TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Anna-Maria Kolessova 212035IVGM

Estonia's Data Embassy Initiative: A Framework for Building Cyber Resilience in Other Countries

Master's thesis

Supervisor: Eric Blake Jackson
PhD Candidate

Tallinn 2023

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia
teaduskond

Anna-Maria Kolessova 212035IVGM

Eesti andmesaatkonna algatus: Raamistik küberkerksuse suurendamiseks teistes riikides

Magistritöö

Juhendaja: Eric Blake Jackson
Doktorant

Tallinn 2023

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature, and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Anna-Maria Kolessova

08.05.2023

Abstract

The thesis examines the data embassy initiative in regard to cyber resilience. It focuses on practical implementation by exploring the factors and criteria for selecting a host country for a data embassy. In addition, the research discusses the future evolution of data embassies and suggests practical recommendations for countries interested in opening a data embassy.

This study used a case study approach, data triangulation, semi-structured interviews and thematic analysis to achieve the study's objectives.

The findings indicate that the data embassy initiative contributes significantly to Estonia's cyber resilience and is a part of the national cybersecurity strategy to enhance cyber resilience. The factors for selecting a location include political, technical, legal and geographical considerations. Several risks and challenges are associated with establishing a data embassy. The thesis summarises essential aspects and provides a practical guide for implementing data embassies in the Data Embassy Implementation Framework.

This thesis is written in English and is 60 pages long, including 6 chapters, 12 figures and 2 tables.

Keywords: Data embassy, cyber resilience, digital continuity, Estonia

List of abbreviations and terms

AWS	Amazon Web Services
BENELUX	Belgium, Netherlands, Luxembourg
CERT-EE	Computer Emergency Response Team Estonia
CIIP	Critical Information Infrastructure Protection
CIO	Chief Information Officer
CTIE	The Government IT Centre (*Centre des technologies de l'information de l'État*)
CTO	Chief Technology Officer
EU	European Union
IT	Information Technology
KSI	Keyless Signature Infrastructure
NAS	National Academies of Science
NATO	North Atlantic Treaty Organisation
NIST	National Institute of Standards and Technology
OECD	Organisation for Economic Cooperation and Development
OEEC	Organisation for European Economic Cooperation
UNESCO	United Nations Educational, Scientific and Cultural Organisation

Table of contents

List of figures

List of tables

1 Introduction

The world has faced various disruptive events recently, such as the pandemic and wars. In addition, the Russo-Ukrainian war has caused consequences beyond the directly involved countries. As a result, the question of security in all possible areas is becoming increasingly important. After removing a Soviet-era tank from its pedestal in Narva, in 2022, Estonia was subject to extensive cyberattacks [1]. It was not the first time Estonia experienced that; in 2007, Estonia also fell under massive cyberattacks that disrupted services on governmental servers [2]. Thanks to the lessons learnt in 2007, Estonia was prepared, and the recent attacks were ineffective. However, due to the attacks and extensive reliance on digital assets, cybersecurity has become a national priority. Estonia has been implementing solutions that could ensure digital continuity, protect critical data and ensure that government services are always available. For that, Estonia enhanced the protection of critical data. However, considering the geopolitical situation and previous experience with cyberattacks in Estonia, taking additional measures and mitigating risks was necessary. That is where the idea of backing up important information and databases outside Estonia while having complete control appeared as a solution. The idea developed into the data embassy initiative. Data Embassy is a cloud extension of the Estonian Government that involves server resources owned by the state outside its territorial boundaries. The data stored in the data embassy is secured against cyberattacks or crises and is under Estonia's control. In addition to providing a backup, the data embassy can operate Estonian e-services in case of crisis [3].

Estonia has developed and opened the world's first data embassy in Luxembourg. The need to have a data embassy is not only justified by the attacks in 2007; in today's context, the ongoing war, recent cyberattacks, and potential electricity outages [4] threaten the digital continuity of an e-country. Having a backup server outside of Estonia in the form of a data embassy is putting Estonia in a more secure position. Besides, the security and availability of digital services are essential for uninterrupted e-residency programme support [5]. In 2021 Estonia announced its plan to open an additional data embassy in a different location [5], which indicates its need and importance. Moreover, several

countries, such as Monaco, Bahrain, and India, have expressed interest in the Estonian data embassy and are incorporating the concept into their digital context. Therefore, the data embassy initiative is a timely and innovative measure that significantly ensures digital continuity. Furthermore, having a comprehensive understanding of the concept and its essential aspects can be a helpful tool for fostering cyber resilience in other countries.

The data embassy initiative is a novel case in international law, being the first bilateral agreement that expands the Vienna Convention on Diplomatic Relations. It is also novel regarding technical solutions and opportunities because setting up a data embassy required designing an unprecedented way of synchronising data in two sites [6]. Additionally, the novelty reflects in the limited amount of available information. While the number of relevant academic sources has been growing and expanding theoretical understanding, the practical side of the data embassy remains unexplored or undisclosed to the public. The data embassy in Luxembourg has been operating since 2018, and, therefore, it is a valuable learning case that could be used by other countries looking for cyber resilience and digital continuity-ensuring solutions.

The thesis intends to research the initiative of a data embassy and its role in Estonia's cyber resilience. The research focuses on the data embassy opened in Luxembourg, as currently, it is the only operating Estonian data embassy. The thesis investigates the factors that determined the location of the named embassy and examines its effectiveness. Additionally, the study seeks to propose a framework that would be helpful for other countries interested in implementing data embassies.

In order to meet posed aims, the thesis sets the following research questions and corresponding sub-questions:

RQ1: How does the data embassy contribute to Estonia's cyber resilience?

> **SQ1:** How is the data embassy related to Estonia's cybersecurity strategy?

RQ2: How does Estonia determine the criteria and factors for selecting an external host country for its data embassy?

> **SQ1:** What factors were considered for Estonia to establish a data embassy in Luxembourg?

SQ2: What is the current status of Estonia's data embassy in Luxembourg?

SQ3: What countries are being considered for future Estonian data embassies?

RQ3: How can countries make informed decisions about establishing their data embassies abroad by using Estonia's model?

SQ1: What countries consider implementing a data embassy concept for cyber resilience?

SQ2: What factors should those countries consider when implementing data embassies?

SQ3: What is the future evolution of data embassies?

The aims are being reached using a case study approach and data triangulation for an in-depth understanding. The theoretical framework is centred around the concept of cyber resilience, specifically on a national level.

With Chapter 1 as the introduction, Chapter 2 of this paper examines and reviews relevant literature and presents a theoretical framework. It then goes on to explain the methodology of the research in detail in Chapter 3. Chapter 4 is concerned with describing the results of the study and finding from conducted interviews. Chapter 5 discusses the findings and connects the outcomes with the goals of this research. Lastly, chapter 6 concludes the thesis, analyses limitations, and suggests future work.

2 Theoretical framework

The following chapter introduces the theory and key concepts used as the framework for the thesis. First, it describes the situation in cyberspace and shows the importance of cyber resilience these days. It is followed by a definition of cyber resilience and a national perspective, with Estonia as the example. The last part of the theoretical framework presents Estonia's approach to reinforce cyber resilience and the tools to ensure it.

2.1 Cyber resilience

The advancement of technology and increased use of digital systems have brought many benefits but also new challenges for protecting against cyberattacks and maintaining the confidentiality, integrity and availability of these services. As interconnected systems become increasingly complex, vulnerabilities can be unintentionally created, exposing organisations to negative consequences. The annual report by the Estonian Information System Authority indicates that the number of cyberattacks against Estonia has increased. In 2022, there were 27,115 reports registered in Estonia, where 2,672 of them were incidents with an adverse impact. In perspective, attack volumes were often more than a hundred times greater than in 2007 following the monument's removal honouring the Bronze Soldier. Yet, Estonia is not the only country experiencing cyberattacks. According to the report, 2022 was a restless year in international cyberspace [7]. Various countries faced attacks against national systems, e-services, and public sector agencies. In Albania, a cyberattack led to the websites, the computer systems of the police, and the e-services of state agencies being offline for hours. Montenegro experienced attacks that affected the provision of critical services, including transport and water services. Ransomware attacks targeted at Costa Rica put the country in a state of emergency, and due to unpaid ransoms, the services of the Ministry of Finance, the General Customs Administration, the General Tax Administration, the Social Security Fund, and several other agencies were disrupted even one month after the attack. In Belgium, a cyberattack targeted the local Government and, as a result, disrupted city services, such as police, residents,

schools, nursing homes, and kindergartens [7]. These are only a few examples of cyberattacks in 2022, which means that today countries are becoming more vulnerable in cyberspace. Strengthening cybersecurity, preparing for unexpected attacks, and ensuring the ability to respond is becoming crucial for the state's security.

To tackle the issues and make digital assets more protected, the European Union authorities started negotiating a Cyber Resilience Act [7]. Additionally, there are now more guidelines for protecting critical infrastructures, including the NIST (National Institute of Standards and Technology) framework created by the United States. These guidelines prioritise cyber resilience, which is especially important as cyberattacks frequently target critical sectors [8]. Therefore, in recent years, cyber resilience is becoming one of the focus areas in cybersecurity. Understanding and implementing the cyber resilience concept is essential for ensuring the digital continuity of a country.

Resilience is a concept that draws from multiple fields, such as ecology, sociology, psychology, organisational behaviour, and engineering and encompasses a range of perspectives and meanings [9]. However, in terms of cyberspace, the National Academies of Science (NAS) defines cyber resilience as "the ability to prepare and plan for, absorb, recover from, and more successfully adapt to adverse events", as cited in Linkov.

Cybersecurity and cyber resilience are often used together, but cyber resilience is a more comprehensive concept. Conklin and Shoemaker [10] explain that cybersecurity aims to prevent attacks on all areas of an organisation, respond to any identified compromise, and protect against all potential threats to maintain the organisation's security. On the other hand, cyber resilience focuses on creating a security framework that ensures an organisation's core operations can function continuously and efficiently, even during a security breach or disruption. Cyber resilience is similar to locking only an organisation's most valuable assets in a safe rather than trying to protect the entire organisation. As a result, cyber resilience aims to provide comprehensive defence and recovery systems against internal and external threats while maintaining operational continuity. Implementing cybersecurity and cyber resilience together is crucial in creating a secure organisation since both approaches collaborate more effectively [10].

Despite its relative newness, several strategies have emerged for building a cyber-resilient organisation. These strategies involve altering enterprise architecture to increase resilience, typically focusing on the assessment process. The primary goal is to evaluate the enterprise's current architecture, enhance its resiliency, and understand its ability to minimise the negative impact of incidents while recovering fully within an acceptable timeframe. This approach is intended to be a gradual and strategic development process that integrates necessary capabilities into existing enterprise processes over time in a planned and rational manner. Cyber-resilience operates on the premise that the system will eventually be breached. Therefore, it establishes a robust framework of procedures and checks to safeguard the critical subset of operations necessary for the organisation to function continuously, even in a compromise of other system activities. The cyber-resilience process also outlines clear and practical approaches to restoring any lower-priority functions that may have been impacted by the breach [10].

Organisations must focus on several dimensions to achieve cyber resilience, including governance and control environment. Governance involves setting up structures and processes, developing policies and frameworks, and ensuring efficient process management. When an organisation adheres to internationally recognised frameworks, it is considered to have high governance standards. The control environment comprises prevention, detection, response, and recovery controls. These controls can be implemented at different levels of maturity. For example, protection controls secure the company's network by implementing a multi-step process for access. Detection controls help identify attacks promptly, while response controls involve technical and non-technical measures such as separating affected assets, blocking attacks, and making assets unavailable. Recovery controls also play a crucial role in restoring after an attack [11].

Resilience in an organisational system is the capability to proactively and effectively manage potential hazards by making necessary adjustments to its processes, actions, and systems. That ensures that the organisation can successfully carry out its core functions despite external factors [12, 13].

2.1.1 National cyber resilience

Cyber resilience is most linked to businesses and organisations; however, it is also essential on the governmental level, mainly if the country relies on its digital

infrastructure. In “Building national cyber resilience and protecting critical information infrastructure”, Heli Tiirmaa-Klaar argues that building cyber resilience is a matter that should be discussed on a national level. It is crucial to have a national cyber policy and a team consisting of civil servants from cyber incident response, CIIP (Critical Information Infrastructure Protection) and cybercrime areas, top civil servants, interior and justice ministries, diplomats, the defence community, research and education policymakers, trade and industrial policy officials [14], which means that cyber resilience is not only a concern of the cybersecurity domain. It is a broad concept that requires a complex approach with relevant experts.

A well-coordinated and built national cyber policy consisting of cyber incident response, fighting cybercrime and protecting critical information infrastructure are vital components of national cyber resilience. Safeguarding the critical cyber assets of a nation is a fundamental aspect of its cyber initiatives. Policymakers responsible for enhancing their country's cybersecurity framework now face the challenge of defining and securing critical information infrastructure, which has evolved from a physical infrastructure-focused approach to a more service-oriented approach. An essential step for building national cyber resilience is determining what services are critical to a given country, as they vary. One of the simplest ways to determine those is to focus on the services on which people are the most dependent, including energy, telecommunications, transport, finance, public health, and public administration. Once the critical services are determined, it is essential to identify the companies and public sector organisations that offer the services listed as critical [14].

Analysis of various national models for CIIP or cybersecurity in Europe has revealed some patterns that may be transferable to other regions. Early success in establishing a functional CIIP system has been observed in medium-sized or smaller European countries. The "small-country model" relies heavily on solid trust relationships within homogenous societies. A core group of critical companies and national cyber organisations have developed technical cyber information exchange and early warning systems with critical operators. As the system matures, a full-time CIIP organisation with policy functions is established as a national coordinator overseeing and advising essential companies and organisations. In addition, the CIIP organisation informs higher-level policymakers, provides training, prepares national cyber exercises, and collaborates with key government agencies. Ideally, this organisation should be co-located with a national

incident response structure to ensure technical cyber competence and access to operational cybersecurity information. In Europe, the prevailing trend in national cyber efforts involves establishing a robust governmental institution with secure funding and strong political leadership at its core. Since the national CIIP organisation is expected to involve numerous public and private sector stakeholders, it can benefit from being associated with a national institution with direct access to senior political decision-makers and sufficient authority to oversee operations [14].

2.1.2 Cyber Resilience in Estonia

Several points can be highlighted by looking at cyber resilience in Estonia from the perspective introduced by Heli Tiirmaa-Klaar in an earlier discussion about national cyber resilience. First, the fact that Estonia has a national cybersecurity strategy refers to Estonia's understanding that cyber resilience is a matter discussed nationally. Cybersecurity is an essential national policy focus, and Estonia has a dedicated national cybersecurity strategy that reflects current issues and proposes solutions. The strategy's objective is to make Estonia a sustainable digital society with solid technological resilience capable of coping with crises. The strategy's primary focus is to protect essential operations and services from cyberattacks. To succeed, it focuses on tackling essential issues and preparing for future trends through a national strategy and cooperation that promotes interoperability [15].

The Cybersecurity Strategy of Estonia results from cooperation between national institutions such as the Government Office, Ministry of Defence, Ministry of Economic Affairs and Communications, Ministry of Interior, Ministry of Justice, Ministry of Foreign Affairs, and Ministry of Education and Research. In order to coordinate the objectives of the Cybersecurity Strategy, the ministries involved in implementation, along with the Government Office, appoint a responsible official. This individual handles matters related to national cybersecurity within their jurisdiction and ensures that the priorities outlined in the Cybersecurity Strategy are included in the respective ministry's planning documents. They also prepare an annual progress report made in implementing these priorities for the cybersecurity council. The Ministry of Economic Affairs and Communications is responsible for organising cooperation and information exchange between the appointed officials [15]. Another significant effort in promoting cybersecurity in Estonia is the establishment of CERT-EE (Computer Emergency

Response Team Estonia) in 2006. CERT-EE is responsible for managing security incidents in computer networks within Estonia and serves as a national contact point for international cooperation in IT security. In addition, they provide support to Estonian Internet users in implementing preventive measures to minimize the potential damage caused by security incidents and help them respond to security threats effectively. CERT-EE's main focus is on security incidents that occur in Estonian networks, originate from there, or are reported by citizens or institutions in Estonia or abroad. Their primary goal is to safeguard Estonia's computer networks against cyberattacks and ensure users receive timely and appropriate assistance during a security breach [16]. In other words, Estonia has a team dedicated to building and ensuring cybersecurity and taking care of the most critical infrastructure, similar to what has been described by Tiirmaa-Klaar, 2016 [14].

In terms of defining the most critical services in Estonia, databases containing vital information about citizens, the state's territory, and legislative drafting are considered the most significant digital assets requiring protection. Those include the Land Register, Commercial Register and Population Register. The updating of the list takes place regularly. The unauthorised modification or destruction of critical data could hinder the state's ability to fulfil its responsibilities [15]

Cybersecurity and national cyber resilience play an important role in Estonia’s agenda, which is reflected in the steps made by the governmental institutions. However, maintaining a high level of security for every government institution is not feasible due to the substantial investment required. To address this issue cost-effectively, a potential solution is to move critical databases and essential e-services to the Government Cloud and establish data embassies beyond Estonian territory. Such a solution enables the access of applications and databases, ensuring the high availability of critical services, even in situations where Estonia’s data centres become inoperable. Implementing the Government Cloud and data embassy solutions will likely mitigate the risks associated with the unauthorised modification or destruction of critical data while facilitating remote critical services [15]. The following part of the thesis explores the concept of data embassies in greater detail.

2.2 Estonian Government Cloud

The Estonian Government Cloud is a modernisation and renewal solution that allows for more agility in providing e-services by government agencies and critical service providers to residents and e-residents. The data between private and public institutions are exchanged through a secure data exchange layer X-Road [17]. The system integrates the existing IT infrastructure of the public sector into a shared pool of resources while complying with national IT Security Standards for safety and quality. The Government gradually transitions from legacy systems to the new Government Cloud solution, which is planned to be deployed in two locations, including one outside the capital, to accommodate physical security requirements and manage data and information systems in a distributed manner. To ensure the uninterrupted operation of public IT services and digital independence, the Government has established the data embassy initiative as part of the plan, along with the Government Cloud [18].

2.3 Data Embassy

Estonia's approach to ensuring cyber resilience includes the implementation of the Government Cloud and data embassies. However, the thesis focuses on the data embassies initiative. In "Concept of Estonian Government Cloud and Data Embassies", Taavi Kotka and Innar Liiv give a thorough overview and explanation of the idea behind data embassies. They argue that it is important for Estonia to have a server infrastructure entirely under the control of the Estonian Government, even if it is outside the country's borders. In addition, it is important to have protocols for backing up important data and applications to ensure that services can be restored in case of disruption. It is especially essential for registries like the State Gazette - containing all Estonian legislation - to have a real-time, updated copy that meets legal requirements. It is particularly crucial when the government loses control of data centres in Estonia or if a crisis or emergency renders it impossible to operate the State Gazette application within the country [19].

In the process of conceptualising data embassies, two options were evaluated. The first option involved utilising Estonian embassies abroad as backup facilities for critical data and registries since they are already established outside Estonia. This approach would entail providing the necessary technical resources to enable embassies to store backups, mirroring, regular data, and application backups and perform service operations. In

addition, the transition to this model with a weekly backup schedule would offer several advantages over the conventional method of quarterly or twice-annual backups, including keeping information up-to-date and ensuring digital continuity. Nevertheless, embassies may lack the technical expertise to maintain the infrastructure and respond effectively in a crisis and may not be capable of safeguarding themselves from cyberattacks. Additionally, they may not have control over their telecommunications services, which is a crucial consideration in the event of an attack [19].

The Data Embassy was seen as an alternative option to enhance Estonia's data storage and backup capabilities. The idea entails securing resources through bilateral agreements with friendly states' Government Clouds. This approach involves signing a treaty between Estonia and the host country, allowing Estonia to rent a dedicated space in an existing data centre that meets the necessary standards. The leased space would be physically isolated, fitted with security devices, and placed under Estonian jurisdiction. Compared to constructing server rooms within physical embassies, the Data Embassy concept offers several advantages, including meeting dedicated data centre standards, employing professional staff trained to safeguard service availability during emergencies and cyberattacks, and aligning with the legal agreements [19].

The initiative of the data embassy encompasses three significant elements that contribute to the continuity and uninterrupted operation of Estonia's e-government services. These include maintaining data backups and live services within the country's borders, keeping backups at physical Estonian embassy locations or dedicated data centres in allied countries designated by the Government, and maintaining backups of non-sensitive data in public cloud services provided by private companies. These three components provide additional security measures that guarantee smooth governance and service operation in a physical or cyber emergency. Initially, Estonia aimed to establish data centres and backup facilities within its boundaries to support its e-government services as part of its government-run cloud infrastructure. However, to achieve digital continuity, it is essential to guarantee that the authorised version of government services, such as the State Gazette, remains accessible and updatable in real-time and under all circumstances. Therefore, the Physical Data Embassy aspect of the initiative utilises a server resource that is entirely under the Estonian Government's control while being physically located outside the country's borders. As a result, two approaches were formulated to establish

the Physical Data Embassy. The first approach involves leveraging cloud computing solutions developed by Estonia's closest allies. In addition, the Government could sign bilateral agreements to access dedicated data centres in allied countries [20].

The second approach of the data embassy initiative proposes using established Estonian embassies to store backups for registries, leveraging their diplomatic status to extend Estonia's jurisdiction to e-government services and provide the same protections as physical embassies, consulates, or ambassadorial residences. By converting server rooms in physical embassies into data embassies, Estonia can establish a network that ensures digital continuity, even in the face of determined efforts to disrupt or take it offline. The third component of the initiative is the Virtual Data Embassy Solution, which aims to enhance digital continuity using commercial cloud computing [20].

While Virtual Data Embassies could offer higher availability, hosting specific data or services, such as state secrets, in privately-owned cloud services may raise concerns about data protection, privacy, and data integrity. However, public clouds can mitigate some of these risks, as they can handle the most widespread cyberattacks. Moreover, their location outside Estonia's physical borders and within the global cloud environment makes public clouds suitable for achieving the digital continuity objectives of the Virtual Data Embassy Solution [20].

According to the original plan, the Data Embassy network would be established in three locations, two in Europe and one outside. Among these, two locations would require the construction of new server rooms within Estonian embassies. In contrast, the third location would entail securing space for Estonia in the Government Cloud of a friendly nation [19].

3 Methodology

The thesis uses a case study approach that allows looking into the matter of data embassies in depth. It helps to determine the main characteristics and important aspects that support further topic development. The case study has exploratory, explanatory and descriptive elements. The research implements data triangulation when examining the case. According to Wilson, data triangulation refers to “using more than one particular approach when researching to get richer, fuller data and/or to help confirm the research results" [21, p. 66]. Starting with academic literature helps build a solid theoretical framework for cyber resilience, leading to a better understanding of data embassies. Due to the limited available scholarly works on data embassies, the sources include news releases and official government statements regarding data embassies in Estonia and abroad. In order to meet posed aims, the thesis set the research questions and sub-questions presented in Introduction.

When the thesis moves on from the example of Estonia to examine data embassies initiated by other countries, all available information about similar solutions found with the help of search engines was of use. A semi-structured interview was conducted to gather information about the data embassy initiative and its essential factors. Most interviewees participated in developing the concept of data embassies and establishing the data embassy in Luxembourg, who, therefore, could share valuable insights. One interviewee is currently working on a data embassies initiative in the Ministry of Foreign Affairs. In order to get an academic perspective, one interview was conducted with a researcher focusing on the data embassy. The interviewee affiliations are presented in Table 1. In total, five interviews were conducted. The semi-structured interview consisted of 14 questions that are presented in Appendix 2. All interviews were conducted online via Microsoft Teams and recorded upon the consent of participants, as well as transcribed using the transcription feature on Microsoft Teams. That was followed by manual proofreading and correcting to get a clear, edited text.

Table 1. Interviewee Affiliations.

Interviewee	Data Embassy role
A	Former CTO and chief architect of Estonia
B	Former CIO of the Estonian Government
C	Legal Architect of Estonian Data Embassy
D	An employee of the Ministry of Foreign Affairs working on data embassies
E	Data Embassy expert

Once the interview transcripts were ready, a thematic analysis was implemented. Thematic analysis is a qualitative approach that helps to identify, analyse, and report patterns within a data corpus, as defined by Scharp and Sanders [22]. The use of thematic analysis in this study allows for a detailed exploration of participants' experiences and perspectives, providing a rich source of data for addressing the research questions set by the thesis. The analysis is done following a six-steps method introduced by Braun and Clarke [22, 23]:

1. becoming familiar with the data
2. generating coding categories
3. generating themes
4. reviewing themes
5. defining and naming themes

6. locating exemplars

The transcripts were reviewed several times to become familiar with the data and uncover initial ideas and concepts. After the initial data familiarisation stage, a coding framework was developed, which involved identifying significant phrases, words or sentences within the data and assigning descriptive codes. These codes were organised into categories, and categories were then refined and organised into themes that captured broader patterns within the data. Next, the themes were reviewed and refined through an iterative process until the final themes accurately represented the data and addressed the research questions. Once the themes and corresponding keywords were determined, it was organised into thematic maps on each theme using the software tool “Diagrams.net”. The thematic maps are presented as figures in the section Thematic Analysis.

4 Results

The chapter below introduces the results of data collection and semi-structured interviews presented in thematic analysis. The first subchapter describes the data embassy in Luxembourg in greater detail, including the current status based on the publicly available information. The following subchapter focuses on examples of implementing data embassy initiatives in other countries, such as Monaco, Bahrain, India and Ukraine. Finally, the last subchapter presents the results of the thematic analysis.

4.1 Data Embassy in Luxembourg

E-Estonia's introduction states that the Data Embassy is an innovative concept where the Estonian Government extends its cloud infrastructure beyond its borders by owning server resources abroad. This contrasts with traditional methods, where states store information within their physical boundaries. The Data Embassy is secured using KSI Blockchain technology, a globally utilised blockchain technology that ensures the integrity of networks, systems, and data while maintaining complete data privacy [24]. The KSI blockchain technology enables the cryptographic verification of the accuracy of data and information transmitted through networks and systems [25]. It protects against cyberattacks and crises. It can provide backups of data and critical services and is located in a Tier IV data centre in Luxembourg. Although not functioning as a typical embassy, the Data Embassy is granted immunity rights similar to physical embassies under the Vienna Convention on Diplomatic Relations. It is entirely under Estonian control [26].

The world's first Data Embassy was established by Estonia in Luxembourg, with the project beginning in 2015 and an agreement signed between the two countries in 2017. Since 2018, Estonia's 'cloud' extension has been housed in LuxConnect's certified Tier IV data centre [26].

The development of the solution involved a collaborative effort from various stakeholders such as the Ministry of Economic Affairs and Communication, the State Information System Authority, the Ministry of Education and Research, the Centre of Registers and Information Systems, the Information Technology Centre of the Ministry of Finance, the

Land Board, the IT and Development Centre of the Ministry of the Interior, the National Archives, the Ministry of Foreign Affairs, the Ministry of Social Affairs, the Data Protection Inspectorate, the Estonian e-Health Foundation, the Police and Border Guard Board, the Estonian Internal Security Service, and the National Library [27]. In addition, from the private sector, companies such as Cybernetica, Dell EMC, Ericsson, OpenNode, and Telia also participated in the collaboration [26].

In total, the data embassy in Luxembourg hosts ten datasets [3]:

- e-file
- treasury information system
- e-land registry
- taxable person's registry
- business registry
- population registry
- State Gazette
- identity documents registry
- land cadastral registry
- national pension insurance registry

4.1.1 The current situation with the data embassy

Publicly, there has not been any recent information or updates about the data embassy in Luxembourg. However, the data embassy is mentioned in Estonia's Digital Agenda 2030, and according to the information, the embassy has been established. However, its current functionality is limited and needs further development [28]. In 2021 the Government announced that it plans to open another data embassy outside of Europe [6]. The lack of information about current status of data embassy in Luxembourg is covered by findings from the semi-structured interviews in the section 4.3.7.

4.2 Implementing the concept of data embassies in other countries

Since Estonia opened the data embassy in Luxembourg in 2018 [26], several countries increasingly find the embassy framework appealing. As mentioned in the theoretical part of the thesis, critical services are becoming the main targets of cyberattacks. Meanwhile, countries are also becoming more reliant on the digital infrastructure that comes with digitalisation. That is why Governments seek solutions to address cyber resilience related concerns. Estonia, having the title of the most advanced digital society in the world [29], appears to be a trustworthy example to learn from. E-embassy, digital embassy, and the virtual embassy are used as synonyms for data embassy in the initiatives of other countries. In the following subchapters, several cases of implementation of data embassies will be examined using the examples of Monaco, Bahrain, India and Ukraine. Currently, these are the only publicly known cases.

4.2.1 Monaco

Monaco has established a data embassy in Luxembourg to protect its sensitive data from cyber threats and natural disasters. This initiative, inspired by Estonia's data embassy, was led by Frédéric Genta, a member of the Monaco Government responsible for digital affairs and country transformation, and took two and a half years to finalise. The data embassy aims to ensure the sovereignty of Monaco's national digital data by providing the same level of inviolability and immunity as a physical embassy. Similar arrangements have been made between Luxembourg and NATO, the European Commission, and Estonia [29]. Monaco perceives data embassies as facilities that store duplicate copies of a nation's highly sensitive and confidential data or digital replicas of its cloud. With the increasing occurrence of cyberattacks, e-embassies are developed to protect essential data and services for a country's smooth functioning, minimising the potential effects of a cyberattack. In other words, Luxembourg is trusted to host the digital twin version of Monaco's Government Cloud [30].

Before establishing the data embassy, Monaco first set up a "sovereign cloud" Monaco cloud. The Chief Digital Officer of Monaco, Frédéric Genta, introduced the idea of the Monegasque sovereign cloud, built on the cutting-edge technology of Amazon Web Services (AWS) and would serve as the foundation for developing and introducing novel digital services in Monaco. AI is gaining importance in smart cities, e-health, e-education,

and e-government and Monaco can benefit from AI's processing power and storage capacity in the cloud, especially with its expected role in the economy [31]. AWS was also the cloud provider selected for the data embassy in Luxembourg. Monaco and Estonia have their data embassies in the same data centre LuxConnect, located in Bissen [30].

4.2.2 Bahrain

In 2018, Bahrain introduced new legislation allowing foreign entities to store their data in data centres located in Bahrain, referred to as a "data embassy." This move aligns with Bahrain's goal of becoming a hub for cloud computing and blurs national borders and sovereignty concerning data storage regulations. Implementing this legislation is innovative because it enables individuals to store their data in Bahrain's data centres while ensuring that their data is governed by domestic data protection laws of their country of residence [32].

In the same year, Bahrain passed the Cloud Law, which aims to provide a legal framework encouraging foreign parties to invest in cloud computing services. As per Article 3 of the law, if overseas consumers of cloud services store data in data centres in Bahrain, the domestic laws of the foreign state where the consumer resides will apply to their data. This means that courts and competent authorities of the foreign state will have jurisdiction over any disputes that may arise between the overseas consumer and the domestic service provider in Bahrain. The service provider must inform the Attorney General in writing when they receive an order from a foreign court or competent public authority and must provide a copy. Bahrain's competent judge and Attorney General can enforce any executable order that concerns matters relating to providing access, disclosure, preserving, or maintaining the integrity of customer contents [32].

It should be noted that a data localisation or data residency law requires that data about country's citizens or residents must be collected, processed, and stored within that country. Therefore, businesses operating on the Internet must keep and process data within the country's borders.

4.2.3 India

In early 2023, Finance Minister of India Nirmala Sitharaman announced that the Government would set up data embassies to enable digital transfers and continuity for other countries [33]. According to senior lawmakers, a new policy may be announced soon to allow governments and corporations to establish "data embassies" within India. These embassies would provide "diplomatic immunity" from local, national and commercial digital data regulations. The policy may be introduced as part of the Digital Data Protection Bill, which is expected to be presented in March. The interest from India might be explained by the idea that the approval of "data embassies" could encourage more technology infrastructure investment in India. Moreover, Rajeev Chandrasekhar, the Minister of State for Electronics and IT, says this initiative is part of a larger strategy to establish a dependable data storage ecosystem in India. One potential solution to address concerns raised by data centre companies and cloud service providers about the updated Digital Personal Data Protection Bill [34] is to introduce "data embassies" for data storage and cross-border data flows.

4.2.4 Ukraine

The eruption of armed conflict between Russia and Ukraine on February 24, 2022, has left Ukraine in a hazardous position, calling for safeguarding its national infrastructure and databases [35]. In March of the same year, the Ukrainian Government announced its preparedness to relocate its data and servers overseas, should the need arise. Initially, officials began the physical transportation of servers and removable storage devices, as well as the digital migration of data from one server to another, to more secure areas within the country. However, the Government also considered moving its digital assets abroad for added security. Victor Zhora, the deputy chief of Ukraine's State Service of Special Communications and Information Protection, noted that several countries have offered to host the data, although their names were not disclosed. Zhora believes that the Government prefers European locations. If data is to be moved out of Ukraine, it can only happen with the approval of Ukrainian lawmakers and the establishment a protocol for removing digital assets. The plan does not involve the complete relocation of the Government's data abroad. Instead, Ukrainian agencies would make decisions on a case-by-case basis regarding which data should be relocated [35].

According to Stupp, as of June 2022, Ukraine had already begun storing some of its sensitive state data abroad, including 150 registers from various government institutions or their backup copies [36]. Before, the Ukrainian Government stored their data in local data centres. They needed to move the information to a cloud platform to create backup copies. It was possible thanks to legal and security provisions specified by the Government. Storing national databases on the cloud provides security to Ukraine, as the government can still access essential data from an external centre if the local data centre is destroyed, as stated by George Dubinskiy, Ukraine's deputy minister of digital transformation. The Government prioritised the transfer of "VIP" databases, including those supporting the economy, digital identification, and tax data. As the conflict continues, the Government monitors the data that should be listed as sensitive or risky [36]

As reported in the news, Ukraine currently stores some of its governmental data in a private cloud in Poland. The server hosts only Ukrainian data; all other details regarding this topic are confidential. Poland is the first location, and Ukraine is working on implementing similar arrangements with other countries, including Estonia and France [36].

In a recent report outlining the defence strategy of Ukraine's information environment, it has been disclosed that Ukraine collaborated closely with prominent technology firms such as Microsoft, Amazon Web Services, and Google to transfer its information infrastructure to the cloud [37]. The mentioned companies assisted in relocating critical government data to infrastructures hosted outside of Ukraine in data centres throughout Europe. Through its cloud services, Microsoft ensures that Ukrainian government agencies, critical infrastructure, and other sectors can operate seamlessly and serve the needs of its citizens. Similarly, Amazon and Google provide cloud services to selected firms and humanitarian organisations in Ukraine [37].

The examples of Bahrain, Monaco, India and Ukraine show that the concept of a data embassy can be interpreted in various ways depending on the goals and needs of the country. In general, it indicates that such a solution is needed in today's society, and it can be useful for various countries.

4.3 Thematic analysis

The following section presents a thematic analysis of the interviews conducted for this thesis. The interviews provide valuable insights into the aspects of the concept of a data embassy. The chapter explores the interview themes and offers a comprehensive overview of the findings. Through an in-depth examination of the collected data, the chapter aims to provide a deeper understanding of the research questions. In total, thematic analysis detected 11 themes presented in the following sections. As it is shown in Table 1, each interviewee was assigned a unique letter. The given letters are also used for referring to a specific interview throughout the thematic analysis.

4.3.1 Contribution to cyber resilience

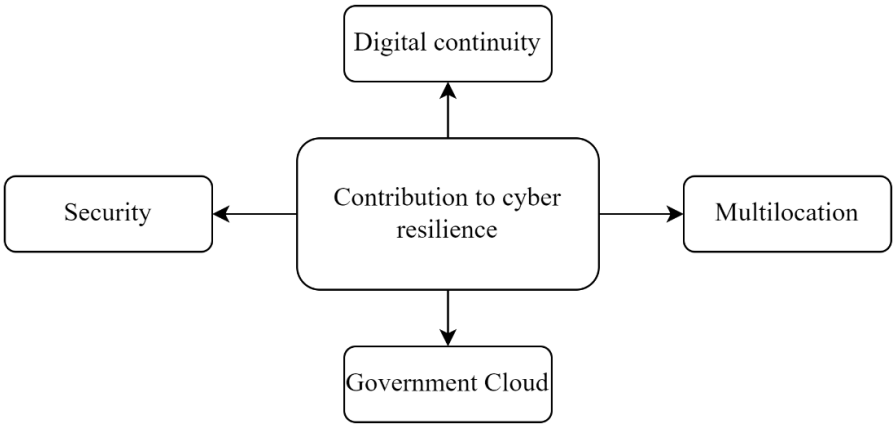

Figure 1. Theme "Contribution to cyber resilience".

Figure 1 shows the first theme that emerged from the interviews, and it explains how the data embassy initiative contributes to cyber resilience. Based on the interview, implementing the data embassy concept significantly contributes to a country's cyber resilience. In the case of Estonia, it is a necessary step for ensuring national cyber resilience and digital continuity (C). The digital assets of a country are like a key that, if stolen, could lead to significant disruptions. Similarly, if all critical registries are physically stored inside the country and get taken away, they can be misused, such as for false voting (B).

The concept of a data embassy is based on the fact that it is a network, and the data is not stored in one location (B). Thanks to the multilocation factor, the data embassy helps to mitigate or, at the very least, distribute the risk of losing critical data (C). The solution is resilient thanks to the fact that it is an extension of the Government Cloud (D), which already makes sure that the data is stored securely.

According to standard (A), the network of embassies must be set within 250 kilometres from the primary location. However, setting up a data centre on the eastern border of Estonia is unsuitable due to national security interests. On the other hand, on the western side there are islands like Saaremaa and Hiiumaa, and setting up a data centre on an island is not a convenient location infrastructure-wise (E). Distance is not the only lacking aspect in Estonia. There are no data centres with Tier IV security, which is crucial for storing sensitive national data (D). The data embassy makes Estonia resilient by covering the missing aspects and ensuring that if something happens on the territory of Estonia, Estonia can still restore the data and continue as usual (D). It is a way to protect information and services and ensure that the country always retains its integrity (E).

4.3.2 Alternative solutions

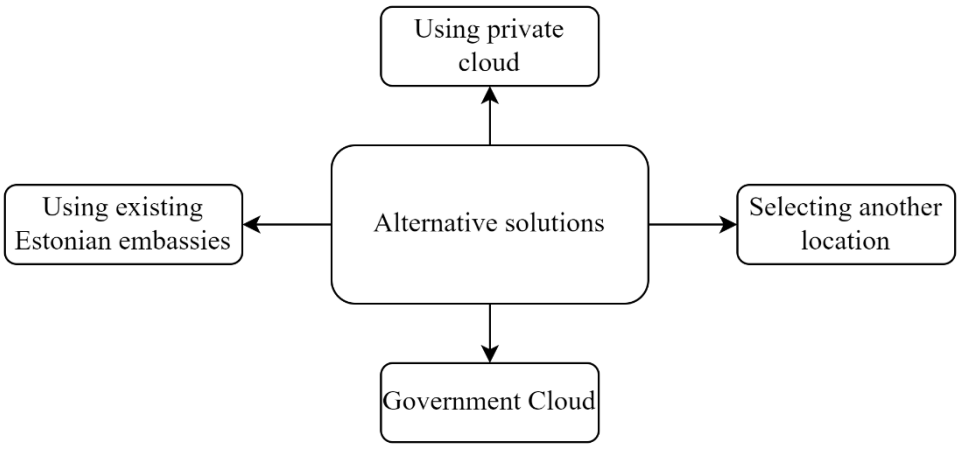

Figure 2. Theme "Alternative solutions".

Figure 2 presents alternatives that have been considered before establishing a data embassy. Since 2005, Estonia has developed a system to back up important data and store it in different locations. For example, Estonia’s registries and databases were initially

backed up to hard drives and delivered to various Estonian embassies worldwide using diplomatic bags (E). The data embassy concept is an advancement of this process, which is more efficient and secure.

One alternative solution is storing the information in private or public clouds like Amazon or Azure. However, considering the importance and sensitivity of the data, these options cannot be used as ownership over data could be used as a tool and lead to potential manipulation by larger countries, leaving Estonia in a vulnerable state (B). Other than that, no other alternatives that would serve the purpose of a data embassy have been discussed nor considered (A, C, D). Other hosting countries were initially considered, with the United Kingdom being the first intended location. However, technical and bureaucratic complications were slowing down the process, and as result, the project did not go through (E). Other considered partners cannot be disclosed due to security reasons (B).

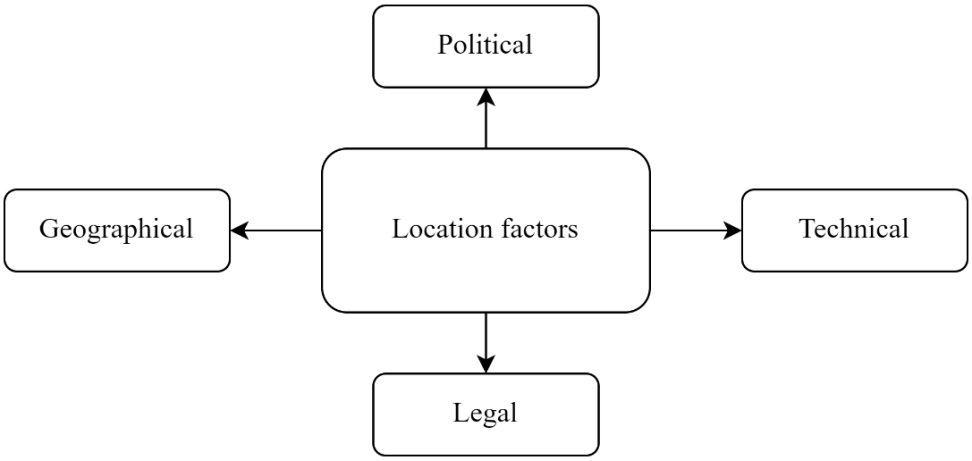

Figure 3. Theme "Location factors".

4.3.3 Location factors

Figure 3 shows the main factors that play a role in selecting a host country for data embassy. The selecting process requires a complex approach involving several important factors (A, B, C, D, E). One of the essential considerations is political aspects, as the host country must be friendly (A, C, D) and have a good and trustworthy relationship with the embassy's country of origin (B). Additionally, the two nations should share membership

in international organisations such as the EU and NATO (D, E) and have strong diplomatic ties (E).

Technical factors also play a crucial role in determining the ideal host country. The chosen location must have robust connectivity and excellent internet infrastructure (B, C, E) and possess the appropriate technological infrastructure, including high-level IV Tier data centres that ensure maximum security for stored data. Moreover, the host country should have a government-owned data centre, or at least majority of the data centre should be owned the Government (D). Therefore, the host country must have a data centre meeting these requirements.

Geographical factors also need to be considered while selecting a suitable location in terms of multilocation. The backup site should not be located too close to Estonia, with aligning with a standard of 250 kilometres distance (A). Otherwise, it does not pose any use, because if an emergency happens in Estonia, it will also likely occur in the area close to Estonia (E). The safety of the territory and susceptibility to political conflicts or natural disasters are among the key aspects that need to be evaluated (E).

Finally, several legal factors must be considered when choosing the host country for a data embassy. The selected location must be open to building a mutual understanding in legal terms (A, D), and, therefore, the potential country must undergo a process of due diligence (E). Choosing the perfect host country for a data embassy is a complex process involving political, technical, geographical, and legal factors.

4.3.4 Risks

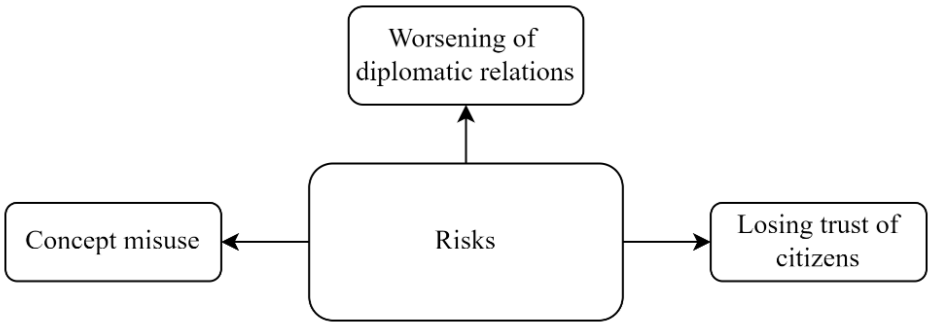

Figure 4. Theme "Risks".

Figure 4 illustrates keywords associated with risks that establishing a data embassy comes with. Most risks are linked to the misunderstanding of the concept and overreliance. There is a risk of viewing the data embassy as a backup, which might lead to overreliance (A). The backup only in one location does not serve as much (B) as the concept relies on the multilocation factor. Besides, storing data in another country can be risky as the relationship between countries can worsen unexpectedly (D). It is crucial to remember that in case of emergency, the consequences of issues with registries and data are more significant than monetary losses in other industries, in a bank, for instance (A). The data about citizens is not measured by monetary value, there are fundamental values associated with a trust between the Government and its citizens, and the trust should never be lost (D). Therefore, handling citizens' data, which is Estonia's most valuable digital asset, should be careful and justified.

4.3.5 Challenges

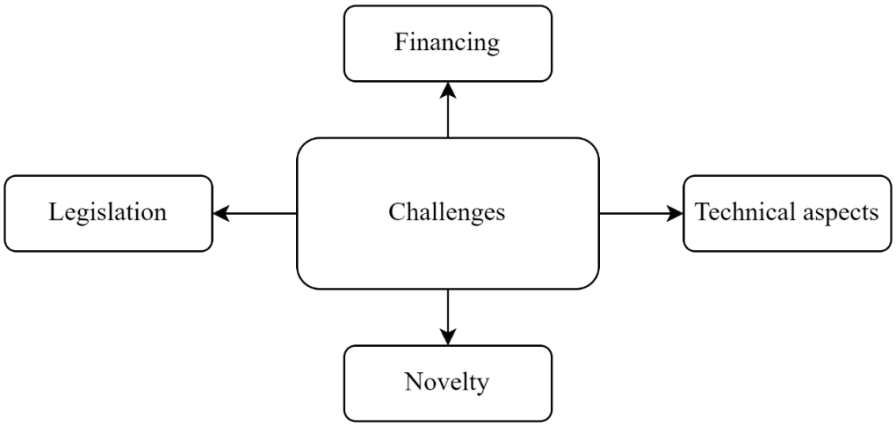

Figure 5. Theme "Challenges".

The establishment of a data embassy also involves several challenges, as presented in Figure 5. The project's main challenge is planning and establishing its legal foundation (A, B, C, D, E). As this is a new concept that has not been implemented before Estonia, preparing the legal side of the project was difficult and time-consuming (D). It was unclear if international legal agreements, such as the Vienna Convention, would be applicable (D, E). Since this project requires substantial investment (D), sustaining its financing may be burdensome (E). The constant evolution of technology presents a long-term risk and challenge as such initiatives must adapt to societal changes (C). In Estonia,

the newness of the concept posed a challenge that caused delays in the project. Being a pioneer in the concept meant the project had to be built from scratch (A, B).

4.3.6 Expectations for the data embassy in Luxembourg

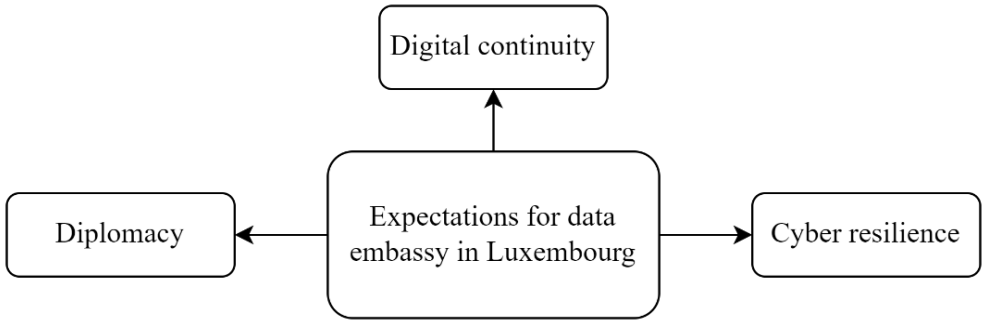

Figure 6. Theme "Expectations for data embassy in Luxembourg".

Figure 6 shows the expectations of policymakers for the data embassy in Luxembourg. As previously mentioned, the data embassy initiative is a novel concept launched with a "let us test it" mindset. Therefore, it was intended to serve as a test on multiple levels: firstly, to determine if it works legally and allows for copying and backing up data. Additionally, it aimed to assess whether this concept enables live data sharing and live data storing from Luxembourg, making it possible to switch between Estonia and Luxembourg (D).

Estonia had certain expectations for the project, including the volume of computing power and finding trusted partners (B). It was expected that if there was a risk or threat on Estonian territory, the data embassy would be activated in another location, and everything would continue to work as usual (C). From a national security perspective, the data embassy was expected to ensure digital continuity by replicating systems and services within another country and enabling a smooth operation outside of Estonian borders (E). Additionally, the data embassy was initiated to serve diplomacy-building purposes (E).

Are the mentioned expectations met? The existence of a data embassy is justified (C), and it is an actual technical mechanism of backup that works and functions (A). The Estonian

policymakers are satisfied with the service, as the presented needs are being delivered (A, B). Estonia and Luxembourg see the initiative as good and valuable and wish to continue cooperation on this project (D).

Since its official opening in 2018, the data embassy in Luxembourg has been operating as a unique solution to ensure the continuity and resilience of Estonia's critical digital infrastructure. Despite its success as a backup mechanism, the operation has brought a deeper understanding of technical limitations and areas for improvement. The current procedure for collecting and transferring data is not yet ideal, so there is a continued effort to refine the process (B). Initially, the contract was signed for five years, and as of the beginning of 2023, it has been extended (C, D). The concept of a data embassy is still evolvig and being tested to improve its effectiveness and efficiency (D).

4.3.7 Current status of data embassy in Luxembourg

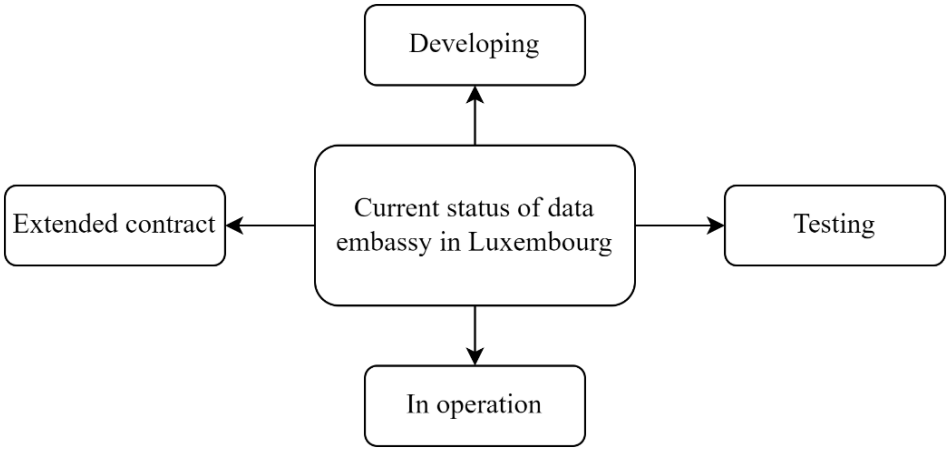

Figure 7. Theme "Current status of data embassy in Luxembourg".

As the concept of data embassy continues to develop, questions arise about its effectiveness in ensuring the continuity and resilience of critical digital infrastructure. Figure 7 introduces insights into the current status. Measuring the effectiveness of the data embassy is a challenging task, as it serves as a risk mitigation measure. As it has been noted, "You cannot really measure this because fundamentally it is a risk mitigation measure, and the only way you can measure this is when you have an active crisis" (A). The data embassy is an insurance policy, and its value may only become apparent during a crisis, such as a cyberattack or natural disaster that affects Estonia's digital infrastructure. The fact that Estonia has not experienced a significant digital crisis since

the establishment of the data embassy in 2018 can be seen as a positive sign of its effectiveness (A). Also, it has been only five years since the launch, and currently, there is only one data embassy, so discussing the effectiveness of the concept is relatively early (C). However, the data embassy is a working mechanism for backing up and storing data outside the border – the copies of critical data sets are in Luxembourg and are frequently tested (A). If something were to happen, Estonia would be ready to tackle it with the help of the data embassy in Luxembourg (C). The war in Ukraine highlights the importance of having tools that ensure the state's cyber resilience and digital continuity (C).

The data embassy initiative also has some secondary outcomes. For instance, the novelty of the initiative has given Estonia a high level of visibility (A, C). Estonia has opened a conversation about the legal significance of data sets, which positively contributes to the digitalising society. The data embassy works for the Estonian Government as a brand, bringing attention to the country through this kind of visibility (E). Overall, looking at the measurable aspects of the effectiveness of the data embassy, the initiative is proving itself to be effective. Ongoing talks about selecting the following location indicate that the project shows a positive outcome (E).

4.3.8 The next location

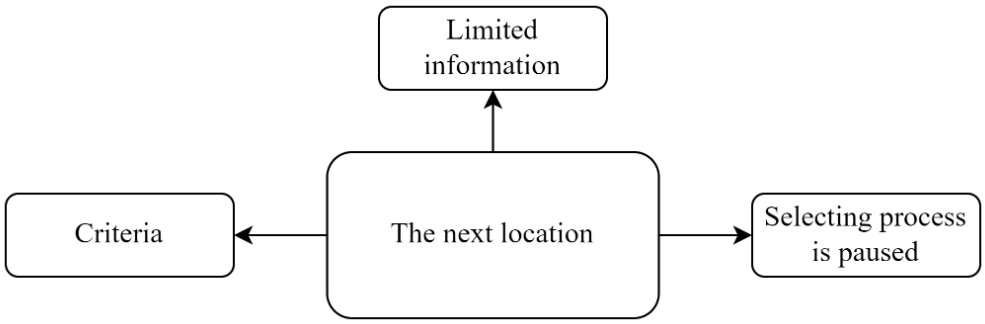

Figure 8. Theme "The next location".

The theme about next potential location is discussed in Figure 8. Information about the following potential location of the data embassy is limited. None of the interviewees has information about the next country (A, B, C, D, E) – the location has not been selected yet, and the selection process has been paused due to undisclosed reason (C). However,

all interviewees are aware of the plan to open more data embassies in other locations. In principle, opening additional data embassies is seen as a good, justified idea (A). According to the plan to set up a data embassy network, the following location should be outside Europe to test whether the concept would work in a different geopolitical environment (E).

4.3.9 Important aspects of the data embassy initiative

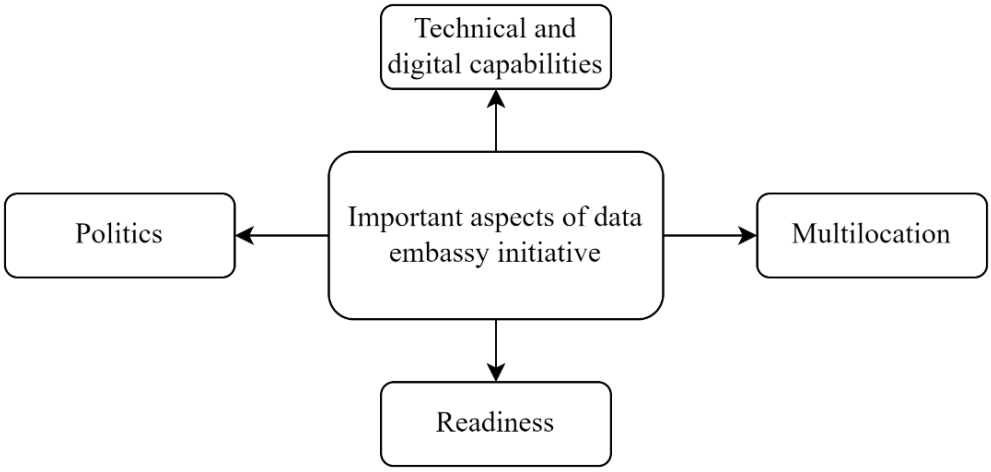

Figure 9. Theme "Important aspects of data embassy initiative".

As more countries recognise the importance of digital sovereignty and the need to protect their critical data, the idea of a data embassy has gained interest from several countries. However, opening a data embassy requires careful consideration of various aspects that are summarised in Figure 9. Firstly, the technical capabilities of the information system must be capable and mature enough to handle the embassy's data (A). Multilocation is also very important, and the legal procedures must support having embassies in several locations. Preparing the legal ground for the project might be the most challenging part compared to the technical side (A, B). Finally, the countries should assess and understand their needs and capabilities (C).

Additionally, the readiness of the country's system to start using that type of service should be evaluated (D). It is worth noting that the maturity of Estonian systems compared to some other countries might be different (D), hence a thorough evaluation of the political and technical aspects should be conducted before proceeding (C). It is important to have a clear understanding of the objectives set for the project since the justification of

the need for opening a data embassy involves substantial investments (D). The key is to have a robust technological infrastructure within the country, with sufficient government-operated data centres in the host country (E). Therefore, selecting a suitable country is essential (E) for the reasons mentioned in the section describing location-determining factors.

4.3.10 Evolution of data embassies

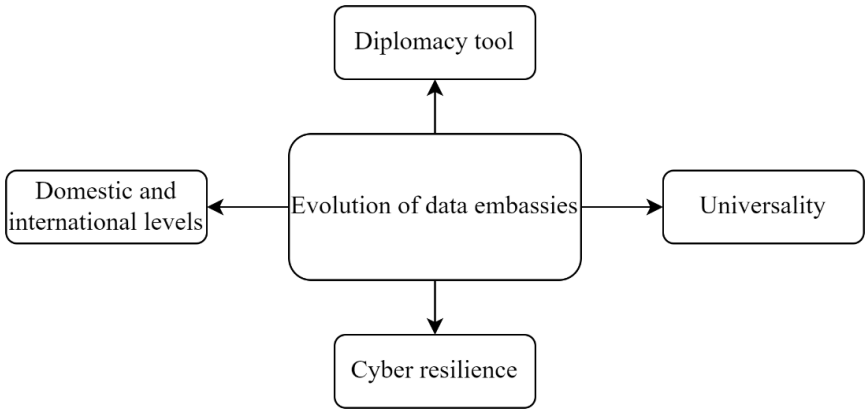

Figure 10. Theme "Evolution of data embassies".

Over the years, data embassies have evolved from a pioneering concept introduced by Estonia to a practical solution for countries seeking to ensure the security and availability of their data abroad. The future of this concept is multifaceted and varies for Estonia and other countries. The theme about evolution of data embassies is presented in Figure 10. For example, one development line for Estonia involves operating live data sets, which would require live backups and storage in constant synchronisation. However, current capabilities do not allow this, and technical improvements are needed to achieve this plan (A).

At the international level, data embassies could become a universal tool that enhances countries' cyber resilience by operating data embassies at each other's locations worldwide (A). The concept raises important questions, such as whether a country can survive when its physical location is occupied or destroyed. Data embassies may be a solution for people to organise themselves as a country without a physical location (B) and for countries struggling with international legitimacy, such as Palestine (E). Countries

that face geographical constraints and conflicts may use data embassies to demonstrate their legitimacy to the international community (E). Data embassies will continue to enhance diplomatic relations between countries, leading to economic benefits (E).

To ensure that the concept is universally accepted and legally recognized under the Vienna Convention, the initiative must be taken to the international level (D). This would prevent confusion and any legal questions that may arise.

Developing data embassies can boost national resilience and provide tangible benefits for states (E). By having secure backups of critical data in multiple locations, countries can reduce the impact of disasters and maintain critical services in case of significant disruptions (A, B, C, E). This is particularly important for small countries with limited resources and capabilities for managing cyber threats and other risks. In addition, data embassies can provide a cost-effective solution for securing critical data and ensuring it is available when needed (E).

Overall, the evolution of data embassies represents a positive step towards enhancing cyber resilience and protecting national security. As more countries adopt this approach, continued cybersecurity improvements and excellent protection against emerging threats can be expected.

4.3.11 Lessons from Estonia

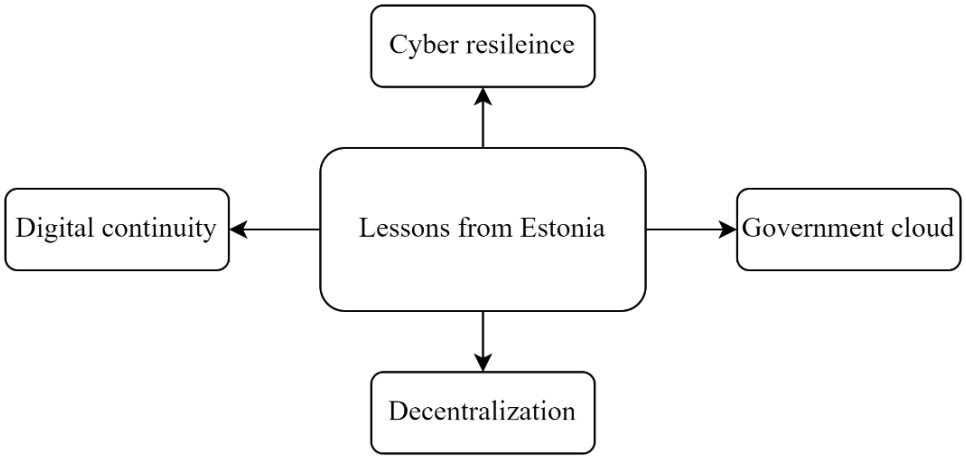

Figure 11. Theme "Lessons from Estonia".

Estonia's experience developing data embassies and other innovative solutions for ensuring digital continuity can serve as a model for other countries striving to boost their cyber resilience. Figure 11 summarises important lessons that could be taken away from

the experience of Estonia. If a country trusts its critical data to a public cloud or a private company, it comes with a loss of sovereignty over data (A). If a country is digitally in a similar position as Estonia, it is worth considering copying the concept of a data embassy (B). The political situation in the world can often be unpredictable, and if "collapse cannot be avoided", it is important to be prepared and ready to restore critical information such as birth, ownership, and property registries once independence is regained (B). The legal side tends to be the most challenging; once the legal part is clear, "there is nothing complicated" (B). Since experiencing cyberattacks in 2007, Estonia has valued the digital society's security, which has been building up keeping resiliency, safety, and security considerations (C). Another critical aspect is decentralisation (C, D, E), which is explained in section 5.3.

In order to implement the data embassy concept, the countries themselves should be in a good place in terms of their cyber resilience and ICT systems infrastructure that should interact with each other. In contrast, the data embassy is an extra layer that can make the country more secure but will not solve internal problems alone (D). Therefore, using the governmental cloud is the foundation for implementing the initiative. The awareness of cyber threats is also essential since attacks are getting more advanced at the same time that technologies are developing (D).

5 Discussion

Based on the thesis findings, including a thematic analysis of the interviews, a framework for implementing a Data Embassy is suggested. The proposed framework serves as a guideline for countries interested in implementing a data embassy based on the experience of Estonia (Figure 12).

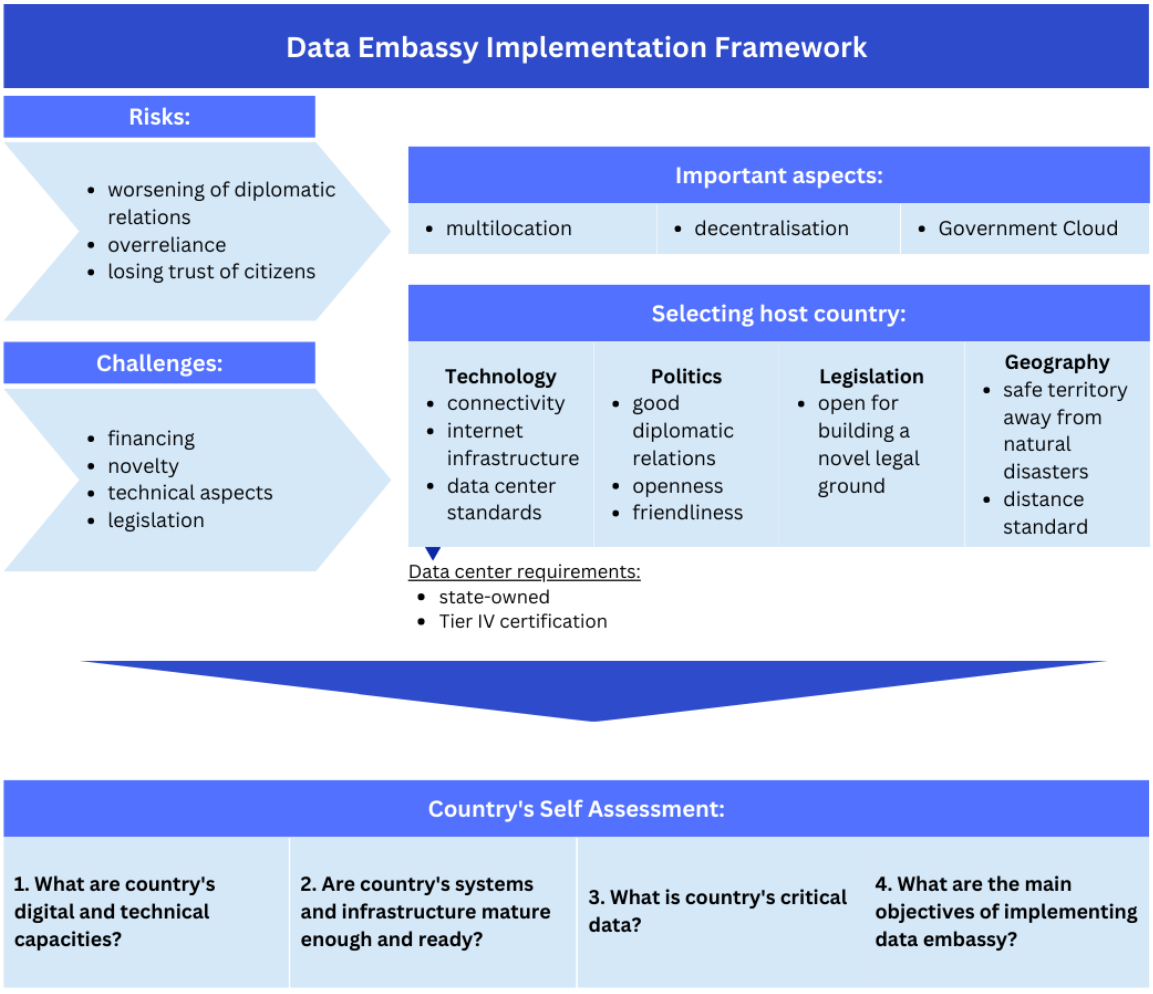

Figure 12. Data Embassy Implementation Framework.

The framework includes risks, challenges and important aspects that countries should consider. As selecting a suitable partner for hosting a data embassy is one of the fundamental things of successful implementation, the framework brings out the main factors that play a role in selecting the location. Lastly, after presenting the core aspects

of data embassy implementation, the framework suggests some questions that help a country assess its readiness or need for adapting such an initiative. The present chapter reviews components of the framework in greater detail as well as links findings with the research questions of the thesis.

5.1 Data embassy's contribution to Estonia's cyber resilience

The first question in this study sought to determine how the data embassy concept contributes to Estonia's cyber resilience. As a part of Estonia's cybersecurity strategy, the data embassy has been identified as a crucial tool for achieving cyber resilience. Estonia, heavily reliant on its digital infrastructure and e-services, faces risks and challenges related to its national security and sustainability. Any damage to critical data could jeopardise the functioning of Estonian society by making the provision of essential e-services impossible. The Estonian Government has recognised such risks and proactively works towards mitigating them. Investment in solutions that ensure digital continuity is essential for the long-term success of E-Estonia. The data embassy contributes to this objective by storing critical data in the Government Cloud and distributing it to multiple locations as well as provides the availability and accessibility of the vital e-services in crisis. This approach allows Estonia to identify vulnerabilities and develop continuous solutions to mitigate the impact of any compromising event.

As highlighted in the theoretical framework, Linkov and Kott [9] define "cyber resilience" as the ability to successfully prepare for, absorb, recover from, and adapt to adverse events. Due to historical, geographic, political, and technical reasons, Estonia is vulnerable to cyberattacks, military actions, natural disasters, and electricity outages. While it is impossible to predict when or if such events may occur, the country can anticipate them and implement risk mitigation solutions. Estonia can adapt to the situation and recover from a disaster by leveraging its cyber resilience measures.

5.2 Determining criteria and factors for selecting an external host country for data embassy

The third question in this research was about evaluating how Estonia determines the criteria and factors for selecting an external host country for its data embassy. Choosing a location plays a vital role in the implementation of the concept. The selection process

includes political, technical, legal, and geographical factors. Estonia placed its data embassy in Luxemburg because it satisfied the set criteria. The following sections reviews Luxembourg according to the mentioned factors.

5.2.1 Politics

Luxembourg is a politically stable country. Even though the Grand Duchy lost the status of a neutral state, peace is being secured through unity, it is a founding member of all post-war multilateral cooperation institutions such as The United Nations and UNESCO, the Benelux, the Organisation for European Economic Cooperation (OEEC), the Council of Europe, the North Atlantic Treaty Organisation (NATO), the Organisation for Economic Cooperation and Development (OECD) [38]. Luxembourg is one of three European capitals, along with Brussels and Strasbourg, that have hosted many EU institutions since 1952, including the Secretariat General of the European Parliament, the Court of Justice, the European Investment Bank, various units of the European Commission, the European Court of Auditors, the Publications Office, and others [39].

Estonia and Luxembourg have been diplomatically tied since 1923, when Luxembourg recognised the Republic of Estonia. The relations were not consistent; however, it was renewed in 1991 with re-recognition of Estonia by Luxembourg [41]. Throughout the years, the governments mutually considered each other as reliable partners and role models in many areas, including economy [42] and digitalisation [43]. For instance, when Estonia was making efforts to join the Eurozone, Luxembourg expressed its support and approval [44]. According to the Ministry of Foreign Affairs of Estonia, relations between Luxembourg and Estonia are good, which is expressed in bilateral cooperation in areas such as defence, digitalisation and cybersecurity [45]. For Estonia Luxembourg is a trusted reliable partner thanks to membership in mutual organisations and active cooperation in multiple areas.

5.2.2 Technology

Luxembourg was also a good fit from a technical perspective. As mentioned, Luxembourg has high-level data centres qualifying for IV Tier standards. The Uptime Institute's Tier Standards are well-respected globally for evaluating the reliability and performance of data centres, covering physical infrastructure and operations team competency and processes. Each tier classification has specific design and performance

requirements. The Tier Certification confirms that a data centre has been built, designed, and operated in accordance with these standards, and is widely recognized as a mark of excellence. This rigorous program takes into account individual and corporate needs, component performance, and impartial on-site assessments. Data centres that undergo the Tier Certification process can be awarded one of four classifications, ranging from Tier I to Tier IV, based on the criteria outlined in the Uptime Tier Standards. Table 2 [40] represents the classification of the tiers. These standards are comprehensive and stringent, and their impartiality is widely recognised in the industry. Uptime Institute has issued over 2,500 certifications in over 110 countries, including Luxembourg [40].

Table 2. Uptime Institute Tier Classification System [40].

Tier I	**Tier II**	**Tier III**	**Tier IV**
Basic Capacity	**Redundant Capacity Components**	**Concurrently Maintainable**	**Fault Tolerant**
Site-wide shutdowns are required for maintenance or repair work. In addition, capacity or distribution failures will impact the site.	Site-wide shutdowns for maintenance are still required. Capacity failures may impact the site. Distribution failures will impact the site.	Every site's capacity component and distribution path can be removed and planned for maintenance or replacement without impacting operations. However, the site is still exposed to equipment failure or operator error.	An individual equipment failure or distribution path interruption will not impact operations. A Fault Tolerant site is also Concurrently Maintainable.

As mentioned in the description of the data embassy in Luxembourg, the data centre hosting Estonian data is LuxConnect. According to the information on the website [41], LuxConnect is a leading ICT and data centre operator in Luxembourg, providing high-quality data centre services to customers in various industries. LuxConnect is a private

company owned by Luxembourg state, which also meets the requirement set by Estonia. The company operates four state-of-the-art data centres in the country, offering secure and reliable hosting solutions to businesses of all sizes. LuxConnect's data centres are built to meet the highest availability, security, and energy efficiency standards. They have advanced technologies and infrastructure, such as redundant power and cooling systems, advanced fire detection and suppression systems, and physical security measures. Customers can choose from network providers for their connectivity needs since the facilities feature carrier-neutral connectivity. Apart from data centre services, LuxConnect provides various other ICT services, including cloud computing, managed hosting, and IT consulting. The company collaborates with its clients closely to comprehend their specific requirements and develop tailor-made solutions to meet their needs. Also, it is brought out that the location is outside a natural disaster risk zone. Overall, LuxConnect is a trusted and reliable provider of data centre and ICT services in Luxembourg, offering world-class facilities and expertise to help businesses operate and grow in the digital age [41]. Looking at the technical capacities Luxembourg offers proves that it is an excellent technical partner.

5.2.3 Legislation

Preparing the legal ground is considered to be one of the most challenging parts of setting up a data embassy; part of that is finding a cooperation partner willing to provide necessary legal frameworks and guarantees for safeguarding critical data.

The explanatory document by the Government of Estonia described the process of developing the solution. On September 3, 2015, the Estonian Government approved the concept of the state cloud and its implementation plan, which included the establishment of a "Data Embassy." On November 14, 2016, the Estonian Minister of Economic Affairs and Infrastructure and Luxembourg's Minister of Media and Communications signed a Memorandum of Understanding to begin negotiations to establish the first "Data Embassy." On June 15, 2017, the Estonian Government approved the agreement between Estonia and Luxembourg on data and information systems hosting. On June 20, 2017, the Prime Ministers of Estonia and Luxembourg signed the agreement in Luxembourg. On October 8, 2017, the Estonian Minister of Entrepreneurship and Information Technology, and the Luxembourg Minister of Public Service and Administrative Reform, signed an

agreement to lease Luxembourg's national data centre. The confidential lease agreement outlines the terms and conditions of the services and assets provided and the financial obligations that come with them. Additionally, it describes the responsibilities of the parties involved and the technical requirements that the services must meet [27].

The bilateral agreement operates with the same principles as the Vienna Convention on Diplomatic Relations. It obligates both the "sending State" and "receiving State" to meet specific responsibilities and diplomatic safeguards associated with a regular embassy [42]. In legal terms, the Vienna Convention on Diplomatic Relations lays down the regulations for exchanging embassies between sovereign states. These regulations, which safeguard the security of diplomats and allow them to perform their duties, are the oldest and most essential principles of international law. The treaty is crucial to the modern global legal system [43].

5.2.4 Geography

The necessary multilocation principle also finds application in geographical requirements. Countries located very close to Estonia would not serve the purpose. The distance between Estonia and Luxembourg is 1,563 kilometres [44]. The distance is significantly over 250 kilometres, a standard followed by Estonia. The territory of the Great Duchy is not prone to natural disasters, and all neighbouring countries are allies who share the same international organisations, most importantly EU and NATO.

5.3 Update on the data embassy in Luxembourg and the next location

The data embassy in Luxembourg has been operating since 2018 and successfully completed the initial 5-year contract that was prolonged in 2023. As a vital component of Estonia's cybersecurity strategy, the data embassy serves as a working mitigation mechanism, which can support Estonia's critical e-services in case of a cyberattack or a natural disaster. Despite the effectiveness of the data embassy being challenging to measure in the absence of an actual crisis, the geopolitical situation near Estonia, including the Russian-Ukrainian war and the increased frequency of cyberattacks, justifies the operation of the data embassy. The data embassy was launched as a pilot project to test and detect the technical limitations and areas that require improvement. As of 2023, the policymakers of Estonia mostly focus on analysing and improving the existing data embassy, therefore the Government is not actively looking for a new partner.

The potential locations that have been considered for the next data embassy remain undisclosed due to the sensitivity of information. It is only known that the Government plans to test the concept in a different environment and for that goes outside of Europe. Still, the selection of next host country would follow the same considerations and steps as it was with Luxembourg.

5.4 Using Estonia's model to make informed decisions on establishing data embassies abroad

The third question was examining how countries could use Estonia's approach to establish their own data embassies overseas and make informed decisions. The novelty of the concept and its extensive benefits have sparked interest from countries that, as a result, reach out to Estonia and Luxembourg for cooperation. Currently, it is known that Monaco followed the example of Estonia and implemented the same solution in Luxembourg. Bahrain, India and Ukraine are also adapting and implementing the concept. Estonia and Luxembourg set an example for countries interested in hosting another country's data and those interested in storing their data elsewhere. Monaco, Bahrain, India, and Ukraine are countries that have been public about using the solution. Both Estonia and Luxembourg mention that many countries reach out for the inquires. However, those countries do not share such intentions with the public, which could be linked to national security concerns.

The countries that intend to implement the data embassy initiative should thoroughly understand the concept and why it has worked for Estonia. Pure copying of the concept may not be practical or may not work due to differences in technical and digital capabilities. For Estonia, the data embassy is only a part of the broad digital society infrastructure. Therefore, getting familiar with Estonian digital infrastructure in general, is crucial. As with the example of Monaco and Ukraine, before moving the data abroad, they first moved data to the cloud and only then proceeded with the transfer. Another vital aspect is decentralisation. The term refers to transferring control and decision-making from a centralised entity to a distributed network [45]. Decentralisation offers several benefits, including creating a trustless environment where no one has to know or trust anyone else, improving data reconciliation by having a decentralised data store, reducing

points of weakness in systems, and optimising the distribution of resources for better performance and consistency. In addition, it reduces the likelihood of failure [45].

In order to use the data embassy as a cyber resilience ensuring tool, the country needs to have a robust cybersecurity strategy and be technologically mature in terms of information systems. Moreover, financing, legislation, and technical challenges must be considered. Setting up a data embassy does not give a guarantee, and the risks that come with it should be evaluated beforehand. Before implementing a data embassy, a country should assess its digital and technical capacities, evaluate the maturity and readiness of systems and infrastructure, and determine critical national data and the objectives of implementing a data embassy.

5.5 The future of data embassies

The present study raises the possibility that data embassies could become a universal cyber resilience tool that helps to ensure the digital continuity of a country with a similar need or a profile like Estonia. In an interview with the Luxembourger Wort, Gilles Feith, the director of the Luxembourg government IT centre (CTIE), expressed that the data embassy concept would become normal within ten years [46]. Estonia will continue working on the data embassy in Luxembourg and improve current limitations and capacities. In the future, the pioneer of data embassies will expand the network.
In perspective, data embassies will continue evolving and contributing to cyber resilience and digital continuity of digital societies. On the international level it also means enhancement of diplomatic relations.

In an explanation about data centre certifications by Uptime University, it was mentioned that there are four tiers. Recently, American company Switch announced that it had developed a new data centre standard called Tier 5 Platinum, which goes beyond traditional fault tolerance to incorporate fault sustainability in design, implementation, and operation. This standard includes Switch's proprietary technologies and takes a holistic approach to ensure data centre integrity and reliability, addressing critical elements such as power and cooling systems, internet connectivity, carrier services, physical security, regional disaster risks, and energy efficiency. While the Uptime Institute does not certify data centres as Tier V, Switch's Tier 5 Platinum sets a new

benchmark for data centre excellence and guarantees fault sustainability and comprehensive protection [47]. In the future, the upgrade to Tier 5 could be used for developing technical aspects of data embassy solution and introduce new potential partners.

6 Conclusion

The present research aimed to examine the data embassy initiative and its contribution to the cyber resilience of Estonia on the example of the data embassy in Luxembourg. The research questions were focused on understanding the role of the data embassy in Estonia's cybersecurity strategy, the criteria and factors involved in selecting an external host country, and how other countries can adopt this model.

Through thematic analysis of interviews and literature review, this study has identified that the data embassy contributes significantly to Estonia's cyber resilience by ensuring the security and integrity of its critical data and systems. Estonia's criteria for selecting a host country include political, legal, geographical and technical factors.

This study proposes a Data Embassy Implementation Framework to assist other countries in making informed decisions about establishing their data embassies abroad. The framework addresses the risks, challenges, and important aspects to consider and includes assessment questions.

The study is subject to several limitations that should be considered when interpreting the results. Firstly, the lack of information on the current status of the data embassy in Luxembourg and the potential location of the next data embassy may have impacted the analysis. This limitation might be due to the sensitivity of the information and the potential risks associated with disclosing it, which could compromise national security.

Additionally, the study's results may not fully reflect the experiences and perspectives of establishing data embassies due to the small sample size of five interviews. This limitation could be attributed to the sensitivity of the information, causing current policymakers to refrain from commenting on the matter. Nevertheless, the five knowledgeable interviewees provided valuable insights. Among the interviewees, high-level officials were the core people at the time of developing and establishing the data embassy. Therefore, they are the most valuable source for an in-depth understanding of the initiative, which serves as a foundation of the Data Embassy Implementation Framework.

As the concept is still novel, it is natural that the number of involved people is limited, which is also reflected in the sample size.

Keeping mentioned limitations in mind, the findings of this study have several important implications for future practice. The Data Embassy Implementation Framework could be a valuable tool for countries interested in learning from the experience of Estonia and building their own data embassy.

More work will need to be done to determine the effectiveness of data embassies and their current application as a cyber resilience tool. Future research could focus on the experience of other counties that also implemented the initiative. It would help to understand another perspective in greater detail and serve as valuable input for developing the framework. Additionally, further work needs to be done to understand the perspective of the hosting country.

References

[1] ERR, "Estonia subjected to 'extensive' cyberattacks after moving Soviet monuments," 18 8 2022. [Online]. Available: https://news.err.ee/1608688201/estonia-subjected-to-extensive-cyberattacks-after-moving-soviet-monuments.

[2] R. Ottis, "Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective," *Proceedings of the 7th European Conference on Information Warfare and Security*, pp. 163-168, 2008.

[3] E-Estonia, "Data Embassy Factsheet," 2020. [Online]. Available: https://e-estonia.com/wp-content/uploads/2020mar-facts-a4-data-embassy.pdf.

[4] ERR, "Estonia subjected to 'extensive' cyberattacks after moving Soviet monuments," 2022. [Online]. Available: https://news.err.ee/1608688201/estonia-subjected-to-extensive-cyberattacks-after-moving-soviet-monuments. [Accessed 05 05 2023].

[5] OECD, "Establishing the first Data Embassy in the world," 2017. [Online]. Available: https://oecd-opsi.org/innovations/establishing-the-first-data-embassy-in-the-world/#:~:text=The%20Data%20Embassy%20is%20established. [Accessed 2 3 2023].

[6] ERR, "Estonia mulling new data embassy outside of Europe," 2021. [Online]. Available: https://news.err.ee/1608338096/estonia-mulling-new-data-embassy-outside-of-europe. [Accessed 3 10 2022].

[7] Republic of Estonia Information System Authority, Cyber Secuirty in Estonia 2023, Tallinn: Information System Authority, 2023.

[8] Y. Maleh and Y. Maleh, "National Cyber Resilience Strategy in a Post-COVID-19 World," *SpringerBriefs in Cybersecurity*, pp. 67-75, 2023.

[9] I. Linkov and A. Kott, "Fundamental Concepts of Cyber Resilience: Introduction and Overview," *Cyber Resilience of Systems and Networks*, pp. 1-25, 2018.

[10] W. A. Conklin and D. Shoemaker, "Cyber-Resilience: Seven Steps for Institutional Survival," *EDPACS*, vol. 55, no. 2, pp. 14-22, 2017.

[11] E. Tsen, R. K. L. Ko and S. Slapnicar, "An exploratory study of organizational cyber resilience, its precursors and outcomes," *Journal of Organizational Computing and Electronic Commerce*, pp. 1-22, 2022.

[12] R. van der Kleij and R. Leukfeldt, "Cyber Resilient Behavior: Integrating Human Behavioral Models and Resilience Engineering Capabilities into Cyber Security," *Advances in Intelligent Systems and Computing*, pp. 16-27, 2019.

[13] N. McDonald, "Organisational resilience and industrial risk," *Resilience Engineering*, p. 155–180, 2006.

[14] H. Tiirmaa-Klaar, "Building national cyber resilience and protecting critical information infrastructure," *Journal of Cyber Policy*, vol. 1, no. 1, pp. 94-106, 2016.

[15] Republic of Estonia Ministry of Economic Affairs and Communication, 2019-2022 Cybersecuirty Strategy Republic of Estonia, Tallinn: Ministry of Economic Affairs and Communication, 2019.

[16] Republic of Estonia Information Security Authority, "Republic of Estonia Information Security Authority," 2023. [Online]. Available: https://www.ria.ee/en. [Accessed 5 5 2023].

[17] E. B. Jackson, R. Dreyling and I. Pappel, "A Historical Analysis on Interoperability in Estonian Data Exchange Architecture: Perspectives from the Past and for the Future," *14th International Conference on Theory and Practice of Electronic Governance*, 2021.

[18] E-Estonia, "Government Cloud," [Online]. Available: https://e-estonia.com/solutions/e-governance/government-cloud/. [Accessed 21 4 2023].

[19] T. Kotka and I. Liiv, "Concept of Estonian Government Cloud and Data Embassies," in *Electronic Government and the Information Systems*, Springer, 2015.

[20] Republic of Estonia Ministry of Economic Affairs and Communication; Microsoft, "Implementation of the Virtual Data Embassy Solution - Summary Report of the Research Project on Public Cloud Usage for Government, Conducted by Estonian Ministry of Economic Affairs and Communications and Microsoft Corporation".

[21] T. C. Wilson, "Rethinking digital preservation: definitions, models, and requirements," *Digital Library Perspectives,* vol. 33, no. 2, pp. 128-136, 2017.

[22] K. M. Scharp and M. L. Sanders, "What is a theme? Teaching thematic analysis in qualitative communication research methods," *Communication Teacher,* vol. 33, no. 2, pp. 117-121, 2019.

[23] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative research in psychology,* vol. 3, no. 2, pp. 77-101, 2006.

[24] E-Estonia, "KSI Blockchain," [Online]. Available: https://e-estonia.com/solutions/cyber-security/ksi-blockchain/. [Accessed 30 4 2023].

[25] T. Liisi, "KSI blockchain provides truth over trust," Invest in Estonia, 2022. [Online]. Available: https://investinestonia.com/ksi-blockchain-provides-truth-over-trust/. [Accessed 30 4 2023].

[26] E-Estonia, "Data Embassy," [Online]. Available: https://e-estonia.com/solutions/e-governance/data-embassy/.

[27] The Government of Estonia, "Seletuskiri Eesti Vabariigi ja Luksemburgi Suurhertsogiriigi vahelise andmete ja infosüsteemide majutamise kokkuleppe ratifitseerimise seaduse eelnõu juurde," Riigikogu, Tallinn, 2013.

[28] The Ministry of Economic Affairs and Communications of Estonia, Estonia’s Digital Agenda 2030, Tallinn: The Ministry of Economic Affairs and Communications of Estonia, 2021.

[29] M. Reynolds, "Welcome to E-stonia, the world's most digitally advanced society," Wired, 2016. [Online]. Available: https://www.wired.co.uk/article/digital-estonia#:~:text=Estonia%20is%20the%20world's%20most%20digitally%20advanced%20society.. [Accessed 7 5 2023].

[30] T. Labro, "Monaco gets its Luxembourg data embassy," Delano , 2021. [Online]. Available: https://delano.lu/article/monaco-opens-itsluxembourg-dat. [Accessed 22 3 2023].

[31] C. Tanti, "Monaco establishes its first e-Embassy in Luxembourg," Monaco Life, 2021. [Online]. Available: https://monacolife.net/monaco-establishes-its-first-e-embassy-in-luxembourg/. [Accessed 23 3 2023].

[32] Extended Monaco, "Monaco Cloud, the Monegasque sovereign cloud set for launch in 2021," Extended Monaco, 2020. [Online]. Available: https://extendedmonaco.com/en/project/monaco-cloud-the-monegasque-sovereign-cloud-set-for-launch-in-2021/. [Accessed 15 4 2023].

[33] A. Tamimi, R. Fawcett, K. Jhala and H. Osman, "Diplomatic immunity for data: Bahrain's Data Embassy Law," Lexology, 2020. [Online]. Available: https://www.lexology.com/library/detail.aspx?g=1498c8dc-5902-4f90-8a87-9c7eea170998. [Accessed 23 3 2023].

[34] P. Yadav, "Budget 2023 | What are 'data embassies' that FM Sitharaman proposes to set up," CNBCTV18 , 2023. [Online]. Available: https://www.cnbctv18.com/technology/budget-2023-what-are-data-embassies-that-fm-sitharaman-proposes-to-set-up-15824141.htm. [Accessed 23 3 2023].

[35] R. Majumdar and S. Agarwal, "Govt may notify data embassy policy as part of new Data Bill," The Economic Times, 2023. [Online]. Available: https://economictimes.indiatimes.com/tech/technology/govt-may-notify-data-embassy-policy-as-part-of-new-data-bill/articleshow/97560396.cms. [Accessed 24 3 2023].

[36] R. Satter and J. Pearson, "Exclusive: Ukraine prepares potential move of sensitive data to another country - official," Reuters, 2022. [Online]. Available: https://www.reuters.com/world/europe/exclusive-ukraine-prepares-potential-move-sensitive-data-another-country-2022-03-09/. [Accessed 10 4 2023].

[37] C. Stupp, "Ukraine Has Begun Moving Sensitive Data Outside Its Borders," Wall Street Journal, 2022. [Online]. Available: https://www.wsj.com/articles/ukraine-has-begun-moving-sensitive-data-outside-its-borders-11655199002. [Accessed 15 4 2023].

[38] E. Schroeder and S. Dack, "A parallel terrain: Public-private defense of the Ukrainian information environment," Atlantic Council, 2023. [Online]. Available: https://www.atlanticcouncil.org/in-depth-research-reports/report/a-parallel-terrain-public-private-defense-of-the-ukrainian-information-environment/. [Accessed 14 4 2023].

[39] European Union, "Luxembourg," [Online]. Available: https://european-union.europa.eu/principles-countries-history/country-profiles/luxembourg_en. [Accessed 1 5 2023].

[40] Luxembourg, "The European institutions in Luxembourg," luxembourg.public.lu, 2023. [Online]. Available: https://luxembourg.public.lu/en/society-and-culture/international-openness/eu-institutions.html. [Accessed 1 5 2023].

[41] E. M. o. F. Affairs, "Estonia and Luxembourg," 2012. [Online]. Available: https://web.archive.org/web/20120511205238/http://www.vm.ee/?q=en/node/96. [Accessed 8 5 2023].

[42] R. o. E. Government, "Ansip: Luxemburg is a reliable partner and great role model for Estonia," 2011. [Online]. Available: https://valitsus.ee/en/news/ansip-luxemburg-reliable-partner-and-great-role-model-estonia. [Accessed 8 5 2023].

[43] R. o. E. Government, "Prime Minister Ratas: Estonia and Luxembourg are pioneers of digital cooperation," 2017. [Online]. Available: https://valitsus.ee/en/news/prime-minister-ratas-estonia-and-luxembourg-are-pioneers-digital-cooperation. [Accessed 8 5 2023].

[44] R. o. E. Government, "Luxembourg's Prime Minister Juncker supports Estonia's attempts to join the Eurozone," 2009. [Online]. Available: https://valitsus.ee/en/news/luxembourgs-prime-minister-juncker-supports-estonias-attempts-join-eurozone. [Accessed 8 5 2023].

[45] Välisministeerium, "Luksemburg," 2023. [Online]. Available: https://vm.ee/luksemburg. [Accessed 8 5 2023].

[46] Uptime Institute, "Tier Certification Overview," [Online]. Available: https://uptimeinstitute.com/tier-certification. [Accessed 5 5 2023].

[47] LuxConnect, "LuxConnect's Data Center," [Online]. Available: http://www.luxconnect.lu/infrastructure/. [Accessed 5 5 2023].

[48] N. Robinson, L. Kask and R. Krimmer, "The Estonian Data Embassy and the Applicability of the Vienna Convention," *International Conference on Theory and Practice of Electronic Governance*, 2019.

[49] E. Denza, Diplomatic law Commentary on the Vienna convention on diplomatic relations, Oxford Oxford University Press, 2018.

[50] Geodatos, "Distance between Estonia and Luxembourg," 2023. [Online]. Available: https://www.geodatos.net/en/distances/countries/from-estonia-to-luxembourg. [Accessed 26 4 2023].

[51] AWS, "What is Decentralization in Blockchain?," [Online]. Available: https://aws.amazon.com/blockchain/decentralization-in-blockchain/#:~:text=Decentralized%20networks%20strive%20to%20reduce,the%20functionality%20of%20the%20network..

[52] H. Pritchard, "Estonian data embassy in Luxembourg to cost €2.2m," Luxembourg Times, 2017. [Online]. Available: https://www.luxtimes.lu/en/luxembourg/estonian-data-embassy-in-luxembourg-to-cost-2-2m-602d0e11de135b9236c4d4e1. [Accessed 25 4 2023].

[53] Switch, "The World's Only Tier 5 Data Center Provider | Switch," Switch, [Online]. Available: https://www.switch.com/tier-5/. [Accessed 26 4 2023].

[54] L. S. Sterling, The Art of Agent-Oriented Modeling, London: The MIT Press, 2009.

[55] "E-embassies in Luxembourg," 2023. [Online]. Available: https://luxembourg.public.lu/en/invest/innovation/e-embassies-in-luxembourg.html.

Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis[1]

I Anna-Maria Kolessova

Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis "Estonia's data embassy initiative: a framework for building cyber resilience in other countries, supervised by Eric Blake Jackson

1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.

2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

08.05.2023

1 The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.

Appendix 2 – Interview Questions

1. What is your experience with Estonian data embassies?
2. One of the objectives of the Estonian cybersecurity strategy is to ensure that Estonia is a sustainable digital society with strong technological resilience and readiness to cope with crises. Implementing a network of data embassies is presented as one of the solutions. How does the concept of a data embassy contribute to a country's cyber resilience?
3. Were any other technical alternatives (besides the data embassy) considered when developing the solution to ensure digital continuity?
4. What are some of the key factors that should be considered when selecting a location for a data embassy?
5. What are some of the risks and challenges associated with establishing a data embassy?
6. What were the expectations for the data embassy in Luxembourg?
7. In your opinion, has the data embassy in Luxembourg met the expectations of policymakers?
8. How do the involved parties perceive the current effectiveness of the data embassy in Luxembourg?
9. According to the news, Estonia plans to open another data embassy in another location. What is the current status of this initiative?
10. What are the potential countries?
11. Following the experience of Estonia, Monaco opened a data embassy, and Bahrain and India are also working on a similar solution. Are there any important aspects to consider when implementing this kind of initiative?
12. How do you see the concept of data embassies evolving in the future?

13. What impact do you think it will have on cyber resilience?

14. What can other countries learn from Estonia in order to make their states cyber-resilient and ensure digital continuity?

Transcripts of conducted interviews are available upon request.