercepted in transit by an adversary? Although it is unclear whether the VCDR can be interpreted in this way, it was made clear during the Estonian government and Microsoft’s early legal analysis in 2015 that this was a desired outcome:

“In time, we hope that the corpus of law will extend protections afforded to a physical embassy to the virtual world, recognizing virtual data embassies, as well as to all other government assets as they move from a physical world to the online environment.”

16 Typically, discussions have centred around limiting the scope of diplomatic immunity, and draw on a number of cases where immunity has been sought by diplomats (or their families or staff members) after committing a crime. Mitchell Ross notes examples whereby prosecution has been escaped for crimes ranging from “driving under the influence, to shoplifting, assault, drug trafficking, kidnapping, rape, the imposition of slavery, and even murder” (2011: 174-175).
Moving forward just a few years, following the establishment of the Estonian Data Embassy in Luxembourg, where does this leave us with regards extending diplomatic immunities and protections to the virtual world? In ongoing research with colleagues from Tallinn University of Technology (TTÜ) and the University of Tartu, we suggest that in the specific context of the Data Embassy in Luxembourg “there is significant progress to suggest that the Vienna Convention could be extended in its current form to incorporate the protection of data and information systems outside the traditional diplomatic mission” (Robinson et al., 2019: 395). Thus, as other states begin to follow Estonia and Luxembourg’s lead, we argue that there is potentially enough scope and legal precedent that the “re-assessment of international law and the Vienna Convention may prove a beneficial solution” (ibid) in the future.

Some respondents I spoke to were sceptical of this proposal, however, citing that the VCDR was so entrenched in diplomatic tradition and modern international law that it would be extremely difficult to ‘rewrite’ or even slightly adapt (as expressed in the Rana quote above):

“Again, this is my personal view, but I am really hoping that the Vienna Convention will be left untouched […] I think the underlying – what I’m viewing this as – is that Estonia has, for the lack of a better word, been using the word embassy…I don’t really think that the Vienna Convention applies to it at all. I’m glad that they did it, under the meaning of the Vienna Convention, but the Vienna Convention has its purposes. It’s for the diplomatic communication. This is not…every government information that moves around the world is not a diplomatic communication, so if there is a need to move towards better data security in the world, I think that would need a new perspective from the international community.”

(interview 19 - 21/11/18)

I broadly subscribe to this view and believe that a complete ‘rewrite’ of the Vienna Convention is unlikely. However, as highlighted above, there is scope to suggest that if more states follow Estonia and Luxembourg’s lead, and more Data Embassies are established, then an adjustment to the VCDR would be appropriate in order to reflect changes in diplomatic practice in today’s digital age. How could this be achieved? In truth, gaining consensus from the international community at present would be unlikely, particularly as we are yet to see the Estonian Data Embassy fully operational and legally stress-tested in any form. But, as a form of policy recommendation going forward, I propose that the Estonian government could look to lead on the creation of a Tallinn Convention - an extension or appendage to the existing Vienna
Convention that would aim to incorporate the diplomatic protection of state data, information systems and infrastructures to outside that of the traditional diplomatic mission. Taking inspiration from the success of the *Tallinn Manual* (Schmitt, 2013; 2017), and its influential role in capturing how existing international law applies to cyberspace, the *Tallinn Convention* could look to build consensus within the international community regarding extraterritorial data storage and the interpretation of diplomatic law in a digital age.

Building consensus within the international community is a crucial aim/goal if any amendments to the VCDR were ever going to take place. As one interviewee warned: “of course they have to convince the rest of the world that this applies, because you cannot be a law unto yourself” (interview 3 - 16/05/18). One step in this direction is to draw on other relevant examples where similar immunities have been afforded to data in this way. As highlighted in Section 4.2.3, there are now other examples whereby similar immunities have been provided outside of a state context – such as agreements between the Luxembourg government and NATO, the European Patent Archives and EU Commission, who are hosting their data with similar immunities being afforded in another one of Luxembourg’s Tier IV data centres. Although none of these examples reflect the exact circumstances described in this research – i.e. an agreement between two states – they nonetheless demonstrate how new technological advances have had an influence on the interpretation of existing international Conventions and declarations. As such, our analysis concluded that if more examples of this kind of diplomatic agreement enter into force in the future, then it could well root into customary international law (Robinson et al., 2019: 395). Of course, it may well be some time until we see additional Data Embassies in full operation, but given the growing interest in the Data Embassy and the promise of extraterritorial data storage (as outlined in this chapter), any subsequent examples that emerge in the coming years may offer credence to the suggestion that the Vienna Convention should be updated or extended to reflect changes to diplomatic practice in today’s digital world. One of the biggest hurdles, however (as stated by the interviewee above), is that Estonia and Luxembourg now face the task of convincing other states that such an approach to state-level data storage and security is warranted and justified.

### 7.3 Conclusion

This chapter has explored what impact the Data Embassy has had (or may have in the future) on conceptualisations of geopolitics, diplomacy and international law. By viewing the Data Embassy through

---

17 A similar agreement is also in place at eu-LISA (an agency for operational management of large-scale IT systems, based in Tallinn) which at an EU-level enforces that “The Protocol on the Privileges and Immunities of the European Union shall apply to the Agency” (EUR-Lex, 2017).

18 The International Committee of the Red Cross (ICRC) defines customary international law as being comprised of “rules that come from ‘a general practice accepted as law’ and that exist independent of treaty law” (ICRC, 2010). Still considered a primary source of international law, it is often used to fill the gaps left by treaty laws and conventions (such as the VCDR).

19 Interestingly, in 2018 the Kingdom of Bahrain passed national legislation that will allow “foreign parties” to store their data in data centres located in the country whilst being “subject to the domestic law in the ‘Foreign State’ where the relevant consumer resides” (Fawcett et al., 2020). Although it has been described as ‘Bahrain’s Data Embassy Law’ it is important to note that it does not function like the Data Embassy conceptualised in this thesis – rather, it relates to the storage of commercial data. But this does point to the influence the Data Embassy concept could have on international law in the future as other states begin to implement different forms of data sovereignty laws (see Section 2.1).
the lens of an anomalous geopolitical space (Jeffrey et al., 2015), I have argued how the Data Embassy embodies an alternative form of geopolitics that deviates from international norms and traditional forms of statehood. In doing so, the preceding analysis has charted a number of ways the Data Embassy challenges conventional forms of geopolitics, diplomacy and international law, drawing a number of cogent (yet tentative) conclusions around the Data Embassy and its impact upon the notion of the state, embassy and Vienna Convention.

In the first half of the chapter, I examined how the Data Embassy has opened up new debates regarding statehood, sovereignty and political legitimacy in a digital age. First, I analysed the novel practice of ‘hibernating’ the state in the context of the Estonian Data Embassy. As a form of state improvisation, I argue that the process of hibernation not only plays on ideals of self-preservation and political legitimacy, but also serves as a mechanism for the state to recover and repurpose itself in the event of an emergency. I also addressed concerns around the Data Embassy’s utility in the event of an emergency, determining that it has a fairly reduced functionality and benefit for the everyday Estonian if, for example, its government were forced once again into exile. Thus, I concluded that the Data Embassy is at its most expedient as a form of data backup/recovery for the state.

Next, I reflected on how the Data Embassy has been reimagined in an array of different geopolitical contexts and futures. Drawing on examples involving Catalonian independence or attempts by ISIS to ‘backup the caliphate’ to the cloud, I recognised how, in just a number of years, the Data Embassy has evoked a number of distinct imaginaries regarding how the state could survive and operate in the event of an emergency (e.g. natural disaster, loss of territory, forced exile). Critiquing the notion of a virtual state and its effectiveness in the event of an emergency, I then argued that an extraterritorial Data Embassy would unlikely be considered a legitimate political entity under international law. Nevertheless, it is clear that there is further research required on the topic of virtual states and their limitations within a conventional international system.

In the second half of this chapter, I examined what impact the Data Embassy may have on the future practice of diplomacy. Speaking to McConnell et al.’s (2012) work on unofficial diplomacies, I argue that the Data Embassy has formalised a new ‘alternative’ form of diplomacy that is sited within the extraterritorial data centre. From this, I explored what impact the Data Embassy could have on future inter-state relations, contending that the bilateral agreement signed between both Estonia and Luxembourg has signified a new kind of diplomatic relationship between the two countries, one that is grounded through the extraterritorial hosting and storage of state data. Furthermore, I suggest that states may look to utilise the Data Embassy strategically in the future, arguing that the siting of future Data Embassies may play an influential role in establishing new diplomatic relations around the world.
Next, in recognising that the Data Embassy is something of a misnomer, I have argued that we should extend the definition of an embassy outside the traditional confines of a diplomatic mission. Conceptualising the notion of a digital embassy, I suggest that such a term allows us to attend to novel diplomatic sites and spaces (such as MFA websites and data centres) that function like embassies. Furthermore, for Estonia, I argue that the ‘embassy’ plays an important affective role for the state, providing ontological security for both the Estonian elite and its citizenry. Finally, I examined to what extent the Data Embassy has impacted upon international law, arguing that the agreement between Estonia and Luxembourg has set an influential legal precedent with regards to the diplomatic protection of state data and information systems outside of a traditional embassy. Building on ongoing research in this area, I suggest, as a form of policy recommendation, that with the advent of more Data Embassies in the future, an extension to the existing Vienna Convention could be beneficial to reflect changes to diplomatic practice in today’s digital age.
‘Leaving Tallinn after spending the last three months here has been incredibly difficult. I’m sad to leave behind friends, colleagues and the challenges/freedom that fieldwork has afforded me – not that I’ll miss -6 degrees and snow (I’ve been told it gets even colder in January and February). The last few months have been a rollercoaster, from writing papers and conducting countless interviews (and receiving a number of rejections too), to exploring the Estonian countryside and the experience of living away from home for the first time. I’m grateful for the connections made, happy with the data I’ve collected and the progress that’s been made with my research. I’m sad to be leaving this city behind – and wish I could do it all again – but I know I’ll be back soon. Whether as a researcher or tourist, I’m not sure.’

(December 2018)
Chapter 8 – Conclusion
This thesis has explored the geopolitical, diplomatic and legal implications of extraterritorial data storage, specifically, in the context of a state-level emergency or crisis. With the Estonian Data Embassy serving as the central focus and case study of this research, its main aim has been to examine how this novel e-government/national security concept challenges many fundamental principles of geopolitics, diplomacy and international law. Drawing on nearly three years of ethnographic engagements with Estonian policymakers, cybersecurity professionals, academic experts, and those working close to the project itself, it has contextualised the Data Embassy’s emergence alongside Estonia’s own unsettled past, its present-day realities, and the enduring uncertainties surrounding its future, arguing that the concept is intertwined in an ongoing state continuity project that is rooted in the ontological insecurities and collective memory of the state. Reflecting on the potential advent of more Data Embassies in the future, this thesis has also considered the wider utility and function of the Data Embassy and what impact this may have on the future practice of statecraft and diplomacy – from the anticipatory logics of state hibernation in mitigating the threat of conflict or climate change, to the creation of novel diplomatic relations and norms within the extraterritorial data centre.

Touching on a number of emerging interdisciplinary debates across fields of geopolitics, cybersecurity, digital governance, diplomatic studies, critical data studies and international law, this thesis makes several important contributions to these areas whilst laying the conceptual foundations from which future research on the Data Embassy can emerge.

The first relates to statehood and the practice of statecraft. In many ways, the Data Embassy’s emergence points to a radical shift in how states may look to function and endure in the future. As this thesis has identified, at a macro level, the premise and promise of extraterritorial data storage and operating a state from the cloud will continue to attract interest around the world in the coming decades, particularly from those states that are facing limited political recognition, existential threats to their independence, or threats from natural hazards and the wider climate emergency (see Chapter 7). Situating the initiative alongside work in political geography that examines contemporary forms of statehood and alternative sites of political legitimacy (Jeffrey, 2013; McConnell, 2009; Pistor, 2020), I argue that the Data Embassy is best understood in the context of an anomalous geopolitical space and entity where “international norms and ideals of statehood” are increasingly being “called into question” (Jeffrey et al., 2015: 180). With more Data Embassies potentially on the horizon, such an entity raises a number of critical (and novel) questions for scholars and policymakers as we consider geopolitical logics and imaginaries of states ‘hibernating’ or existing virtually in the cloud. Indeed, whilst the ideal of an entirely virtual, cloud-based state seems unlikely within a conventional state system (see Section 7.1.2), the practice of hibernation allows us to reconceive the state in a digital age – one that is not only marked by logics of survivability and self-preservation, but of recovery and repurpose too. Furthermore, by introducing the notion of a
Government-in-anticipation-of-Exile (see Section 6.4), albeit from an Estonian context, this research posits the Data Embassy as a form of state intervention and anticipatory logic that seeks to prevent, pre-empt and prepare for a future emergency or crisis (Anderson, 2010). Future work in areas of state theory/state recognition and futures research could benefit from adopting such a lens – in particular, when considering attempts by state and non-state actors to ‘futureproof’ themselves from emergencies – whilst future research on the Data Embassy could be augmented by examining the concept as part of a state’s wider national security strategy and governance of emergencies (Adey and Anderson, 2012; Adey et al., 2015; O’Grady, 2018a).

At a micro level, this thesis has also explored what the Data Embassy reveals (or potentially ‘masks’) about the everyday practice and performance of the Estonian state. Attending to one of the main research questions of why Estonia is looking to ‘backup’ the state to the cloud, it found the government’s motivations to be somewhat inconsistent and ‘cloudy’ which, in turn, revealed the Data Embassy to be part of a much more profound state continuity project that is embedded in the ontological insecurities and collective memory of the state (see Chapter 5). Reflecting on the archival ‘realities’ facing Estonia, its everyday security discourse regarding the Russian threat, and how the country frames (and brands) itself as part of a wider geopolitical culture, this research has captured the tensions and unique circumstances that led to the Data Embassy’s emergence, and how the state engages in various practices and performances (such as data backups and marketing itself as a digital pioneer) in an effort to manage its everyday ontological insecurities.

These performative practices, I argue, are symptomatic of a much wider, collective state-level anxiety that is not only rooted in the material archive and perpetual uncertainties over the state’s digital ecosystem, but also lived and felt through an everyday affective geopolitics that centres on the Russian threat and ‘sticks’ to historical events such as Soviet occupation, the 2007 cyberattacks and the annexation of Crimea in 2014 (see Chapter 6). In recognising the distinct temporalities to Estonia’s anxiety – and how it is pervasive yet equally productive for the state – this research contributes to wider debates around how certain emotions/affects can be collectivised and identified at a state-level in world politics (see, Mercer, 2014; Nugent, 2019; Toal, 2017), whilst also speaking to a growing body of work that critically attends to Estonian/Baltic/post-Soviet geopolitics and memory studies (Aalto, 2003; Berg, 2000; Kaus, 2002; Mälksoo, 2000; Tamms, 2008).

The second key contribution of this research concerns the precedent set by the Data Embassy and the impact this will have on the future practice of diplomacy and international law. Through a critical examination of the Estonian Data Embassy and its historic hosting agreement with Luxembourg, this thesis has underlined the concept’s novelty and profoundness, whilst making a number of central claims that are of interest to diplomats, policymakers and scholars of diplomacy and international law. The first concerns the formalising of a novel, ‘alternative’ (McConnell et al., 2012) diplomacy that now takes place from the extraterritorial data centre. Recognising that this was the first time two states had ever agreed to provide
these kinds of protections and immunities outside of a diplomatic mission, this research has argued that the decision to establish a Data Embassy in Betzdorf, Luxembourg, signifies a new kind of diplomatic relationship between two countries that is grounded in the extraterritorial hosting and storage of state data (see Section 7.2.1). Speculating on future Estonian Data Embassy locations, and Luxembourg’s role as a Data Embassy ‘hub’, this thesis also questions whether states may look to locate Data Embassies strategically as a means of enhancing their diplomatic standing around the world. Pointing to a new era of ‘Data Embassy diplomacy’, future work in political geography and diplomacy studies can build on this early analysis whilst addressing the wider geopolitical, diplomatic and security implications of a global network of Data Embassies should other states follow Estonia and Luxembourg’s lead in the future.

This thesis has also considered the role and function of an embassy in a digital age (see Section 7.2.2). Acknowledging the precedent set by affording embassy-like provisions within an extraterritorial data centre, this research has called for the definition of an embassy to be extended outside of the traditional confines of a diplomatic mission. Building on a growing interest in ‘virtual embassies’ and forms of digital diplomacy more broadly (see Section 2.3), this thesis has coined the notion of a digital embassy in an effort to capture and attend to novel forms of diplomatic practice and alternative diplomatic sites and spaces (such as the Data Embassy) that adopt similar functions and characteristics to that of a traditional diplomatic mission. Finally, this research has examined what impact the Data Embassy may have on international law and diplomatic protocols in the future. Building on ongoing research that has recognised that the Vienna Convention is not deemed presently suitable for the protection and inviolability of data and information systems outside of the traditional diplomatic mission (Robinson et al., 2019), this research has questioned whether the protocol is fit for purpose within a digital age. With the Data Embassy again serving as a precedent in this area, and binding both countries to fulfil specific obligations and similar diplomatic protections and immunities to that of a traditional embassy, our research concluded that there is enough scope and legal precedent to suggest a re-assessment or extension of the Vienna Convention may prove beneficial in the future to reflect changes in diplomatic practice in today’s digital age – recommending the Estonian government leads on the creation of a Tallinn Convention (see Section 7.2.3). The success of such an approach does, however, hinge on the advent of more Data Embassies and whether states are willing to adopt similar agreements, whilst there is also a greater need for interdisciplinary research on diplomatic and legal implications of extraterritorial data storage and their role in the context of the diplomatic protocols such as the Vienna Convention.

Providing one of the first in-depth, critical studies into the Data Embassy, this research has highlighted the concept’s novelty and significance, not only for scholars interested in geopolitics, cybersecurity and diplomacy, but also for policymakers, diplomats and the security practitioner community. Yet, in offering a rich, contextual case study of the Data Embassy in an Estonian context, and by speculating on its transformative potential for other states around the world, this work also recognises its limitations as a
study and the conclusions it makes. Thus, given the novelty of both this research and the Data Embassy itself, any future research in this area will be strengthened by any retrospective analysis or review of the pilot phase of the Data Embassy project in Luxembourg. Going one step further, if other countries follow Estonia and Luxembourg’s lead, future work will also benefit from comparative studies which allow the Data Embassy to be compared and contrasted across different geopolitical contexts and spatio-temporalities. Addressing a limitation of the Estonian government’s own startup approach (see Section 5.3), and overall scope of this thesis, further academic scrutiny from the information security community could also help address potential future roadblocks regarding data security and cloud infrastructure if a network of Data Embassies emerges in the future.

In drawing this thesis to a close, I want to briefly reflect on where this research and the Data Embassy itself may be headed. Bringing the key findings and contributions of this research project together, this chapter has highlighted why the Data Embassy matters – not only conceptually/empirically, but practically too - whilst outlining its significance to a number of emerging debates across a wide variety of disciplines. Like the Data Embassy itself, this area of research is still very much in its infancy and it will be fascinating to observe where future directions of work and practice begin to emerge. One cursory prediction will be that over the next decade or so, in light of rapid technological change and rising global insecurities, a number of states will begin to re-evaluate their national security strategies and emergency contingency plans; whilst the utility and overall value of the Data Embassy will begin to rise, particularly for states facing up to legitimate threats to their independence and existence.

In my own work, I will continue to trace these developments, whilst exploring the wider utility of the Data Embassy and consider to what extent it can enable states to endure and achieve political legitimacy in the face of potential conflict and exile, or natural disaster and climate catastrophe. From an Estonian perspective, once the success of the Luxembourg project is fully assessed, attention will likely turn to where the next Data Embassy will emerge, with a candidate likely to fall outside the EU and with strong links diplomatically (e.g. the U.S. or Canada). It may be a little too early to predict if we will see a future network of Data Embassies around the world. Nevertheless, this thesis has illuminated and interrogated the transformative potential of the Data Embassy and the ontological security it offers via the extraterritorial data centre. As such, the Data Embassy will continue to elicit interest from other states as they navigate and negotiate their function and role within a strategically challenging digital age.
Bibliography


Bilo, E. and Mountz, A. 2016. “For institutional ethnography: Geographical approaches to institutions and the everyday”, Progress in Human Geography, 40(2), 199-220.


Griffith, E. 2014. “Why startups fail, according to their founders”,


Jackson, T. 2018 Paradiplomacy and political geography: The geopolitics of substate regional diplomacy”, *Geography Compass*, 12(2), 1-11.


Mills, S. 2013. “Cultural-Historical Geographies of the Archive: Fragments, Objects and Ghosts”, Geography Compass, 7(10), 701-713.


Rühle, M. 2014. “NATO Enlargement and Russia: Discerning Fact from Fiction”, The Journal of the National Committee on American Foreign Policy, 36(4), 234-239.


Trendall, S. 2019. “We have only scratched the surface’ – Estonia’s CIO on what’s next for the world’s most celebrated digital nation”, (https://www.publictechnology.net/articles/features/%E2%80%98we-have-only-scratched-surface%E2%80%99-%E2%80%93-estonia%E2%80%99s-cio-what%E2%80%99s-next-world%E2%80%99s-most), (accessed: 20 February 2020).


Vooglaid, K. 2018. “What should be the state’s role in a digital future?”,
(accessed: 10 January 2020).


Walker, S. 2019. “Estonia’s president plays down criticism over Putin meeting”,


The White House. 2014. “Remarks by President Obama to the People of Estonia”,


Appendices

A – Data Embassy protagonists
Throughout this thesis, I will refer to a number of key protagonists that have played a crucial role in this story. Some played a vital role in the development and implementation of the Data Embassy itself, whilst others stand as key ‘intellectuals of statecraft’ (Ó Tuathail and Agnew, 1992) that have played some part in Estonia’s (or the Data Embassy’s) recent political history. By introducing them here, I hope to avoid any repetition or positional confusion throughout subsequent chapters and analysis.

First, is Taavi Kotka. Kotka can be credited with spearheading the Data Embassy concept during his time as government Chief Information Officer (2013-2017), but first came to my attention during my Master’s research into the Estonian e-Residency program in 2015 (Robinson, 2015). At the time, Kotka had proclaimed that by 2025 Estonia would have ‘10 million’ e-Resident’s, with the idea of offering every world citizen a government-issued digital identity, and for non-residents to access Estonia’s wealth of digital services - such as creating a company online, banking and tax declaration services (Pardes, 2016). Prior to this, Kotka had made serious inroads in the private sector, where, as CIO of Nordic tech giant Nortal, he was awarded Ernst Young’s Entrepreneur of the Year (2011). But it was in government where Kotka began to make serious advances. Playing a central role in the development of Estonia’s Digital Agenda 2020 strategy (MoEAC, 2013), Kotka is credited with reforming many aspects of Estonia’s public e-services, including the introduction of a no-legacy policy (see Chapter 4). He was awarded European CIO of the year in 2014, and it could be argued that without his entrepreneurial approach to digital government, and the success of e-Residency, that his ‘moonshot’ Data Embassy proposal may not have got off the ground quite so easily.

Kotka is mentioned on a number of occasions throughout this thesis, from early quotes in government reports relating to the Data Embassy (MoEAC, 2015; 2016) to his general role in orchestrating the project during its early stages (see Section 4.2). Right at the end of this process, I was fortunate to sit down with Taavi to talk a little more about my research, but to also learn a little more about how he believes the project came to be and how it has progressed in the intervening years. Now working in the private sector on areas of digital transformation, he is still regarded as a prominent voice and figurehead in Estonia’s digital society.

---

1 I was fortunate to speak both on and off the record with a number of individuals close to the project. As Chapter 3 will explain in greater detail, for issues of anonymity of consistency, I have decided to anonymise all quotes throughout the thesis, except for Taavi Kotka, who insisted that all quotes were attributed.
2 This figure has since been revised with the project’s goals changing considerably, with the Estonian government now aiming for 1 million e-Resident’s and an indirect income to the economy of €1.8bn (Pau, 2017).
An example of this was Kotka’s appearance in a recent VICE documentary on ‘The Future of Work’ that featured on U.S. channel HBO, cross-country skiing with the presenter and detailing many of the practical innovations now found in ‘e-Estonia’ (HBO, 2019). As well as recently serving as Special Advisor to European Commission vice-president Andrus Ansip on matters delating to the digital single market, Kotka is also in the latter stages of finishing his PhD thesis on the topic of the Data Embassy.

Prior to Kotka, there was Linnar Viik, often referred to as one of the ‘founding fathers’ of Estonian e-governance. Known as a “serial entrepreneur” and founder of the e-Governance Academy in Tallinn, Viik was ICT advisor to the Estonian Prime Minister Mart Laar, where he pioneered many of Estonia’s technological advances throughout the 1990s, and is often credited as having more power and influence than many ministers at the time (Kattel and Mergel, 2018). Former Prime Minister Mart Laar is also credited throughout this thesis, particularly in Chapter 4, for his drive and leadership throughout the 1990s and early 2000s (although, some that I spoke to felt Laar’s role has been exaggerated slightly).

If Viik was Laar’s right-hand man for much of the 1990s, then it would be fair to suggest that Taavi Kotka was the same for former President Toomas Hendrik Ilves. Another leader, and prominent figure in this thesis, Ilves’ decade in office (2006-2016) presided over some of the most significant events in recent Estonian history, including the 2007 cyberattack, the 2008 Russo-Georgian war, and the annexation of Crimea in 2014. Although the position of president is largely symbolic, throughout this period (and arguably still today), Ilves has been a vocal critic of Russia and its leader Vladimir Putin on the world stage (Keen, 2016) – most notably on Twitter, very much serving as a window to Estonia’s foreign policy views.

Prior to becoming president, Ilves also played a major diplomatic role as U.S. ambassador in 1993 and Minister of Foreign Affairs intermittently between 1996-2002. As Neil Taylor notes, Ilves worked closely with then President Lennart Meri on driving Estonia closer towards EU and NATO membership (2018: 191). Discussed further in Chapter 4, it is during this period that Ilves is also credited (along with education minister, Jaak Aaviksoo) with pioneering project ‘Tiger Leap’ that led to large-scale improvements in ICT and education. Learning to program himself at the age of 13, Ilves was in the rather unique position as being a ‘president that could code’, and would often be lauded for his thought-leadership

3 Despite his obvious achievements as government CIO and international acclaim from the media, Kotka was something of a divisive figure to many that I spoke to during the course of completing this thesis – some highlighting his roughshod approach, but also that his entrepreneurial mindset likely ruffled a few feathers. Kotka hinted at such himself, openly admitting that when he announced the Data Embassy in 2013 he received “lots of criticism […] Like ‘why is Kotka messing with the Data Embassies?’” (Taavi Kotka interview - 15/07/19).

4 Today, Linnar Viik sits on the Estonian ‘e-government council’ – a fairly inconspicuous committee (at least to the wider public) that steers current e-government innovation and development, including other government ministers and the current prime minister, Jüri Ratas.

5 One interviewee described Kotka as Ilves’ ”technical guy” (interview 28 - 17/07/19) and I believe he shared a similar relationship to the president as Linnar Viik did to Prime Minister Mart Laar during the 1990s. Both Viik and Kotka are described as serial entrepreneurs, and I purposefully make this connection as I also believe this may have played a key role in Kotka’s ability to drive initiatives such as e-Residency and the Data Embassy in government.

6 Ilves also served as Canadian and Mexican ambassador at the same time, perhaps stressing the lack of Estonian diplomatic resource and infrastructure at the time.
and direction in areas of e-government and cyber security (particularly after the 2007 cyberattack). British journalist Edward Lucas recently remarked that Ilves had well and truly “put Estonia on the map” during his presidency, and that his ceremonial role still afforded him diplomatic successes, namely through his twitter account (Taylor, 2018: 202).

Kersti Kaljulaid was announced as Ilves’ successor as president in October 2016, becoming Estonia’s first female (and youngest) head of state since the country declared its independence in 1918. Announced as president during the development of this thesis (and the Data Embassy), Kaljulaid joins current Estonian Prime Minister Jüri Ratas (2016-present), as two key figureheads that have aimed to publicly promote the Data Embassy on the global stage. Ratas is mentioned during vital milestones in the development of the Data Embassy, such as the signing of the historic bilateral agreement between Estonia and Luxembourg (see chapter 4). In what might be seen as shift from Ilves’ vocal criticisms, I’ve been struck by Kaljulaid’s more cautious and diplomatic stance on issues relating to Russia, but also how she directly refuted a causal link between Russia and the emergence of the Data Embassy (see Chapter 5).

Finally, I turn to other noteworthy names that have been close to the Data Embassy project throughout the years I have been completing this research. Kotka’s successor as government CIO, Siim Sikkut, is now spearheading the Data Embassy project through its initial pilot phase in Luxembourg, and has been a key fulcrum for any public discussion or media attention that has surrounded the Data Embassy during the completion of this thesis. Over the coming years, if Sikkut stays in his role, he will become a vital figure in the Data Embassy’s future strategy and may have a major say over any future Data Embassy locations. From a Luxembourgian perspective, Prime Minister Xavier Bettel and former government CIO Gilles Feith also warrant a mention as they played crucial diplomatic and administrative roles in instigating the first Data Embassy to be located in Luxembourg from 2015 onwards. In future years, they may also play a key role in Luxembourg positioning itself as a ‘hub’ for other states to establish Data Embassies within their government-operated data centres (see Chapters 4 and 7).
## B – Interview data

<table>
<thead>
<tr>
<th>Interview</th>
<th>Date</th>
<th>Sector</th>
<th>Role</th>
<th>Data Emb</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interview 1</td>
<td>09/08/17</td>
<td>Public</td>
<td>Estonian Civil Servant – Technology Policy</td>
<td>Embassy</td>
<td>I</td>
</tr>
<tr>
<td>Interview 2</td>
<td>12/02/18</td>
<td>Academia</td>
<td>Professor of Innovation and Public Governance</td>
<td>Embassy</td>
<td>O</td>
</tr>
<tr>
<td>Interview 3</td>
<td>16/05/18</td>
<td>Private</td>
<td>Defence and Security Policy Expert - Think Tank</td>
<td>O</td>
<td></td>
</tr>
<tr>
<td>Interview 4</td>
<td>17/05/18</td>
<td>Public</td>
<td>Estonian Civil Servant – Technological Systems</td>
<td>I</td>
<td></td>
</tr>
<tr>
<td>Interview 5</td>
<td>17/05/18</td>
<td>Public</td>
<td>Estonian Civil Servant – Technological Systems</td>
<td>I</td>
<td></td>
</tr>
<tr>
<td>Interview 6</td>
<td>18/05/18</td>
<td>Public</td>
<td>Estonian Civil Servant – Policy and Law</td>
<td>I</td>
<td></td>
</tr>
<tr>
<td>Interview 7</td>
<td>18/05/18</td>
<td>Academia</td>
<td>Professor of e-Governance</td>
<td>O</td>
<td></td>
</tr>
<tr>
<td>Interview 8</td>
<td>23/05/18</td>
<td>Academia</td>
<td>Associate Professor in International Relations</td>
<td>O</td>
<td></td>
</tr>
<tr>
<td>Interview 9</td>
<td>28/05/18</td>
<td>Private</td>
<td>Cybersecurity Policy and Law Policy Expert – Think Tank</td>
<td>O</td>
<td></td>
</tr>
<tr>
<td>Interview 10</td>
<td>31/05/18</td>
<td>Private</td>
<td>Cybersecurity and Defence Policy Expert</td>
<td>O</td>
<td></td>
</tr>
<tr>
<td>Interview 11</td>
<td>01/06/18</td>
<td>Public</td>
<td>Estonian Civil Servant – Cybersecurity and Defence</td>
<td>I</td>
<td></td>
</tr>
<tr>
<td>Interview 12</td>
<td>01/06/18</td>
<td>Public</td>
<td>Estonian Civil Servant – Digital Government and Diplomacy</td>
<td>O</td>
<td></td>
</tr>
<tr>
<td>Interview 13</td>
<td>03/10/18</td>
<td>Public</td>
<td>Estonian Civil Servant – Economic Policy</td>
<td>O</td>
<td></td>
</tr>
<tr>
<td>Interview 14</td>
<td>12/10/18</td>
<td>Private</td>
<td>Cybersecurity Policy – Think Tank</td>
<td>O</td>
<td></td>
</tr>
<tr>
<td>Interview 15</td>
<td>12/10/18</td>
<td>Private</td>
<td>Defence, Security and Technology Policy Expert – Think Tank</td>
<td>O</td>
<td></td>
</tr>
<tr>
<td>Interview 16</td>
<td>15/10/18</td>
<td>Academia</td>
<td>Associate Professor in Computer Science</td>
<td>I</td>
<td></td>
</tr>
<tr>
<td>Interview 17</td>
<td>29/10/18</td>
<td>Public</td>
<td>Estonian Civil Servant – Digital Policy</td>
<td>O</td>
<td></td>
</tr>
<tr>
<td>Interview 18</td>
<td>07/11/18</td>
<td>Public</td>
<td>Estonian Civil Servant – Legal Affairs</td>
<td>I</td>
<td></td>
</tr>
<tr>
<td>Interview 19</td>
<td>21/11/18</td>
<td>Public</td>
<td>Estonian Civil Servant – Legal Affairs</td>
<td>O</td>
<td></td>
</tr>
<tr>
<td>Interview 20</td>
<td>27/11/18</td>
<td>Academia</td>
<td>Research Analyst – Cybersecurity</td>
<td>O</td>
<td></td>
</tr>
<tr>
<td>Interview 21</td>
<td>28/11/18</td>
<td>Academia</td>
<td>Professor of Public Administration and Governance</td>
<td>O</td>
<td></td>
</tr>
<tr>
<td>Interview 22</td>
<td>06/12/18</td>
<td>Private</td>
<td>Management Consultant – Cybersecurity</td>
<td>O</td>
<td></td>
</tr>
<tr>
<td>Interview 23</td>
<td>06/12/18</td>
<td>Public</td>
<td>Estonian Civil Servant – National Heritage</td>
<td>O</td>
<td></td>
</tr>
<tr>
<td>Interview 24</td>
<td>12/12/18</td>
<td>Academia</td>
<td>Lecturer in Law</td>
<td>O</td>
<td></td>
</tr>
<tr>
<td>Interview 25</td>
<td>04/04/19</td>
<td>Public</td>
<td>Diplomat</td>
<td>O</td>
<td></td>
</tr>
<tr>
<td>Interview 26</td>
<td>21/05/19</td>
<td>Private</td>
<td>Cybersecurity and Technology Policy Expert</td>
<td>I</td>
<td></td>
</tr>
<tr>
<td>Interview 27</td>
<td>15/07/19</td>
<td>Private</td>
<td>Taavi Kotka - CEO, Proud Engineers</td>
<td>I</td>
<td></td>
</tr>
<tr>
<td>Interview 28</td>
<td>17/07/19</td>
<td>Private</td>
<td>Information Security Professional</td>
<td>O</td>
<td></td>
</tr>
</tbody>
</table>
C – Interview questions

An example of my research questions used during interviews (September – December 2018). I worked off a number of iterations of this crib-sheet design during my time in the field – adapting my questions and themes as my research progressed.

1. Why is the Data Embassy Initiative necessitated?

Under what circumstances? What would you say is the primary motivation?

- A combination of all of these? Virtual/physical dichotomy → threats to digital ecosystem obvious, but also escalating physical tensions in past/present → threat of future occupation: ‘it could happen again’
- 2007 as a cornerstone moment? ('Digital fault line' Priisalu & Ottis)
- Might it serve as a deterrence?
- Gov. very clear to play down Russian influence – surprise to you?

This research is arguing that Estonia may be experiencing a geopolitical anxiety: over its information systems, over Russia, over the futurity of the state. Would you agree?

- Occupation, territorial integrity, threats to future of Estonian Republic → something that is engrained/deep-rooted/embedded into Estonian psyche:
  - Perhaps explain why Anxiety > Fear. Anxiety not always a negative.
  - Anxiety relevance e.g. often states/gov are seen as ‘fearful’
  - Russia are not building up military presence along border, but previous events/moments may play into government thinking/actions

This research will also consider that the Estonian government is operating as a Government-in-anticipation-of-Exile. [discuss under a hypothetical scenario] [maybe drop if convo to o long?]

- Documentation talks of Estonian government potentially operating ‘outside of its own borders’
- But how/would this actually function in practice? Under what circumstances? e.g. under occupation, what services would critically still be required/be able to function anyway? e.g. healthcare records, tax…
- Anxiety being put to work productively – the process of ‘backing up’ the state as an anticipatory logic.

2. The Data Embassy and its impact upon traditional concepts

(Geopolitics, Cyber/Information Security, Law, Diplomacy)

Extraterritorial Data Storage: data sovereignty and diplomatic immunity

- Does Estonia buck trend on our current understanding of data sovereignty?
- New, difficult legal and political questions are being asked in terms of data and sovereignty:
  - What happens when government data is stored outside of its own borders?
  - How should governments respect the integrity of other governments’ data held in the cloud?
- Yet-to-be-tested scenarios – no clear precedent on international legal frameworks: so DEI has extra-legal layer offered by bilateral agreement.
- To quote Microsoft – maybe Estonia is “setting an influential precedent for Data Sovereignty” in a digital era?
Bilateral agreement (w/Luxembourg):
- [if needed, explain the procurement of server space in government-operated data centre]
- Similar protections/provisions to a traditional embassy – *in the spirit of* VCDR
- “the agreement grants the Estonian premises a similar inviolability under international law.”
- VCDR was ‘not sufficient to set a legal framework for the hosting of data and information systems’
- Initial scepticism concern over ‘data embassy’ terminology usage (particularly in legal community) → bilateral agreement also explicitly does not use term ‘data embassy’ → but also concern on whether VCDR could be applied this way → might the VCDR (1961) be outdated in a digital era?

Reconceptualising the Embassy
- Should we be extending the classical notion of Embassy in a digital era?
  - A new role?
  - Not strictly an embassy per se, but embassy-like provisions for information systems, data and services
  - Digital Embassy [?]: Serving as a digital representation of a traditional diplomatic mission, the digital embassy may also function as a crucial mechanism/device for protecting critical national infrastructure of the sending State from outside of its own borders.

Implications for Diplomacy
- Impact on diplomatic relations – e.g. globally, through bilateral agreements/new relationships between governments
- Might Estonia wish to strategically place/situate data embassies based on: improving diplomatic relations? Links to Russia? (e.g. no links) Increasing its own diplomatic standing on world stage?
  - Luxembourg positioning itself as a ‘hub’ for data embassies.
    - NATO/EU Commission
- Why Luxembourg?
- Future locations?

3. Data Embassy Discourse: past, present and future
- How is/isn't the public debate framed?
  - Any noticeable push back from politicians? Scepticism inside/outside gov? Yourself?
- Data Embassy sustainability/scalability?
  - Could there be a criticism that the project ‘rushed ahead’ without assessing the whole/full picture? (my exp. over there being no clear decisions on technical specs as of yet)
  - Where does this project sit for you? *Conveyor belt* analogy – is this just another in a long line of innovations? A natural progression for any e-gov in the future?
- Good for e-Estonia nation-branding?
  - Pushing boundaries, the first to do X, Y Z. Some might say a PR stunt/gimmick? *(Not necessarily a neg. for a small country)*
Royal Holloway, University of London
Consent Form

To take part in the following research study:

**Distributed Denial-of-Government: The Data Embassy and the geopolitical, diplomatic and legal implications of extraterritorial data storage**

This form is to be read (along with attached participant information sheet) and signed before participation.

<table>
<thead>
<tr>
<th>Statement</th>
<th>Initials or ✓</th>
</tr>
</thead>
<tbody>
<tr>
<td>The nature of this research has been explained to me.</td>
<td></td>
</tr>
<tr>
<td>(if unsure, please see attached participant information sheet)</td>
<td></td>
</tr>
<tr>
<td>I understand that the interview will only be recorded with my consent</td>
<td></td>
</tr>
<tr>
<td>(and used only for transcribing purposes and subsequent analysis).</td>
<td></td>
</tr>
<tr>
<td>I understand that what I say, or any information I provide, will be</td>
<td></td>
</tr>
<tr>
<td>treated as confidential by the researcher.</td>
<td></td>
</tr>
<tr>
<td>I understand that my participation is voluntary and that I am free to</td>
<td></td>
</tr>
<tr>
<td>withdraw at any time without giving a reason.</td>
<td></td>
</tr>
<tr>
<td>I would like to receive a copy of the final research report.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Researcher Name (print below):</th>
<th>Signature:</th>
<th>Date:</th>
</tr>
</thead>
<tbody>
<tr>
<td>______________________________</td>
<td>------------</td>
<td>-----------</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Participant Name (print below):</th>
<th>Signature:</th>
<th>Date:</th>
</tr>
</thead>
<tbody>
<tr>
<td>______________________________</td>
<td>------------</td>
<td>-----------</td>
</tr>
</tbody>
</table>
I am a current PhD researcher at the Centre for Doctoral Training (CDT) in Cyber Security at Royal Holloway, University of London. My research is primarily grounded in Estonia, focusing on the multitude of digital technologies its government started to employ since the regaining of independence from the Soviet Union in 1991.

Exploring initiatives such as Estonian e-Residency, the government’s use of blockchain technology, and now the utilisation of data embassies, my work aims to develop a greater understanding of the impact these technologies have on our traditional conceptualisation of geopolitics and notions of nation-state, border and embassy.

The Estonian Data Embassy Initiative (DEI) stands, arguably, as one of the most transformative government digital strategies in modern times. Its premise - of extraterritorial data security and embassy-like exceptions/provisions for data held in secure data centres – will arguably push the boundaries of what it means to be a state in the 21st Century. It also opens up crucial questions regarding future geopolitical relations and international laws around data sovereignty.

**Project aims and outputs**

The aims of this research are twofold. First, it aims to align the DEI with current geopolitical scholarship, positing that our traditional conceptualisations of terms such as state, territory, sovereignty, border, embassy, and so on, are in need of redefining in a digital age. In doing so, this research will also begin to ask crucial questions around why (and under what historical and geopolitical circumstances) would a government like Estonia’s look to pioneer such an initiative and ‘out-source’ various key components of the state around the world.

Second, this research hopes to invigorate debates within cyber/information security and law, positing the potential ramifications for data security and international law. In asking necessary questions relating to the security of government data storage in the cloud, and yet-to-be-tested scenarios related to the Vienna Convention on Diplomatic Relations (1961) being applied to data, the concept of data embassy is in urgent need of fresh, interdisciplinary attention. This may be even more prescient if we begin to see other governments following Estonia’s lead. By gaining the knowledge and expertise of various experts, officials and policy-makers, this research will help provoke healthy debate and discussion around future data embassy adoption and policies relating to extraterritorial data storage.

**Methods of engagement**

This research is driven by a qualitative methodological approach, utilising semi-structured interviews with selected participants, alongside ethnographic observations during extended periods in Estonia.

Participants are not expected to have specialised knowledge of data embassies per se. Rather, this research project is looking for participants to share their own knowledge, expertise and experiences across a variety of themes – from digital transformation to cyber security and the Estonian digital/political ecosystem more broadly.

**Participants are free to fully or partially withdraw at any time, without giving a reason.**
Data management

All data will be safely stored and only the named researcher will have access to these data. All data will be kept confidential and participant involvement will be anonymised to the extent that no personal data will be released. The results of the study will be written up as an overall thesis, whilst parts may be published further in academic journals and blogs.

As outlined in the consent form, participants may request any final copies of such outputs before publication.

Ethical considerations

This research is not expected to raise any ethical concerns. However, as the work involves human participants, ethical approval and consent must be sought in advance. All research has been approved by the project supervisory team (Prof. Keith Martin & Prof. Klaus Dodds), and also through the Department’s internal approval procedures, and is bound by the College code of ethics in research.

Research themes

This research aims to amalgamate three overarching themes throughout: geopolitical anxieties, data sovereignty and the notion of embassy in a digital era. As such, discussions with participants will centre around the following research questions:

1. To what extent will the Data Embassy reconfigure our traditional conceptualisations of geopolitics?
   i) Under what circumstances is the Estonian data embassy necessitated?
   ii) Can the notion of geopolitical anxiety be applied to our understanding of why the Estonian Data Embassy Initiative is being established?
   iii) Does the Data Embassy Initiative represent a Government-in-anticipation-of-exile?

2. How does the Data Embassy and the extraterritorialisation of data challenge our conventional understandings of data mobility, storage, and law?

3. Do we need to reconsider the notion of ‘Embassy’ within a digital era?
   i) Should we be conceptualising the embassy beyond its traditional confines?
   ii) What impact, if any, will the Data Embassy have on future diplomatic relations or diplomacy more broadly?

Contact details

If you would like any more information, or if you have any outstanding questions, then please feel free to contact the researcher.

Nicholas Robinson
e: Nicholas.Robinson.2014@live.rhul.ac.uk
m: [redacted]
t: @nickdr92

Centre for Doctoral Training (CDT) in Cyber Security
Information Security Group | Department of Geography
Royal Holloway, University of London