Tallinn University of Technology

School of Information Technologies

Department of Software Science

E-Governance Technologies and Services

The potential of the Estonian e-Governance infrastructure in supporting displaced Estonian residents in national emergencies

Master's Thesis

Student:	Lőrinc Thurnay
Student code:	145847IVGM
Supervisor:	Prof. Dr. Dirk Draheim
Co-Supervisor:	Benjamin Klasche, MA

Tallinn

2016

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: Lőrinc Thurnay

12.12.2016

Abstract

This thesis examines the possibilities of using the Estonian e-Governance infrastructure in new ways to help displaced Estonian residents in a hypothetical national emergency. After establishing the theoretical framework of the paper, I begin by exploring the challenges that displaced persons and aid organizations face throughout three key stages of displacement – flight from conflict zones, temporary displacement, and long term integration. The challenges identified will be the basis of analyzing how the Estonian e-Governance infrastructure could be used in a refugee emergency.

I continue by briefly introducing e-Governance in Estonia and by giving a definition of intangible e-Governance infrastructure. I identify the key component of the existing Estonian e-Governance infrastructure as well as the proposed Governmental Cloud and Data Embassy initiatives, and I point out their key features.

Once I identified the challenges of displaced persons and aid organizations, as well as the key features of the Estonian e-Governance infrastructure, I identify linkages where the infrastructure could potentially counter the challenges of displaced persons and aid organizations.

To realize these linkages, I conclude my work by proposing a policy to "make certain refugee-related, otherwise restricted governmental datasets accessible to international aid organizations" in case of national emergencies. I propose a legal framework for the policy, analyze the technological requirements of its implementation, and discuss its communicational and technology export-related implications.

This thesis is written in English and is 54 pages long, including six chapters and one figure.

Keywords

Data Embassy, displacement, e-Governance infrastructure, national emergency, policy recommendation, refugee, UNHCR

Annotatsioon (In Estonian)

Käesolev magistritöö uurib erinevaid võimalusi, kuidas uut moodi kasutada Eesti e-riigi infrastruktuuri võimekust, et aidata ümberasustatud Eesti residente hüpoteetilise riikliku hädaolukorra puhul. Pärast teoreetilise raamistiku loomist, alustab autor erinevate väljakutsete ning probleemide analüüsiga, millega ümberasustatud isikud ja abiorganisatsioonid kokku puutuvad. Analüüsitakse kolme peamise ümberpaigutamise etappi – põgenemine konfliktipiirkonnast, ajutine ümberpaigutamine ning pikaajaline integratsioon. Nimetatud väljakutsed on analüüsi aluseks, kuidas Eesti e-riigi infrastruktuuri võidakse pagulaste hädaolukorraga seoses kasutada.

Autor jätkab magistritööd Eesti e-valitsemise lühikirjeldusega, defineerides immateriaalse e-riigi infrastruktuuri. Autor selgitab Eesti e-valitsuse infrakstuktuuri põhikomponente ning rõhutab valitsuse esitatud pilve ja andmete saatkonna algatuste põhijooni.

Lisaks, kui autor on tuvastanud ümberasustatud isikute ja abiorganisatsioonide väljakutsed ja probleemid, samuti ka Eesti e-riigi infrastruktuuri põhijooned, analüüsib autor ka seoseid, kuidas infrastruktuur võiks ümberasustatud isikute ja abiorganisatsioonide osas abi osutada.

Et mõista neid seoseid, lõpetab autor magistritöö poliitilise ettepanekuga riiklikus hädaolukorras - teha vastavad pagulastega seotud, riiklikud andmebaasid kättesaadavaks ka rahvusvahelistele abiorganisatsioonidele. Autor teeb ettepaneku, milline võiks olla vastav strateegiline õiguslik raamistik, analüüsib ning soovitab tehnoloogilisi nõudeid selle rakendamiseks ning arutleb kommunikatsiooni ja tehnoloogia ekspordiga seotud mõjude üle.

Käesolev magistritöö on kirjutatud inglise keeles ning on 54 lehekülge pikk, sisaldades kuute peatükki ja ühte joonist.

Võtmesõnad

Andmete saatkond, ümberpaigutamine, e-riigi infrastruktuur, riiklik hädaolukord, poliitilised (strateegilised) soovitused, pagulased, UNHCR

Acknowledgements

I would like to express my sincere gratitude to my supervisors, professor Dirk Draheim and Benjamin Klasche for their guidance, patience and excellent ideas, to my classmates, Crystal LaGrone, Iana Nezdemovska, Maarja Pütsep, and Kedi Välba for their advices, encouragement, and for the laughs we shared, and to my friends and family for always supporting me.

Thank you!

List of abbreviations and terms

API	Application Protocol Interface
CCD COE	(NATO) Cooperative Cyber Defence Centre of Excellence
CERT	(Estonian) Computer Emergency Response Team
e-Citizen	Throughout this work the term *e-Citizen* is used to refer to people who hold a digital identification and profile: Estonian citizens, residents, and e-residents.
ICT	Information and communication technology
MKM	(Estonian) Ministry of Economic Affairs and Communications
NARE	Needs Assessment for Refugee Emergencies
NATO	North Atlantic Treaty Organization
PKI	Public key infrastructure
RIA	(Estonian) Information System Authority
UNHCR	United Nations High Commissioner for Refugees
WASH	Water, sanitation, hygiene

List of figures

Table of contents

1 Introduction

Estonia is considered to be a pioneering country in ICT and e-Governance solutions. In the last 25 years, Estonia introduced a number of unprecedented new technology-driven solutions in the public sector, such as Internet voting (Estonian National Electoral Committee, 2010), nation-wide digital signatures (Sertifitseerimiskeskus, 2003) and the e-Residency program (Shabbir, 2014). One of the most recent e-Governmental projects is the Data Embassy initiative, which – when finished – will guarantee that Estonia's heavily relied upon e-Governance services would remain functional even if the country's territorial integrity was breached (Kotka and Liiv, 2015).

The idea of the Data Embassy initiative is very intriguing. The unconditional continuous operation of e-Governance that it provides implies that a state does not necessarily cease to exist if it loses its powers and controls in the conventional sense of the words – it can continue to live on in an extended, digital form. But what would this mean in practice? What difference could a state make if it only existed in a virtual space? Surely, if a country's territorial integrity is breached, its government is forcefully overthrown, and its sovereignty has diminished, the last thing the country's citizens would be concerned about would be the vague concept of a "virtual state". Or would it?

Estonia has found so many interesting, novel ways to tackle problems with ICT and e-Governance that are typically not ICT-related problems. What if the virtual survival of a diminished state could be used to counter some of the many problems that its citizens will face in times of instability and danger?

It is thinking along these lines that lead me to the topic of displaced persons and e-Governance, and to the decision to write my thesis about the "potential of the Estonian e-Governance infrastructure in supporting displaced Estonian residents in national emergencies".

Throughout my studies in the e-Governance Technologies and Services program of the Tallinn University of Technology, I have been feeling encouraged to pursue ideas that lead off the beaten path. It is my impression that this mindset is a owned not only by the University; it is shared in the public sphere as well. Therefore I am excited to pursue this idea of examining the use of ICT in governance in the case of a national emergency – taking a look at e-Governance in the context of yet another problem, and seeing how it can be used in new ways to solve the problem.

1.1 Relevance

One of the goals of the Estonian government's ongoing government cloud and data embassy initiative is enabling the Estonian government agencies to operate even during a possible loss of control over the country's territory. Taavi Kotka (Deputy Secretary General for Communications and State Information Systems at the time), Laura Kask and Karoliina Raudsepp from the Estonian Ministry of Economic Affairs and Communication (MKM) write: "The [Data Embassy] Initiative consists of additional security measures that would allow Estonia to ensure continuity in government and operations, including […] core government services in the event of a physical or cyber emergency" (Kotka et al., 2016b, p. 104)

The relation between the data embassy initiative and concerns for Estonia's (physical) national security was also clearly pronounced by Jaan Priisalu, director-general of the Estonian Information System Authority (RIA) on a council meeting on the topic of e-Estonia: "the original idea is that we would be able to keep functioning as a state even when Estonia's physical territory is invaded" (Aasmäe, 2014).

If a government introduces a program (the data embassy initiative) to mitigate a hypothetical situation (the possibility of the invasion of the country's territory), then the inquiry into such situation will be relevant by policy analysis and political discourse analysis alone, regardless of the actual likelihood of the situation. As Ole Wæver points out, "something is a security problem when the elites declare it to be so" (Wæver, 1995, p. 54). In other words, the fact that the Estonian government is working on the data embassy initiative to increase resilience to territorial occupation is a good enough reason to research the territorial occupation of Estonia, whether such a threat is objectively realistic or not.

In a situation where a country's security and its territorial integrity are breached, a significant surge of people fleeing the country can be anticipated (Van Hear et al., 2012) (Ender, 2010). We can assume that if Estonia was being occupied, many people would attempt to evacuate the country to find shelter abroad. In fact, this had happened during the Second World War when tens of thousands of Estonians fled to Sweden and forward. Therefore, if we accept that political discourse about a hypothetical territorial occupation in the context of the digital embassy initiative justifies the research of territorial occupation, the situation of displaced people as its consequence will also become relevant.

It is not the aim of this work to assess the likelihood of such a scenario – that would require a separate master thesis on its own, in the field of International Relations. This research topic is

not relevant because of a presumed national security threat – it is relevant because the Estonian government deems it relevant.

1.2 Research methodology

The main research questions I wish to answer with this thesis is:

> *How could displaced persons with Estonian digital identities be supported with the utilization of the Estonian e-Government infrastructure?*

To help answer the main research questions, I will ask the following supporting questions throughout the thesis:

> *What are the challenges that displaced persons and organizations aiding them face?*
>
> *What components does the Estonian e-Government infrastructure consist of and what are their main features?*
>
> *What components of the Estonian e-infrastructure are relevant to the challenges of displaced persons and aid organizations challenges?*
>
> *What steps could be taken to enable the relevant components to be used to counter the challenges?*

To answer these questions, I will employ the following methodology.

After this introductory chapter, in the second chapter I will look at the challenges that displaced persons and aid organizations face throughout different stages of persons' displacement. From frameworks and handbooks published by the United Nations High Commissioner for Refugees (UNHCR), I will identify, describe and categorize the main challenges that displaced persons and aid organizations face, thus answering my first supporting research question.

In the third chapter, I will discuss the Estonian e-Governance infrastructure's components and their features. From scientific literature and technical reports published on the topic Estonian e-Government infrastructure, I identify the main infrastructural components and the features with which they contribute to the peculiarities of the Estonian e-Governance.

In the fourth chapter, I will attempt to define linkages between the infrastructural features discussed in chapter three, and the challenges of displaced persons and aid organizations discussed in chapter two. These linkages will highlight which infrastructural components are relevant to which challenges, thus answering my third supporting research question. I will also describe the nature of these linkages – what benefits could the exploitation of the identified technological linkages have, giving basis to answering the fourth supporting research question.

In the fifth chapter, I will make a policy recommendation to realize potential benefits identified in chapter four. I will outline the main opportunities and challenges arising from the policy recommendation, and recommend steps to be taken to implement the policy, while mitigating the challenges and taking advantage of the opportunities, thus answering my fourth supporting question, and in conclusion also my main research question.

To answer the research questions we use qualitative data, because there are no large quantitative datasets available on several of the subject matters, most notably on the topic of Data Embassies (Kotka and Liiv, 2015), which is a project in its early pilot phases.

2 Challenges that displaced persons and aid organizations face

To be able to discuss and analyze the potentials that the Estonian e-Government infrastructure carry in a situation where a large number of people who are Estonian e-Citizens[1], we must first understand the context.

We must understand the problems a mass exodus scenario brings about (the needs of displaced persons and the nature of the challenges they face, as well as the needs of and actions taken by organizations aiding these people) to be able to identify points where certain features of the Estonian system could be exploited to the benefit of these people in dire situations.

In my work, I am looking at how the Estonian e-Government infrastructure and e-Services could help displaced persons that are users of the Estonian e-Services (i.e. e-Citizens). For this, however, we must first understand who displaced persons are, what makes someone a displaced person, and what the common challenges are that a displaced person might face.

2.1 Terminology

When discussing people who are fleeing their homes because of war or armed conflict, the public tends to refer to them as *refugees*. Indeed, the ongoing crisis in the Middle East (where millions of people are leaving their homeland behind because of the terror and peril of the Islamic State) is often described by the media as a refugee crisis[2]. However, while the common discourse speaks of refugees, in the strict legal interpretation of the UNHCR definition of refugees[3], fleeing from war or an armed conflict does not yet qualify a person for refugee status. Therefore, there is a difference in the meaning of the word "refugee" based on whether it is used in general or legal context.

Another term that is used to refer to people in a situation as described above is *displaced persons* or *displaced people*. As per the definition of the United Nations Educational, Scientific and Cultural Organization (UNESCO), "the displacement of people refers to the forced movement of people from their locality or environment and occupational activities. It is a form of social change caused by a number of factors, the most common being armed conflict"

[1] For the sake of convenience, I will refer to Estonian citizens, non-citizen residents, and e-residents – people

[2] See for examples (Spiegel, 2014), (Clayton, 2015), (Tomkiw, 2015), (Thomas, 2015)

[3] "The term 'refugee' shall apply to any person who […] owing to well founded fear of being persecuted for reasons of race, religion, nationality, membership of a particular social group or political opinion, is outside the country of his nationality and is unable or, owing to such fear, is unwilling to avail himself of the protection of that country; or who, not having a nationality and being outside the country of his former habitual residence as a result of such events, is unable or, owing to such fear, is unwilling to return to it." (UNHCR, 2011)

(UNESCO, n.d.). This term focuses not so much on the reason for flight, but rather on the flight itself by emphasizing its involuntary nature.

Asylum seeker is yet another expression we come in the discourse. While the term in its literal meaning refers to someone who leaves their dangerous homeland to find a place of safety, asylum seeker is used mostly as a legal term. As such, an asylum seeker is someone who has applied to be treated as a refugee, in its strict UNCHR definition, but their application has not yet been reviewed.

Migrant is another term that is being often used, notably in European media referring to the contemporary influx of people into the continent. The wider definition of a migrant refers to "any person who lives temporarily or permanently in a country where he or she was not born, and has acquired some significant social ties to this country" (UNESCO, n.d.). Migrant is, therefore, a broader term, encompassing displaced persons, refugees as well as other migrants, and should be used with the specification of the reasons for migration; those who migrate to seek economic benefits have needs, motivations and legal statuses that differ significantly from those who migrate to avoid having their fundamental human rights abused. In this work, I am only considering the needs and challenges of the people who belong to the latter group.

Of the terms listed above, "displaced persons" is the one that is most relevant to this work. However, general discourse, media and even UNHCR choose to use the term "refugee" rather than "displaced persons" as a general term, even when the latter would be more precise (see UNHCR, 2016, p. 1, in footnote). Therefore I will also use both terminologies, based on the context of the references used.

2.2 The challenges of displaced persons

There are no universally applicable stages of displacement that every displaced persons would go through. Each journey is different due to the differences in crises refugees are fleeing from, the world's political climate, the individual's life situation, and even weather. Refugees' journeys might end in drastically different means. After a temporary displacement, they might return to their homes, they might find new homes away from their native land, they might end up in a refugee camp, in a legal limbo, with no resolution in sight, or might perish due to violence, accidents or life-threatening poor conditions.

In this work I attempt to identify the challenges that refugees face during three stages of a – relatively positive – scenario. In this scenario refugees first flee an armed conflict wreaking havoc in their native land, then arrive somewhere where aid organizations manage their displacement temporarily, and lastly, as their homeland's conflict does not get resolved and as

their displacement becomes permanent, they face the challenges of integration into the host community.

Future works could similarly analyze other scenarios and journey stages, such as the planning and decision-making process of flight, the return to native land after the resolution of the source conflict, legal limbo, the formation and management of diaspora (following, or as part of integration), etc.

2.2.1 In transit – flight from an armed conflict

The main aim of people fleeing war, armed conflicts and destruction is to survive, to be in a place of safety and stability, at least until the conflicts resolve. The first set of challenges (and perhaps the most dangerous ones) they face is during the flight away from their homes to safety. In the following paragraphs I will introduce the most prominent challenges that displaced persons might face during flight.

Survival – Leaving a zone of active conflict might relieve people of the primary dangers they are running away from but will introduce new challenges that might be equally threatening to their survival. The route to safety might lead through the conflict zone itself. Armed forces might actively seek to arrest or kill those who try to escape. Even when conflict zones are already behind them, refugees are often left to their own devices, where natural obstacles, weather, hard terrain, and lack of shelter can pose intermediate danger to their lives. Essential resources are scarce, if at all available – and are often expensive.

Coordination – Once someone comes to a decision that they will attempt fleeing the armed conflict in their home-land, they must come to a decision concerning their desired destination. Information on optimal destinations and routes from different media, as well as social networks, are often contradicting, volatile, and hard to come by (especially during transit) (Gillespie et al., 2016). Up-to-date and reliable information is vital for refugees in planning their journeys, which are often dangerous (Ibid.).

Transportation – As transportation services are typically discontinued in active conflict zones, due to embargoes, the risks that transportation personnel would face, or the destruction of infrastructure (Gates et al., 2012, p. 1715), the large numbers of people are fleeing a conflict zone will not be able to use conventional forms of *transportation* to get to safety. Often, refugees will have to travel on foot, or if that is not possible, revert to the services of human traffickers (Buchan, 2016). Traveling with people smugglers is far from safe – overcrowded makeshift boats have cost the life of thousands of people in 2016 alone (Edwards and Savary, 2016), and traffickers might abandon or extort helpless refugees (Harding, 2015). Even if a journey taken

with human traffickers is successful, their services are expensive; therefore many might not be able to afford them at all (Al Jazeera, 2015).

Communication – During their time in transit, refugees have the need to communicate: with authorities that they meet (or would like to avoid), with locals or aid organizations that they ask information or resources from, with their friends and families, back home, in the countries of their destination or also on the road, to know if they are safe, and with each other, to exchange information, resources, and to establish some comfort of human contact. The changing locations, distances, and the multitude of languages can make the aid of ICT (most typically phones, ideally smartphones with internet connection) useful in many (though not all) situations (Gillespie et al., 2016).

The challenges that refugees face during flight are many and depend highly on the nature of the conflict, the region, and individual factors. The challenges I identified above, however, are general enough to be faced by anyone attempting to get away from an active armed conflict. Regardless of the individual's situation, money or other valuables can always be a useful tool to attain vital resources, transportation or information. Physical resources, such as food, shelter, medicine and clothing are essential to survival. Information is of key importance throughout the journey – the quality of information available to refugees can be in direct correlation with the chance of survival. This is likely to be an issue that the e-Government infrastructure could counter. I will use these categories as the basis of further analysis of challenges that refugees face while fleeing a dangerous zone of conflict.

The next stage in a refugee's journey towards safety might be (in a relatively optimal scenario) arriving at a place that is safe and stable enough for aid organizations to be able to offer help in people's displacement. In the next section, I will look at refugee emergencies from the perspective of aid organizations (specifically UNHCR), their activities and the challenges that their activities bring about.

2.2.2 Temporary displacement – the emergency response of aid organizations

Just how every region, refugee crisis and every individual refugee faces different challenges during flight, organizations aiding refugees too have to address different challenges in every situation they work in. To be able to quickly and efficiently react to the diverse challenges that may arise during different refugee crises, the UNHCR developed a Needs Assessment for Refugee Emergencies (NARE) Checklist (UNHCR, 2016).

The NARE checklist is a tool, designed to be used by UNHCR and other aid organizations to help them assess and manage their reaction to refugee crises – to understand the nature of the

refugee crises, to identify the main challenges that coordinating these refugees pose, and to suggest actions based on these assessments (Ibid.).

The checklist is designed to be general enough, and customizable so it could be applied effectively in any refugee scenario. Therefore, I will use this tool to identify the key challenges that aid organizations face in assessing and managing refugee emergencies.

The NARE checklist suggests using several methodologies to assess the nature and severity of refugee crises. I will now briefly introduce these methodologies to understand their function and identify what information sources refugee organizations need to employ them. Based on this information I can later analyze which refugee emergency assessment methodologies could have the potential to be supported by the Estonian e-Governance infrastructure. The methodologies are:

Critical background (pre-influx) information collection and analysis and *post-influx secondary data review* – the pre-existing data sources may come from third party organizations and have to be analyzed in the context of the ongoing refugee situation. The checklist also provides action proposals, depending on the results of the secondary data review. Because this methodology suggests the usage of third party quantitative data, e-Governance might be able to support it.

Community observation and *infrastructure and facility visits* – direct observation of the refugee communities and key facilities is used to get a quantitative, top-down view of the issues.

Community key informants – key stakeholders in the refugee community are identified who can provide valuable field reporting, and may provide an explanation of quantitative, top-down observations. If rich digital data profiles of refugees in the community were available, it could be used to help identify key members of the community.

Focus group discussions – with participants from controlled demographics samples, these discussions can provide practical information, uncover conflicts and their natures, and might result in proposals for action.

Household key informant interview – the holistic study of individual cases can uncover systemic issues.

The NARE checklist also proposes a list of general data to be collected to understand emergency population profile and help their registration, to map population movement patterns, to manage emergency security and mitigate threats, emergency logistics and supply.

The NARE checklist is divided into several sections, where each section focuses on assessing separate key issues. These sections illustrate the primary needs of refugees in a stage where they are no longer left to their own devices – they are coordinated by aid organizations. These sections are: management of water, sanitation, hygiene (WASH)[4], camp management and communal living[5]; settlement development, shelter and management of core relief items (CRIs), food security, health and nutrition, education and the assessment of cross-cutting protection issues (UNHCR, 2016). I will use this categorization as the basis of further analysis of challenges that the refugees face when managed by aid organizations (e.g. in refugee camps).

Based on the content of and the methodologies suggested by the NARE checklist, I identify the following, high-level challenges that refugee aid organizations (specifically UNHCR) face during a general refugee emergency:

- *Resources* – each issue outlined in the checklist's sections (WASH, food, education, etc.) require resources, both physical goods (food, medicine, infrastructure, etc.) and human resources (security personnel, social workers, medics, etc.). In a refugee emergency, adequate resources have to be identified, acquired and distributed urgently.
- *Coordination* – the acquisition, storage and distribution of resources, the performance and efficiency of services, the safe and secure registration and housing of refugees of refugees requires systematic coordination.
- *Stakeholders* – key persons in the refugee community, officials and authorities of the host, transit and home countries, other organizations and NGOs have to be informed, consulted or observed, to provide aid, to help the aid process and to mitigate issues and threats.
- *Information* is a key tool that supports all the above challenges and is gathered using the methodologies recommended by the checklist and summarized above.

I will consider these general categories as the basis of further analysis of challenges that aid organizations face in a refugee emergency situation (e.g. when managing a refugee camp).

2.2.3 Long term displacement – integration into the host society

Ideally, the displacement of any person who fled a conflict zone, crisis situation or disaster area should be temporarily, and they should return to their homes after the conflict, crisis or the

[4] Clean and drinkable water is essential to survival, and often is a challenge to supply. The availability of sanitation and hygiene facilities and their usage is in direct correlation to the health of refugees.

[5] The management of the location, quality and staff of camps that refugees are housed in, as well as the community life of these camps, is needed to guarantee security and stability.

damages done by a disaster have been resolved. History shows, however, that this is often not the case. Central-Eastern Europeans who fled their homelands to the West because of dangers (such as the ethnic cleansing of Nazi Germany or Stalin's Soviet Union) could not return for half a century. Similarly, the conflict between Israel and Palestine has been ongoing since 1948, with millions of people displaced both internally and externally (Chalabi, 2013). Any time span during which entire generations live the majority of their lives could hardly be considered temporary.

People's lives cannot be put on hold for an extensive time with the faint promise of a future resolution to the issues causing their exile. In the case of protracted displacement, they will want to create new lives for themselves in the meantime too – wherever they might be (Crawford et al., 2015, pp. 17–19). The question is whether these new lives will be separate from the host country's society, or integrated with it.

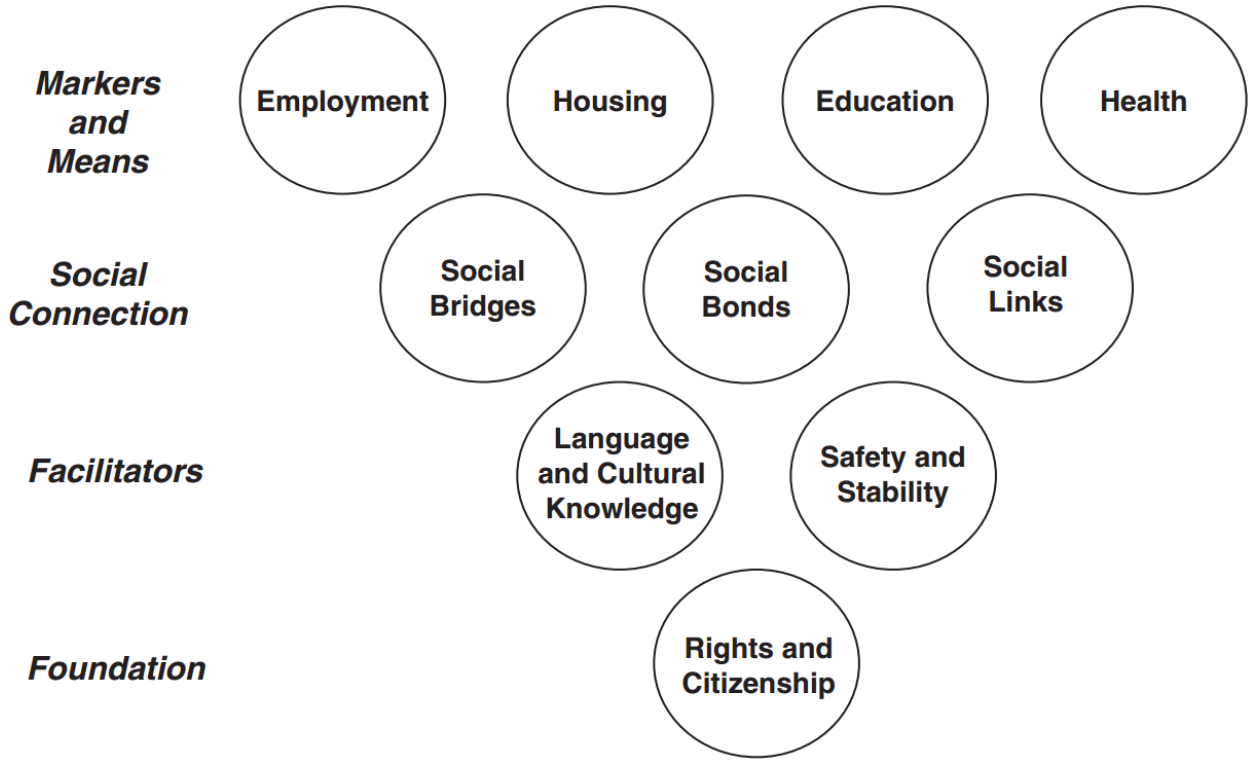
In the case of a long-term displacement, the displaced persons' integration into the host societies is in the interest of both the displaced person and the host society. The more a displaced person is integrated into the host society (in cultural, legal, economic terms), the more they benefit by accessing larger social networks, education and health services, legal protection, career opportunities, etc. The host society benefits from the displaced persons' integration by gaining economically active residents (as opposed to passive residents who do not contribute to the country's economy but use resources).

Integration into the host society is not a process evolving by itself – it takes effort from both the host society and the displaced persons. In the long term lack of integration can result in ethnic conflict between the host culture and the displaced persons' culture (UNHCR, 2013, pp. 74–75).

The contemporary tendencies of displacement show that the number of people living in displacement is larger than ever, and the share of displaced persons repatriating (i.e. returning to the regions of their origin) is lower than ever before (Crisp and Long, 2016, p. 145). These figures further emphasize the relevance of integration efforts.

There is no one, widely accepted definition of what the integration of refugees or displaced persons means. This is due to the fact that integration is highly contextual; the word's meaning depends both on the host country's and the displaced persons' expectations and cultural backgrounds. It is also because the level of integration consists of different aspects – for example, one can be integrated to the host country's workforce, but not be culturally isolated (Castles et al., 2001, p. 12 in Ager and Strang, 2008, p. 167).

While there is no official definition of refugee integration, I have come about existing, universally applicable statements about the subject. UNHCR identifies the goals of refugee integration in general as "equality, inclusion and achievement" (UNHCR, 2013, p. 11). UNHCR also identifies three distinct dimensions of the process of refugees' integration into host societies; namely, that integration is a legal, economic as well as social and cultural process (UNHCR, 2002a, p. 2). A Conceptual Framework Defining Core Domains of Integration has also been developed, providing "…a coherent conceptual structure for considering, from a normative perspective, what constitutes the key components of integration" (Ager and Strang, 2008).



2. figure: A Conceptual Framework Defining Core Domains of Integration (Ager and Strang, 2008, p. 170)

I will take the core domains of integration identified by Ager and Strang as general categories of challenges that refugees (and host communities) might face, and use the three dimensions defined by UNHCR and categorize these challenges by them. This will give us a basic understanding of challenges of local integration, as well as the common features of these challenges.

Legal dimension

If we consider the goal of integration as becoming equal with and included in the host society, the purpose of the legal process is to have the same legal status or rights that the members of the

host community have. Legal equality cannot happen instantly – a displaced person will never be granted the same rights as citizens of the host society. It must be a process, where displaced persons gradually have increased rights and legal statuses closer or identical to those of citizens of the country.

The basis of this legal process is a clear legal status that can best be achieved with the help of documents, proofs and certificates that verify the identity of the displaced person and give bases to their claims. "Re-establishing and preserving identities is key to ensuring protection and solutions for refugees" (UNHCR, 2015). The lack of documents due to losing them during transit or the inability to carry them around is a critical issue in establishing clarified legal status (UNHCR, 2013, p. 19). Host states enforce the identification of incoming refugees and displaced persons because taking in people with unclear identities carries risks. During the ongoing refugee crisis in Europe, a significant (although disputed) portion of the incoming migrants changed or deliberately lost their identities to be able to apply for asylum, when in reality they were not fleeing conflicts zones, and were only motivated by the promise of the better economic perspective of Europe (Mekhennet and Booth, 2015). Some of the perpetrators responsible for terror attacks in France in 2016 also have been found to have arrived at Europe claiming to be refugees, using fake identities (BBC News, 2016).

Missing legal documents, proofs, and certificates make legal proceedings in the host country very challenging, since supplementing them is often impossible due to the disruption of the home state and lost identities of the displaced persons. These challenges are further aggravated by the fact that the legal requirements might differ significantly between the home country and the host country. Legal issues displaced persons face can typically be (but not limited to) family-related issues (marriage, children), issues related to ownership, labor-related issues and certifications, health problems, or criminal cases (Prettitore, 2016). Legal proceedings in such situations can be problematic if the legal history of the involved parties is missing (Ibid.).

The legal dimension of the integration process can be projected onto the framework of core domains – the domains of employment, housing, education, health, safety and stability, and rights and citizenship all have legal implications.

Economic dimension

From an economic perspective, we can consider the goal of integration to be the inclusion into the host country's economy and achievements on the workforce or entrepreneurial achievements. The process is moving from being completely economically dependent on the host state and aid

organizations to being completely self-sufficient and an active, contributing member of society (UNHCR, 2002a, p. 2).

Most refugees have no means to participate in the host country's economy upon their arrival. Lack of permission to work and the lack of or difference in certifications needed for jobs (a connection with a legal dimension), language barriers and a lack of professional network (a connection with the social and cultural dimension) prevents refugees from joining the host country's job market or conducting entrepreneurial activities. Because of these connections, the process of economic integration is intertwined with legal and socio-cultural integration.

The benefit of economic integration in terms of Ager and Strang's core domains is – obviously – employment, stronger social connections, as well as is increased stability and (financial) security, and through that better housing, health and education perspectives.

Social and cultural dimension

From a socio-cultural perspective, the aim of refugee integration is becoming an organic part of the communities of the host country. At the beginning of the integration process, a refugee is typically isolated from the host communities, by linguistic, cultural or religious differences (and possibly by regional seclusion, ghettoization). During the process of socio-cultural integration, this isolation morphs into personal and community-level interactions with the host community, acceptance of each other's cultures and the birth of a new, common identity.

Ideally, social and cultural integration is a two-way process in which the openness and flexibility of the host community are just as important as the refugee's openness and willingness to adapt to the host culture. Socio-cultural integration does not infer the loss of the refugee's native social and cultural values, traditions or connections. At most, it means the reinterpretation of value sets (of both the refugee and the host community) so that the culture and the social values of the native society and the host society could co-exist (on a personal, family, community and societal levels) (UNHCR, 2002a, p. 2).

Social and cultural integration is a more nuanced and is more complicated to quantify than legal and economic integration. Every domain identified by Ager and Strang has some degree of relation to social and cultural integration processes: employment (workplace discrimination), housing (ghettoisation or gentrification), healthcare and education (equal opportunities), obviously domains of social connections, language and cultural knowledge, safety (xenophobia), and rights and citizenship (common national identity).

I will use the above dimensions as general categories and the domains of integration as examples as the basis of further analysis of challenges that aid that refugees and the host society face during the process of integration.

2.3 Conclusions

Throughout different stages of their displacement, refugees and displaced persons face sets of challenges that differ in nature.

Survival, resources, coordination, transportation and communication are the key issues that people must come over during transit.

When receiving emergency response aid from aid organizations, the primary challenges refugees are aided in are related to WASH, communal living, housing, food, nutrition and health, education and security (UNHCR, 2016). I identified the following categories of aid organizations' challenge during a refugee emergency s: resources, coordination, stakeholders and information. I categorized the challenges refugees face during local integration along the lines of the three dimensions identified by (UNHCR, 2002a, p. 2).

3 The Estonian e-Governance infrastructure's components and key features

We must understand the historical and country specific context and the motivating factors that contributed to the Estonian e-Government to be what it is today, because these factors are also amongst the drivers of future developments of the Estonian e-Government. We must understand the infrastructure that is underlying the Estonian e-Governance, what its key components and their most significant features are.

3.1 E-Governance

The Organisation for Economic Co-operation and Development (OECD) defines e-government as "[…] the use of new information and communication technologies (ICTs) by governments as applied to the full range of government functions. In particular, the networking potential offered by the Internet and related technologies has the potential to transform the structures and operation of government" (OECD, 2002). The definition points to the fact that successful e-Government cannot be achieved by technology only; changes in organizations and in the way they work are also necessary.

According to the Council of Europe, "e-governance is about the use of information technology to raise the quality of the services governments deliver to citizens and businesses. It is hoped that it will also reinforce the connection between public officials and communities thereby leading to a stronger, more accountable and inclusive democracy" (Council of Europe, 2004). This definition points out emphasizes the potentials social benefits of e-Governance.

The terms *e-Government* and *e-Governance* refer to different concepts. E-Government is a more narrow term, focusing on the ICT services that are closely related to government functions such as e-Taxation, e-Health or e-Procurement (Saparniene, 2013, p. 2). E-Governance, on the other hand, encompasses the function of government, the private sector and non-governmental organizations, focusing on the linkages facilitated by ICT solutions (Ibid.). While there is a distinct difference in the meaning of the two words, there is often confusion in as to which one to use – some literature uses them incorrectly and interchangeably.

3.2 Estonia

Estonia is a small parliamentary republic in North-Eastern Europe, with a population just under 1.3 million, and the size of 45,228 km^2 (Central Intelligence Agency, n.d.). After almost half a century of occupation, it has regained its independence from the Soviet Union in 1991. Since then, Estonia has become one of the most successful post-Soviet countries with a stable

economy, and very high levels of human development (33rd in the Human Development Index in 2012 (United Nations, n.d.)). Estonia joined the European Union and the North Atlantic Treaty Organization (NATO) in 2004, and became a member of the eurozone by adopting the Euro as its official currency in 2011.

Estonia regained its independence from the Soviet Union relatively peacefully (i.e. without serious casualties). The freshly independent Republic had a priority of cutting ties with its soviet past and repositioning itself towards Europe – politically, economically as well as technologically.

In terms of information and communication technologies (ICT), it meant that the old and dated soviet technologies were gradually scrapped and the emerging and cutting edge technologies of the time – mobile telephony and the Internet – were implemented and the bases of an information society were laid down. (Dutta, 2006, p. 86)

The mission of the Estonian information society policy was to "increase competitiveness; reduce division within society; and foster state–individual relationships" (Runnel et al., 2009, p. 30); these objectives were all in line with the efforts of reforming the structure and values of the Estonian society. A national education program "Tiger Leap" (Tiigrihüpe in Estonian) was rolled out with the aim of bringing Internet access to every school and public library in the country, and disseminating basic computer literacy amongst young people and the citizenry. Analysis of the success and implication of Tiger Leap brought about the even more ambitious plan of "full virtualization of the public sector" (Lopes and Theisohn, 2003, p. 217) (Thurnay, 2014)

This fully virtualized public sector has been realized to large extent and it continues to be developed. By today, the citizens and residents of Estonia have acquired and widely adopted digital identities, there are over 2000 interconnected online state services offered (e-Estonia, n.d.).

The virtualization of the public sector (i.e. e-Governance) has brought about changes, new challenges and opportunities in Estonia. Since the e-Government services and infrastructure has become of critical importance for the operation of the country's public administration, governmental services as well as the operation of private sector organizations such as banks, the reliability and availability of this infrastructure and core services is crucial. Guaranteed availability of e-Services has been a priority of the Estonian e-Governance effort, already from the initial design stages.

In 2007, simultaneously with the rioting and public unrest of some Russian nationals in Tallinn (in reaction to the city government replacing a Soviet military memorial monument from

a central square), key ICT infrastructure, state e-Services, media outlets and online bank services suffered large scale cyber attacks (Ashmore, 2009). The attacks are widely attributed to have been initiated on behalf of the Russian Federation, which made this incident the first major act of cyber warfare in history (Ibid.).

The damage done by the attacks was significant but not severe, due to the fact that a national Computer Emergency Response Team (CERT) was assembled and had been operating a year prior to the incident (Ashmore, 2009). The precedence setting nature of the attacks, and the degree of preparedness and effectiveness with which CERT mitigated them earned Estonia wide international recognition for being a pioneering country not only in the field of e-Governance but national cyber security as well (Ibid.). This led to the decision that NATO's Cooperative Cyber Defence Centre of Excellence (CCD COE) was to be opened in Tallinn, further deepening Estonia's integration and relevance in the Organization (Ibid.).

The Estonian State's heavy reliance on ICT had exposed its national security to cyber threats but the successful countering of the threat upon its realization strengthened the national security as Estonia's position in NATO became more cemented. Therefore we can argue that the information society and e-Governance efforts are intertwined with the national security of the country.

Similar to how successful cyber defense efforts have strengthened Estonia's position in NATO, novel initiatives such as internet voting, the possibility of registering new businesses very quickly, digital signatures that are adapted nationwide, etc. have gotten wide international recognition, and with the help of active country marketing efforts, have established Estonia's image of e-Estonia; "one of the most advanced e-societies in the world" (e-Estonia, 2016). A post-Soviet country with small population and a short history of self-determination, Estonia needed something to be identified by in the world, something to "place it on the map",

Estonia's recognition as a technologically savvy country has not only happened abroad – the achievements in the fields of e-Governance as well as the success of companies with Estonian involvement such as Skype have started to shape Estonians' national identity as well (Bengtsson, 2012).

3.3 The key components of Estonian e-Government infrastructure

When discussing electronic government, the concept of infrastructure can be interpreted in different ways. We can talk about the physical infrastructure that e-Governance services utilize – the servers and network devices, the networks connecting servers with users, the electric grid that powers the servers and network devices, etc. We can also discuss the intangible e-

Governance infrastructure – architectural and design concepts, standards, software, and key services upon which e-Governance services facing end users are based. In this work, I chose to study infrastructure in the non-tangible sense of the word, owing to the fact that the physical infrastructure under the Estonian e-Governance is not the differentiating factor between e-Governance in Estonia and other countries; the peculiarities of the Estonian e-Governance are found in the intangible components.

The (intangible) infrastructure itself can also be classified, divided into components in different ways, depending on whether we approach the subject from a technological or functional perspective. Therefore, there is no canonical, definitive list of Estonian e-Governance infrastructure components (and compiling a definitive list is not the aim of this work either). Nevertheless, certain components do stand out as key e-Governance infrastructure components when studying relevant and competent literature (for example the European Commission's factsheet on the Estonia e-Government (European Commission, 2015, pp. 35–38), the Estonian State's official website promoting "e-Estonia – the Digital Society" (e-Estonia, 2015, sec. "Infrastructure"), the Digital Agenda 2020 for Estonia (MKM, 2013, p. 2)).

These components are the X-Road, electronic identity (eID), the public key infrastructure (PKI, the technical basis for authentication, authorization and the issuing of digital signatures). I will use these components to answer my second supporting research question – what components does the Estonian e-Governance infrastructure consist of – and to analyze their key features.

In addition to these components, I also identified the Government Cloud and Data Embassies project (Kotka and Liiv, 2015) that – once implemented – will be a key component of the Estonian e-Government infrastructure, but is missing from the literature cited above, since the project is still in its early stages; it does not yet play (considerable) role in the infrastructure (Vabariigi Valitsus, 2016, l. 67).

3.3.1 X-Road

X-Road is a "distributed, secure, unified web-services based inter-organizational data exchange framework", and as such it is the backbone of the Estonian e-Government infrastructure. X-Road has a standardized Application Programming Interface (API) that Estonian e-Government services and datasets implement, to form a linked, interconnected, decentralized portfolio of services and datasets (Cybernetica, 2013).

X-Road, as one of the core infrastructural components of the Estonian government is *decentralized*. It is designed so that there would be no single point of failure – even if some components, servers or services malfunction, or cease to operate, the rest of the service portfolio

(at least those services that are not directly depending on the malfunctioning service) remain operational (RIA, 2016, pt. 2). A data exchange framework, X-Road enables services that implement it to *query and link data across different databases* that are managed by different authorities. Each authority can manage which service provider of other authorities can access and query datasets managed.

Its design and protocols make X-Road highly *modular*, as opposed to being one monolithic system (RIA, 2016, pt. 1). This is an important reason behind the success of the Estonian e-Governance. Modularity means that the system is designed so that components – datasets, services – could be added, modified and restructured with ease. The implication is that the Estonian e-Governance is not locked into rigid system that was designed for the needs of the State, and its understanding of the World as it was in the end of the 1990's, during the time of designing X-Road (RIA, 2016, pt. 1), but it can grow and change in an *agile* way, along with the country, the needs of the State and the citizenry.

Also, thanks to the *secure*, *encrypted* communication protocols that X-Road employs, information from databases that are part of the X-Road network can be queried via the public Internet. Developing the Estonian e-Government, there was no need to invest in expensive additional physical infrastructure, and there is no additional network infrastructure to be maintained for the continuous operation of the services (RIA, 2016, pt. 1).

3.3.2 Public key infrastructure

"A public key infrastructure (PKI) is the combination of software, encryption technologies, processes, and services that enable an organization to secure its communications and business transactions" (Microsoft, 2003). The primary features of PKI are

- *authentication* – "assurance that an entity is who he/she/it claims to be" (Adams and Lloyd, n.d.),
- *integrity* – assuring that the data has not been altered during a transaction, and
- *confidentiality* – "The assurance […] that no one can read a particular piece of data except the receiver(s) explicitly intended" (Adams and Lloyd, n.d.).

In the Estonian national PKI, every e-Citizen is issued with a public key – everyone can benefit from the features of PKI. Citizens are issued an identity card, which – in addition to a portrait photo of the citizen, enabling face-to-face visual identification – has a built in chip, with the basic data and the citizen's public key in digital format. The *authentication* feature of the Estonian PKI is realized by e-Citizens inserting their ID cards in a card reader, and entering their

PIN1 (used for authentication, as opposed to PIN2 which is used to issue digital signatures) (Sertifitseerimiskeskus, 2016, sec. What is Digi–ID card, PIN codes).

Public keys being embedded into national ID cards mean that in addition to the conventional personal identification methods, the ID card can be used to identify a person in a digital environment. Instead of ID cards, citizens can also use Mobile IDs; a technology with the same principle, only the chip containing the public keys is the SIM card of the mobile device that is performing the authentication (Ibid.).

The Estonian PKI, embedded to ID cards and Mobile-IDs also enables citizens to issue digital signatures. In Estonia, digital signatures carry the same legal value as conventional, paper-based signatures. Each digital signature also consists of a timestamp. Digital signatures are the component of the Estonian PKI that provides *integrity*, since the signature becomes unverifiable, invalid if any of its properties (the content of the signed file, the timestamp, signer's data etc.) are modified (Sertifitseerimiskeskus, 2003).

Estonian e-Citizens can also use their ID cards and mobile IDs to encrypt computer files. It is possible to specify a list of entities (which, in the Estonian case are mainly e-Citizens and institutions with digital identities) referring to them by their national identity code – only these authenticated citizens will be able to decrypt the encrypted documents. This encryption component provides the *confidentiality* feature of the Estonian PKI (Sertifitseerimiskeskus, 2003).

3.3.3 eID

Every e-Citizen of Estonia has a personal identification code. This code is used as a basis of the citizen's identity by the state, throughout their lives. Most of the Estonian public registers and documents containing citizens' personal information is managed digitally, and these documents are attributed to the citizen by the citizens personal code, therefore the personal code is also a basis of the citizens' *digital identities*, or electronic identities (eID).

As described above, the overwhelming majority of the Estonian e-Governance datasets and services implement X-Road, making them all linkable and interoperable. The fact that most of the e-Citizen's data and documents are managed online and have the citizen's personal ID number associated with them mean that *information on the citizens are also linkable and interoperable*. In practice, this enables the policy that no duplicate information should be stored about citizens – each unit of information is managed by the authority responsible for it.

For instance, the names and birth dates of citizens are managed by the Population Register of the Ministry of the Interior (Ministry of the Interior, 2016), and data on real estate ownership is

managed by the e-Land Register of the Center of Registers and Information Systems (Center of Registers and Information Systems, n.d.). If a citizen wants to see a list of real estate owned by them, he can do it using the service "Registered immovables [sic.] of citizens"[6] on eesti.ee website, one of the main e-Service portals, managed by the Information System Authority (RIA), which operates under the Ministry of Economic Affairs and Communications (MKM). First, the citizen has to log into the portal by identifying themselves using their ID cards or mobile IDs and their PIN code (see PKI). Then, when the citizen makes a query using the service, the service will pull through the name associated with their personal code from the Population Register, and the data of the real estate associated with their personal coed from the e-Land Register. This scenario illustrates how databases containing personal information of citizens are distributed and are managed by separate authorities, but how they are also linkable by citizens' eIDs via X-Road, so any data related to a certain citizen can be inspected together (given that the dataset managers permit our service to access their data).

3.3.4 Government cloud and Data embassies

The U.S. National Institute of Standards and Technology defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources […] that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Mell and Grance, 2011). The benefits of applying cloud computing technology include *rapid elasticity* (i.e. the seamless adjustment of resources to increased demand, under short period of time), *continuous operation* (the system is designed to be redundant, where malfunctioning components are replaced automatically, providing very high system availability) and *location independence* (cloud computing infrastructure is redundant and usually spread out geographically, so the integrity of any one single data center is not crucial to service operation) (Mell and Grance, 2011).

The basis of this chapter on government cloud and data embassies is an article by Taavi Kotka and Innar Liiv, "Concept of Estonian Government Cloud and Data Embassies" in which they outline the peculiarities of Estonian e-Governance, and propose, for the first time, the components of the Estonian government cloud, and as part of that, the concept of Data Embassies (Kotka and Liiv, 2015).

Many European countries, including Estonia, have concluded that these features of cloud computing – rapid elasticity, continuous operation, location independence – could be used as the infrastructural basis of their e-Government services (Kotka and Liiv, 2015, p. 149). However, the

[6] https://www.eesti.ee/eng/services/citizen/raha_ja_omand_1/kodaniku_kinnistud_1

assessment of the possibility of implementing governmental cloud in Estonia shows that the ubiquitous service portfolio, the advanced Estonia information society and the e-Residency project – issuing Estonian digital identities for and granting access to the e-Service portfolio to citizens of any country – warrant additional components complementing the solutions used commonly by other states (Kotka and Liiv, 2015).

These peculiarities of the Estonian e-Government system were the basis of the Concept of the Estonian Government Cloud and Data Embassies (Kotka and Liiv, 2015), which considers three main technological components:

- Cloud infrastructure located in Estonia proper,
- Public clouds offered by big international service providers, and
- Data embassies.

Cloud infrastructure in the country's territory

Creating a governmental cloud infrastructure in the country's territory is the most common strategy; it is the first and most relied upon component of the three. In essence, it refers to the creation of a standardized and distributed network of data centers complying with the above cited definition of cloud computing, where the data centers are located in the territory of Estonia (ENISA, 2013). In comparison with the current state of service infrastructure, this would take the responsibility of operating servers that meet the required security and availability standards away from individual governmental organizations' technical departments. Instead, the secure and stable operation of governmental servers would be centralized in terms of organization structure (the servers would be operated by one governmental cloud operator) but physically decentralized (to meet the definition and enable the benefits of cloud computing (Kotka and Liiv, 2015).

Since much of the e-Government services and databases manage highly sensitive personal and corporate data as well as state secrets, these systems' security integrity is absolutely critical. Having the entirety of the cloud infrastructure in the country's territory provides ideal overview of and control over the systems' integrity from a cyber and physical security perspective. On the other hand, operating the entirety of a government cloud inside the country's territory makes the integrity of the cloud depend directly on the integrity of the country's territory itself. In other words, if the country's territorial integrity is breached, the physical security of the governmental cloud (and consequently the entirety of the e-Service and database portfolio) cannot be guaranteed either (Kotka and Liiv, 2015).

Using public cloud services of multinational private providers

Companies such as Amazon (with Amazon Web Services), Microsoft (with Microsoft Azure) and Google (Google Cloud) offer large, enterprise cloud services with high availability standards, for – enabled by the massive scale of their operation – much lower prices than what operating services of the same standards would cost for a small country like Estonia. More importantly, these companies' global presence also renders the risks of the geographical concentration of country-specific cloud infrastructure irrelevant (Kotka and Liiv, 2015).

However, since the operation of public clouds is delegated to the service providers, a government that would operate its services on public clouds would have limited oversight and control over the actual integrity and security of the underlying infrastructure. While software produced by the state can provide some level of security, isolating itself from the risks derived by the uncharted nature of the infrastructure they would run on, these risks could not be totally eliminated. Storing and processing highly sensitive data on such services is therefore not a viable option – especially in light of the recent secret information leaks on foreign intelligence agencies infiltrating and wiretapping similar services (Kotka and Liiv, 2015).

As a government cloud pilot project, Estonia already migrated some of its services to Microsoft public cloud "Azure" – services that contain no sensitive data, but may be subject to significant growth of demand temporarily and whose availability carry national symbolic significance – so as to better guarantee their availability (e.g. the website of the President or the Government) (Microsoft and MKM, 2015) (Kotka et al., 2016a). The possibility of migrating sensitive data to public cloud services – despite the inherent security risks – to guarantee digital continuity in case the territorial integrity of the country is breached, is also discussed (Kotka and Liiv, 2015).

Data embassies

To combine the benefits of a territorial cloud infrastructure (exclusive control over the cloud infrastructure) and using multinational private cloud providers (global distribution, infrastructure integrity not dependent on the country's territorial integrity), there is a proposed solution to establish data centers on the premises of Estonian diplomatic missions in friendly foreign countries (Kotka and Liiv, 2015, p. 157).

Diplomatic missions operating in foreign countries enjoy diplomatic immunity granted by the Vienna Convention on Diplomatic Relations (United Nations, 1961) and the Vienna Convention on Consular Relations (United Nations, 1963), meaning that diplomatic missions can operate without harassment by the country they are hosted in; the members and buildings of diplomatic

missions in most cases are not subject to the authority of the host countries . Many countries are already using this protection to store passive back-ups of their digitized governmental data on embassy premises, however, the management of offline backups – transferring data using physical storage devices – is suboptimal and not scalable, due to the delay it introduces to the process (McCluskey, 2015).

The lengthy manual process of moving backups to embassies on physical storages could be improved by moving data via networks, to servers on the premises of diplomatic missions, as warm or hot backups[7] (Segue Technologies, 2013). The diplomatic and consular immunities granted by Vienna Conventions mean that servers housed in Estonian embassies, consulates (or residences of heads of mission) also cannot be investigated, confiscated, or their communication wiretapped. If these servers hosted e-Government services and databases, the combined benefits described above would be achieved (Kotka and Liiv, 2015).

However, real estate of diplomatic missions are most often not suited for housing professional data centers complying with the required standards (concerning physical security, HVAC, industrial quality low latency broadband internet connection with high availability, etc.), therefore the technical feasibility of this solution is limited (Kotka and Liiv, 2015).

The Data Embassy project is a novel initiative to mitigate the technical limitations of diplomatic real estate by hosting the cloud infrastructure in friendly countries' professional data centers outside of the physical buildings of diplomatic missions, but under their jurisdiction, under a secured and isolated separate perimeter, in compliance with diplomatic standards, accessible solely by the diplomatic corps, enjoying the diplomatic immunity just as the buildings and information of diplomatic missions do (Kotka and Liiv, 2015). However, while the Vienna Conventions content – guaranteeing immunity – should apply, the case of data embassies is unprecedented; it is therefore unclear how the international community would proceed in this regard (Kotka et al., 2016b).

The creation of data embassies as a mean of guaranteeing digital continuity of the state is part of the Estonia's Cyber Security Strategy 2014-2017 (MKM, 2014). As of 2016 the first virtual data embassy pilot project is finished (i.e. the transfer of the President's website to Microsoft Azure) (Microsoft and MKM, 2015), and the second pilot of moving the e-land registry and electronic ID service to public clouds is ongoing (Vabariigi Valitsus, 2016, l. 67). The preparation works of physical data embassies are underway, one possible host embassy has

[7] I.e.: this would allow the backups to be rolled back to production with smaller efforts

already been chosen (Ibid.). In the same time, the legal aspects of the using friendly countries' governmental data centers as data embassies are being analyzed (Ibid.).

While the implementation of data embassies is still under way, throughout the rest of my work I will assume the completion and operation of data embassies, as it is described by (Kotka and Liiv, 2015) and (Kotka et al., 2016b).

3.4 Key features

The components of the Estonian e-Governance infrastructure that were identified in the previous chapter contribute to the peculiarities of the Estonian e-Governance infrastructure with the following key features.

- *Decentralization* – X-Road's architecture provides that the Estonian e-Governance does not have one single point of failure, services and datasets are not managed by one central authority.
- *Linkable datasets* – Databases implementing X-Road protocols can be connected using common identifiers, even if they are managed by different organizations, as long as the managing organization grants access.
- *Modularity* – Due to X-Road's modular design, new databases and services can be connected to the system, and existing ones can be modified and restructured with ease.
- *Agility* – Its infrastructure's modularity enables the Estonian e-Government to be developed in an agile manner, dynamically responding to ever changing needs and contexts.
- *Security* – Security is provided on multiple levels of the infrastructure. All communication between databases and services are encrypted by X-Road. The PKI provides personal encryption service, and guarantees the integrity of digital signatures.
- *Authentication* – Thanks to the unique personal code, the PKI, every citizen has a digital identity with which they can identify and authenticate themselves in digital environments, express their personal intents by issuing digital signatures.
- *Digital identity* – digital authentication and linkable datasets about citizens' information enable the formation of digital identities: citizens' properties that concern the State or functions of public agencies are available digitally.
- *Continuous operation* – the Governmental Cloud initiative will increase the infrastructure's resilience to demand fluctuation, and failure physical infrastructure, individual databases and services.

- *Location independency* – The Data Embassy initiative will support continuous operation by increasing the infrastructure's resilience to disruptions of the country's territorial integrity.

It is not the aim of this work to compile a definitive list of Estonian e-Government infrastructure components, or to propose a framework its main features. Others might structure the lists compiled above differently, or might consider further elements to be added. However, I find this collection to provide sufficient details to enable the identification of linkages, as described in the research methodology.

4 Components of the Estonian e-Government infrastructure that are relevant to the issues that refugees and aid organizations face

In chapter 2 I established *challenges* that displaced persons and aid organizations face during a refugee crisis. In chapter 3 I defined the key *components* of the Estonian e-Governance infrastructure. In this chapter I will identify possible linkages between these *challenges* and *features*. A linkage is identified when certain *components* have the technological potential to be used to counter the nature of certain *challenges*.

4.1 (Re-)establishment of identities of displaced persons

In the previous chapter I concluded that identity-related issues can cause significant challenges to both displaced persons and organizations aiding them. If a displaced person's identification documents are lost, verifying their identity is going to be difficult. If a displaced person's identity is not verified, authorities of host and transit countries might not grant them entry, since their claims of fleeing dangerous regions (which would be their legal basis of entry) cannot be verified. The same issue arises when a displaced person applies for asylum.

The Estonian e-Governance stores e-Citizens' names, personal codes and biometric data in digitized, linkable databases. In theory, if a displaced person who lost their identity document provides their name or personal code, and have their fingerprints scanned, their names or IDs could be matched up by querying the relevant datasets, and their identity could be re-established. The digital profiles of e-Citizens have the potential to be used to re-establish the identities of displaced e-Citizens who have lost identification.

Even if the identification document of the displaced person in question is available, the possibility of performing biometric identification provides additional guarantee of the genuineness of the identity. Biometric identification could be used to filter out counterfeit identity documents. Also, while authentication using PKI (i.e. with national ID card or mobile ID) is primarily intended to be used for authentication in digital environments, it could also be used to provide additional guarantee of authenticity in an interpersonal situation (e.g. an officer verifies the identity visually, and also prompts the citizen to authenticate themselves digitally).

In fact, biometric identification is already being used by UNHCR to register and identify refugees (UNHCR, 2015). Being able to use the already established biometric identity of an e-Estonian citizen would have the benefit of the continuation of their identity (as opposed to losing their old identities and then gaining a new one from UNHCR), it would make processing their

cases and requests more efficient, and with a clear, credible and "rich" (in terms of data and history) digital profile, would likely make the life and integration of the displaced person into the host country's society easier.

4.2 Information about displaced persons

Each refugee crisis has its own complex set of challenges. In the second chapter I found that to be able to identify and assess these challenges, and to provide survival, safety and acceptable conditions to displaced persons during their temporary displacements, aid organizations need several diverse sources of information. Large, quantitative datasets about the displaced persons, home and host country's population, geography, economy, as well as qualitative data from interviews and focus groups, field reports are needed.

The Estonian e-Governance has a high degree of maturity, and most of state and public registers, databases are and documents are managed in digitized, standardized format, linkable by X-Road. In theory, these databases could be sources for rich, quantitative data of demographics, information on the population health and education, and support aid organizations in their efforts of understanding the complex challenges they are facing.

Given that the identities of displaced persons' have been re-established, verified and registered upon their arrival, the a list on the members of the refugee community can provide an additional valuable dimension to the datasets above. Data analysis of state and public databases, cross referenced with the list of citizens in the refugee could be used to create detailed profiles on help in identifying not only community key informants and ideal focus group discussion participants[8], but also to identify potential community liaisons, persons or groups that are likely to be in vulnerable situations, or who are likely to cause security issues[9]. With conventional method, these benefits could only be achieved if each displaced person would be interviewed in depth, which – depending on the refugee emergency – would be either very difficult, or completely unfeasible.

The availability of rich, linkable, computer analyzable datasets about the refugee community would enable aid organizations to make data-driven decisions[10].

[8] As discussed in chapter 2, they community key informants and focus group participants are needed to perform data collection prescribed by the NARE checklist.

[9] These are merely theoretic possibilities. Any practical implementation of profiling raises ethical and legal questions which are topics that I will cover in chapter 5.

[10] Data driven decision making is "the practice of basing decisions on the analysis of data rather than purely on intuition", according to (Provost and Fawcett, 2013, p. 53).

4.3 Supplementing missing documents

In the third chapter I identified the legal dimension of local integration as a source of challenges that displaced persons are likely to face during their long term displacement. The basis of legal integration into the host society is a clear legal status. Displaced persons are often unable to carry or lose their certificates and proofs – documents that should be the basis of their cleared legal status in the host country.

The Estonian State manages many of its citizens' legal statuses electronically. Records of documents and certificates are stored digitally, in machine readable formats. So long as the e-Government infrastructure and related servers are operational, citizens' documents are going to be available online.

Their genuineness is guaranteed by digital signatures, and as such, the creation of fake electronic documents in implausible. In theory[11], the electronic availability of these documents could enable e-Citizens to establish their clarified legal status and prove their further legal claims, thus facilitating their legal integration into the host society.

For instance, citizens can view their education records and diplomas online (Eesti.ee, 2015), which might help them have their education and skills recognized by the host state, helping them to better career possibilities. They can access several of their health-related records (Eesti.ee, n.d., sec. Health Care and Protection) and records related to benefits (Eesti.ee, n.d., sec. Benefits and Social Assistance), which might not only render repeated medical examinations unnecessary and make receiving treatment quicker, it might help in re-establishing statuses of disability or reduced capacity to work. Legal cases concerning family reunification, marital issues, and heritage and alimony rights could be supported by a multitude of family-related datasets and services (Eesti.ee, n.d., sec. Family).

4.4 Continuous operation

In time of an armed conflict, conventional government services are often severely disrupted, or even seize to be offered completely (ICRC, 2015, pp. 17–19). Similarly, in case of a mass exodus caused by a natural (or anthropogenic) disaster, public services are often disrupted because of destroyed infrastructure, public buildings, or fatalities (Ibid.).

Assuming that the Data Embassy initiative was fully implemented and operational, e-Government services migrated to the government cloud could remain operational even during a

[11] In practice, however, the usage e-Citizens' digital documents and certificates to prove legal claims would require the host country to recognize the legal power of Estonian digital authentication methods' (i.e. digital signatures).

severe impairment of other governmental functions (Kotka and Liiv, 2015). Services that require the active, manual involvement of public servant (e.g. approving requests) could be provided with the condition that the public servant also has access to the online service environment (wherever they might be). Fully automated, autonomous or pro-active services (e.g. making queries to the e-Recipes environment, authentication using national ID cards, and the issuing of digital signatures) on the other hand could remain operational and fully functional – at least temporarily – even in a case of a severe disruption when no public servants are able to carry out their functions.

As I identified earlier in this chapter the Estonian e-Governance infrastructure has the technical potential of helping e-Citizens in re-establishing their identities, clarifying their legal statuses, and the potential of supporting the work of aid organizations by providing rich data sources to analyze. However, in practice, the technical realization of these potentials would require the continuous operation of the underlying infrastructural components. The Data Embassy concept is proposed specifically to guarantee continuous operation in scenarios (i.e. the Government's loss of control over the territory of Estonia (Kotka and Liiv, 2015, p. 152)) that are likely to trigger the displacement of people. Therefore I consider the full implementation of Data Embassies to be a prerequisite of the realization of the potentials identified above and classify Data Embassies as a key component of the Estonian e-Governance infrastructure in refugee emergency scenarios.

Obviously, not all the challenges that displaced persons and aid organizations face can be countered by the peculiarities of the Estonian e-Governance infrastructure. For instance, survival is a very physical challenge – no ICT solution can give protection from bullets, bad weather, or misfortune. While ICT solutions can help with resource management, at the end of the day, they cannot provide new resources themselves, when people in flight would need them.

5 Policy recommendation

In the previous chapter I pointed out that from a technological point of view, the Estonian e-Governance infrastructure has the potential to be used in novel ways to counter certain challenges of refugee emergencies. In this chapter I will propose one concrete Estonian policy recommendation to realize some of these potentials. I will introduce benefits and limitations of this policy recommendation, outline the legal and technological steps that implementing the policy would require, identify the communication challenges that need to be addressed, and explore its potentially beneficial country marketing and technology export implications.

As concluded in the previous chapter, aid organizations could use rich, digital databases and documents that concern displaced persons to better assess the challenges of the emergency and provide aid to the displaced persons more efficiently and effectively. Such databases and documents are currently not available to third parties, but the technological infrastructure of granting aid organizations access to these dataset, even if the country's integrity is severely disrupted, is available[12]. Therefore, my policy recommendation is the following:

> *In case of a national emergency that triggers the mass displacement of Estonian residents, make certain refugee-related, otherwise restricted governmental datasets accessible to international aid organizations.*

This policy would have benefits similar to open data[13] initiatives. Open data has a widely accepted benefit of enabling well informed, data-driven management and decision making in organizations (Davies and Bawa, 2012) (Manyika et al., 2013) (Kelkar et al., 2016). The United Nations specifically encourages the increased publishing and use of open data for helping people in vulnerable situations (United Nations, 2016, p. 3). However, unlike a usual open data policies, the implementation of this recommendation would provide an even wider breadth of data for the targeted support of the work of aid organizations in critical times; data that could not be made open to the general public, due to its sensitive nature.

[12] Assuming the implementation of the Data Embassy initiative.

[13] Open data: "machine-readable information, particularly government data, that's made available to others" (Manyika et al., 2013)

5.1 Legal framework

This policy recommendation has several legal implications. To implement this policy, the definitions and conditions of its subjects must be clarified. Laws or regulations that could serve as the legal bases of the policy also need to be identified; otherwise changes to laws and regulations that would enable the implementation of the policy shall be proposed.

First, the policy recommendation refers to a "national emergency" in which granting aid organizations access to relevant datasets could be considered. Therefore, when implementing this policy, the definition of "national emergency" and the conditions of granting access should be defined.

The conditions in which restricted databases could be granted access to aid organizations should be codified as law. The possibility of codifying these conditions as an amendment to the State of Emergency Act should be examined, since this Act is relevant to the policy recommendation: the purpose of the State of Emergency Act is to provide "the basis, conditions and procedure for declaration of a state of emergency, and the competence of authorities managing a state of emergency [and] the measures to be implemented during a state of emergency, and the rights, duties and liability of persons during a state of emergency" (Riigi Teataja, 1996, para. 1). In other words, this Act already addresses the question of what national emergency is, which institutions are responsible for decisions related to national emergencies, and provides a list of exceptional measures that are only valid in case of national emergencies.

An alternative approach of determining the conditions in which restricted databases could be granted access to could be using the national security model proposed by Kotka et al., (2016b, p. 107) to determine the operation modes of Data Embassies (the infrastructural components that are a prerequisite of this policy recommendation). This model makes distinction between *full control*, *fragile control* and *no control* operation modes of the Government Cloud; modes that are functions of the Estonian government's level of control over the country's territory, and the constraints that core technical and policy staff may have in accessing computer services (Ibid.).

Currently many of the Estonian governmental datasets, documents and other information that would be valuable for aid organizations are not accessible to them as open data, due to the protection of state secrets and personal privacy. Therefore, once the conditions of granting access to restricted databases are identified, the legal basis of granting aid organizations access to otherwise non-accessible personal data should be established.

The possibility of granting international aid organizations access to personal data without the explicit agreement of the citizens in question[14] should be examined in the context of the 14th paragraph of the Personal Data Protection Act. This Act is relevant to the policy recommendation since it states that the "communication of personal data or granting access to personal data to third persons for the purposes of processing is permitted without the consent of the data subject: 1) if the third person to whom such data are communicated processes the personal data for the purposes of performing a task prescribed by law, an *international agreement*[15] or directly applicable legislation of the Council of the European Union or the European Commission" (Riigi Teataja, 2008, para. 14). Estonia, as a member state of its Executive Committee, is in international agreements with UNHCR (UNHCR, 2014), which could be the legal basis of this policy.

As a sub-organization of the United Nations, with over 60 years of operation, presence in 123 countries and an active cooperation with Estonia (Lukosiunaite, 2014), UNHCR could be an ideal aid organization to whom restricted refugee-related datasets could be granted access to in case of emergencies. The possibility of granting UNHCR the right to further share these datasets with other organizations (based on their involvement and the relevance of their work assessed by the NARE checklist in the context of a concrete refugee emergency) could also be discussed.

As explained in Chapter 4, aid organizations might also benefit from the use data such as biometric data, data on the state of health or disability, data revealing ethnic or racial origin, or certain crime-related information. These data are classified as sensitive personal data (Riigi Teataja, 2008, para. 4), and as such cannot be granted access to based on paragraph 14 of the Personal Data Protection Act (Riigi Teataja, 2008, para. 14). Instead, sensitive personal data of individual displaced persons could be collected on the condition of their explicit consent (Riigi Teataja, 2008, para. 12), supporting the efforts of aid organization in providing better individualized services to displaced persons.

5.2 Technological considerations

If the legal framework of granting aid organizations access to restricted datasets in a refugee scenario is established, the technical accessibility and usability of these datasets and solutions supporting them must be assessed and guaranteed, in order to enable these organizations to fully take advantage of the data that has been made available to them.

[14] To be used for general demographic data analysis.
[15] Emphasis by the author.

The Estonian e-Governance infrastructure provides connectivity to and between datasets with the help of X-Road. X-Road has been one of the bases of the Estonian e-Governance infrastructure for over 15 years, and as a highly mature, reliable piece of technology, it could also serve as the facilitator for aid organizations, enabling them to connect and query databases that they are granted access to.

To maximize effectiveness of this policy recommendation, the aid organizations' efforts in developing solutions that query and analyze data from Estonian e-Governmental databases should be supported by making documentation, know-how and best practices produced and gathered by Estonian e-Governance professionals available to them. X-Road is a preferable choice from this perspective as well. The technical specification needed to implement X-Road for data exchange is publicly available, written in English (RIA, 2014), making it ideal for developers of international organizations.

An open source API solution has also been published as part of the effort of making the Estonian and Finnish implementation of X-Road connected and interoperable (EduCloud Alliance, 2016). The Java codebase is accessible to anyone under the European Union Public Licence, and offers documentation (Ibid.). As such, this code base can be a valuable example resource for developers of aid organizations working on accessing and analyzing data granted to the organization via X-Road.

Another solution has been published free of charge by the Estonian Centre of Registers and Information Systems, which aimed to make the development of .NET applications that interact with X-Road more efficient by automatically generating data objects based on the X-Road API (RIK, n.d.). This is highly beneficial, since the speedy development and deployment of code supporting the work of aid organizations is critical, due to the fact that time is an important factor in refugee crises (UNHCR, 2016, p. 1).

To further promote the possibility of quick deployment of X-Road-driven data analytics, the possibility of publishing examples of key datasets containing test content or content with obfuscated sensitive information should be examined. This would enable developers to build fully functioning information systems or data analytics solutions prior to a refugee emergency, enabling the use of X-Road-driven data in early responses to emergencies.

5.3 Communication and export implications

As argued earlier, the relevance of this work lies not in the likelihood of a national emergency, but the fact that the Estonian state is implementing measures to mitigate a hypothetic future national emergency (i.e. the Data Embassy project is meant to provide continuous

operation in case of loss of control over the country's territory (Kotka and Liiv, 2015, p. 152)). If this policy recommendation was implemented as law, the question of its relevance might also arise in the public discourse. Preparatory measures taken by the state to mitigate a future risk can bring the risk in the field of view of the public (Hansen and Nissenbaum, 2009, pp. 1158–1160), and might be interpreted as a sign of increased risk, potentially causing unwarranted public unease or panic. Therefore I think it is worth taking this in account when preparing the public communication regarding the policy's implementation.

As yet another novel, technology-driven public policy from Estonia, implementing this recommendation has the potential of further strengthening the country's international recognition for being a technological pioneer, which could also strengthen the country's position in international organization such as the UNHCR – as the precedent setting national cyber defense achievements cemented the country's position in NATO.

The State giving technological answers to non-technical questions is not a new approach to Estonians. The vision of a "country without borders", virtual e-Residents of Estonia from all over the world, along with a state that can care for its citizens even if it could not control its territory all have potentials to changing Estonians' understanding of fatherland, of the state, and of themselves.

E-Governance is still a new phenomenon – a concept that is being implemented and experimented with around the globe – and Estonia is one of the pioneers of it. The country has built up a mature and ubiquitous portfolio of e-Governance services, several technological companies, consultancy agencies and governmental institutions employ professionals who have created an extensive body of knowledge, know-how and best practices of designing, developing and operating e-Governance solutions. These technologies and the knowledge capacity is also relevant and valuable to other countries in their efforts of implementing ideal e-Governance. Estonia is capitalizing from these technologies and knowledge by exporting them; a process that is supported by Enterprise Estonia (EAS), a publicly funded business promotion foundation.

One of the infrastructural components enabling the benefits of this policy recommendation is X-Road. The technology of and the know-how on X-Road is also one of the e-Governance-related products that Estonia exports abroad. X-Road is being implemented, or is considered for implementation in a number of states and territories such as the Faroe Islands (e-Governance Academy, 2015a), Finland (EduCloud Alliance, 2016), Kyrgyzstan (e-Governance Academy, 2015b), Mauritius and the Indian Ocean Commission Member States (e-Governance Academy, 2015c), Namibia (e-Governance Academy, 2014) and Palestine (e-Governance Academy, 2015d).

Enabled by the implementation of X-Road, this policy recommendation could be considered by all of these countries and territories, especially if it was in the future combined with an initiative similar in nature to the Estonian Data Embassy initiative, guaranteeing continuous operation. The recommendation could especially be relevant to countries who have historical or present struggles with displaced persons, as does Namibia (UNHCR, 2002b) and Palestine (Chalabi, 2013).

Consequently, the benefits of this policy recommendation could be used as an additional argument in the marketing and sales process of technologies and know-how related to X-Road, potentially positively stimulating the Estonian ICT export sector.

In conclusion, the disrupting the contemporary understanding of democratic processes by successful implementation of Internet voting, by rethinking the roles of state and citizens by opening up e-Estonia to citizens of any country via the e-Residency program, by making precedent in international law with the novel concept of Data Embassies, and by using the phrase "country without a territory" not as science fiction utopia, but as a vision, Estonia has been challenging the rest of the world's understanding on the nature and functions of government, statehood, citizenry, and technology. Estonians seem to have no problem with disruptive changes in fields where the rest of the world struggles to innovate. This is why I think, that even though it poses unprecedented legal challenges, this policy could be successfully implemented, providing an additional layer of insurance of the safety of the people of Estonia.

6 Summary and conclusions

This research has shown that the challenges that displaced persons and aid organizations face during displacement are complex and multifaceted. In the second chapter, I analyzed how physical dangers, lack of resources and information, coordination, communication, political, legal and identification-related issues all have different implications to the lives of displaced persons and the work of aid organizations.

Next, I identified the Estonian e-Governance infrastructure's main intangible components as X-Road, the public key infrastructure (PKI), digital identity and the Governmental Cloud and Data Embassies initiatives. I outlined the key features of these components: how X-Road makes the entire infrastructure interoperable and links services and databases in a secure way, that PKI lets e-Citizen identify themselves electronically and issue digital signatures, how the abundance of digitized personal data, the interoperability of X-Road and the citizens' personal codes make rich digital profiles, and how the Governmental Cloud and Data Embassy initiatives provide continuous operation even if the country's territorial integrity is breached.

Once the challenges of displacement and the features of the Estonian e-Governance infrastructure are determined, I identified ways in which some of these components could be used to counter certain challenges of displacement. I found that the digital profiles of e-Citizens could technically be used to re-establish the identities of displaced e-Citizens who have lost their conventional forms of identification. I also found that the rich digitized databases linked by X-Road could enable aid organizations to make better informed, data-driven decisions. I determined that the online availability of authentic information about citizens could help clarify displaced persons' legal status and thus facilitate their integration into the host community. Finally, I established the key role of the Data Embassy initiative that is enabling other components' benefits by providing continuous operation of the Estonian e-Governance throughout a refugee emergency.

I concluded my work by proposing a policy that could enable the Estonian e-Governance infrastructure's benefits to be used in a refugee emergency. I argued that granting aid organizations access to certain – otherwise restricted – refugee-related datasets in a national emergency would allow them to make better informed, data-driven decisions. I proposed a legal framework for this policy: the conditions in which datasets could be granted access to could be codified as part of the State of Emergency Act. I also identified the sections of the Personal Data Protection Act that could provide legal basis for granting aid organizations access to datasets

containing personal data. I assessed the technical requirements of implementing the proposed policy, and found that the essential requirements are already met. Finally, I explored the communication and export-related implications of implementing the policy recommendation, identifying the possibility of the public misinterpreting the policy implementation as a reaction to a threat, pointing out the national identity strengthening potential of the policy, and its possible benefits to technology export.

6.1 Limitations and future work

In my work, I am considering a scenario where a mass of people become displaced due to an armed conflict, but the principles of my findings should apply to mass exodus scenarios triggered by natural or anthropogenic disasters as well. I am not considering such a scenario where the reason for the displaced persons fleeing is the actions of their own government (i.e. the government violating their citizens' human rights, ethnic cleansing or population transfer), since in such events the government will not want help the cases of these individuals – it will not want to offer public services to them.

Similarly, another prerequisite to realizing the potential benefits of the Estonian e-Governance infrastructure and my policy recommendation is that aid organizations would be willing to work with technology and adopt data-driven decision making processes, and that host countries would recognize the legal power of Estonian e-Governance solutions.

This work does not offer a comprehensive overview the challenges of displacement; it studies the challenges that displaced persons and aid organizations face, in three distinct stages of displacement (flight from conflict zones, temporary displacement, and integration in permanent displacement). In future works, the potential of the Estonian e-Governance infrastructure in supporting e-Citizens and aid organizations in other stages of displacement could be examined.

In my view studying the uses of the Estonian e-Governance infrastructure in the context of the Estonian diaspora would have the potential to yield interesting findings. The challenges of the diaspora differ from those of displaced persons, but the two topics are interrelated. If we view the permanent displacement of persons not as a process of individuals, but as a societal process, we will arrive to topic of diaspora – the communities of people far from the national homeland (Pierre, 2013). Some nations have widespread diasporas that have well managed, highly functional relationships with the home country. In the case of Armenia, the diaspora is a significant boosting factor of the national economy, and members of the diaspora are important representatives of the nation's interest around the globe (Gevorkyan, 2016). In this respect, the diaspora has similar effects than what the Estonian e-Residency program would like to achieve

(Shabbir, 2014). E-Governance could be a tool also used for diaspora management, perhaps by integrating diaspora management efforts with the e-Residency program.

6.2 Conclusions

The idea behind the Data Embassy initiative is to achieve the continuous operation of the Estonian e-Governance, so even if the government lost power, even if the country's border were breached, even if its sovereignty diminished, the core operation of the government could continue, and Estonia's symbolic and constitutional integrity could live on in an extended, intangible digital form. The goal of continuous operation is clearly pronounced in the literature and in governmental communication. However, I thought it was also worth taking a look if there were some other, more practical implications of these key governmental functions that could be take advantage of during a worst case scenario.

My work shows that the Estonian e-Governance could provide real life, practical help to those who are perhaps in the most vulnerable positions in a national crisis – those who leave everything behind to seek refuge. It could help people who lost their identification while fleeing from danger by proving their identities to foreign states, granting them entry to safety. It could save their medical records thus helping them get better medical care. It would keep their legal documents, certifications, and licenses, so they could go back to school quicker, enter the work force easier – it would help them find solid ground under their feet in their new host countries.

Estonian e-Governance could also help international aid organizations who give essential support to these refugees by providing them with plenty of valuable detailed information on the refugees' backgrounds. Aid organizations could use this information to understand the complex situation they are working in, and make data-driven decisions on how to help refugees in the best possible way.

These potential benefits are inherent of the Estonian e-Governance infrastructure. Once the Data Embassies initiative is realized, all the necessary technological components will exist, and no expensive additional development would be needed to take advantage of e-Governance to the benefit of the citizenry. The legal basis of using e-Governance to help those who had to flee the country also exists. The concept of providing aid organizations with restricted data to be used to help Estonian residents in displacement could be turned into a policy, just how the concept of Data Embassies – the very concept enabling this suggestion – was turned into a policy, and is being implemented.

7 Bibliography

Aasmäe, K., 2014. Estonia to establish digital embassies. Postimees.

Adams, C., Lloyd, S., n.d. Core PKI Services: Authentication, Integrity, and Confidentiality. Microsoft TechNet. https://technet.microsoft.com/en-us/library/cc700808.aspx (accessed 12.2.16).

Ager, A., Strang, A., 2008. Understanding Integration: A Conceptual Framework. J. Refug. Stud. 21, 166–191.

Al Jazeera, 2015. The billion-dollar business of refugee smuggling. http://www.aljazeera.com/programmes/countingthecost/2015/09/billion-dollar-business-refugee-smuggling-150913113527788.html (accessed 12.4.16).

Ashmore, W.C., 2009. Impact of Alleged Russian Cyber Attacks (Monograph No. ADA504991). School of Advanced Military Studies, Fort Leavenworth, Kansas.

BBC News, 2016. Paris attacks: Who were the attackers?. http://www.bbc.com/news/world-europe-34832512 (accessed 11.24.16).

Bengtsson, S., 2012. Virtual Technologies of the Nation-State: State Administration in Second Life, in: Cultural Technologies: The Shaping of Culture in Media and Society. Routledge, New York.

Buchan, R., 2016. The Syrian Refugee Crisis: A Greenhouse for Human Trafficking. Hum. Rights First. http://www.humanrightsfirst.org/blog/syrian-refugee-crisis-greenhouse-human-trafficking (accessed 12.7.16).

Castles, S., Korac, M., Vasta, E., Vertovec, S., 2001. Integration: Mapping the field. Home Off. Online Rep. 29, 115–118.

Center of Registers and Information Systems, n.d. e-Land Register. http://www.rik.ee/en/e-land-register (accessed 12.3.16).

Central Intelligence Agency, n.d. The World Factbook: Estonia. https://www.cia.gov/library/publications/the-world-factbook/geos/en.html (accessed 5.27.15).

Chalabi, M., 2013. What happened to history's refugees?. The Guardian. http://www.theguardian.com/news/datablog/interactive/2013/jul/25/what-happened-history-refugees (accessed 12.5.16).

Clayton, J., 2015. UNHCR chief issues key guidelines for dealing with Europe's refugee crisis. UNHCR. http://www.unhcr.org/news/latest/2015/9/55e9793b6/unhcr-chief-issues-key-guidelines-dealing-europes-refugee-crisis.html (accessed 11.26.16).

Council of Europe, 2004. e-Governance. https://www.coe.int/t/dgap/democracy/Activities/GGIS/E-governance/Default_en.asp (accessed 12.10.16).

Crawford, N., Cosgrave, J., Haysom, S., Walicki, N., 2015. Protracted displacement: uncertain paths to self-reliance in exile. ODI. https://www.odi.org/publications/9906-refugee-idp-displacement-livelihoods-humanitarian-development (accessed 11.2.16).

Crisp, J., Long, K., 2016. Safe and Voluntary Refugee Repatriation: From Principle to Practice. J. Migr. Hum. Secur. 4, 141–147.

Cybernetica, 2013. X-Road eGovernment interoperability framework. https://cyber.ee/uploads/2013/03/cyber_xroad_NEW2_A4_web.pdf

Davies, T.G., Bawa, Z.A., 2012. The Promises and Perils of Open Government Data (OGD). J. Community Inform. 8.

Dutta, S., 2006. Estonia: A Sustainable Success in Networked Readiness? Glob. Inf. Technol. Rep. 2007, 81–90.

EduCloud Alliance, 2016. Joint X-Road REST Gateway development. GitHub. https://github.com/educloudalliance/xroad-rest-gateway (accessed 12.9.16).

Edwards, A., Savary, M., 2016. Mediterranean death toll soars in first 5 months of 2016. UNHCR. http://www.unhcr.org/news/latest/2016/5/574db9d94/mediterranean-death-toll-soars-first-5-months-2016.html (accessed 12.4.16).

Eesti.ee, 2015. Data from the Estonian Education Information System (EHIS). https://www.eesti.ee/eng/services/citizen/haridus_ja_teadus/isikukaart_eesti_ee_portaali (accessed 12.8.16).

Eesti.ee, n.d. Services and forms for a citizen. https://www.eesti.ee/eng/services/citizen (accessed 12.8.16).

e-Estonia, 2016. e-Estonia homepage. https://e-estonia.com/ (accessed 11.22.16).

e-Estonia, 2015. Components. https://e-estonia.com/components/ (accessed 12.2.16).

e-Estonia, n.d. X-Road. http://e-estonia.com/component/x-road/ (accessed 4.2.14).

e-Governance Academy, 2015a. Support to e-Government Development of Faroe Islands. http://www.ega.ee/project/support-to-e-government-development-of-faroe-islands/ (accessed 12.10.16).

e-Governance Academy, 2015b. e-Governance Academy signed a Memorandum of Understanding to develop X-road in Kyrgyzstan. http://www.ega.ee/news/e-governance-academy-signed-contract-to-develop-x-road-in-kyrgyzstan/ (accessed 12.10.16).

e-Governance Academy, 2015c. Estonian X-road and digital identity will be implemented in Mauritius and in the Indian Ocean Commission Member States. http://www.ega.ee/news/estonian-x-road-and-digital-identity-will-be-implemented-in-mauritius-and-in-the-indian-ocean-commission-member-states/ (accessed 12.10.16).

e-Governance Academy, 2015d. E-services and X-road in Palestine. http://ega.ee/project/e-services-and-x-road-in-palestine/ (accessed 12.10.16).

e-Governance Academy, 2014. Estonia to construct secure data exchange layer X-Road for Namibia. http://www.ega.ee/news/estonia-to-construct-secure-data-exchange-layer-similar-to-x-road-for-namibia/ (accessed 12.10.16).

Ender, M.G., 2010. War causes and consequences. Contemp. Sociol. J. Rev. 39, 399–402.

ENISA, 2013. Good Practice Guide for securely deploying Governmental Clouds. https://www.enisa.europa.eu/publications/good-practice-guide-for-securely-deploying-governmental-clouds (accessed 11.28.16).

Estonian National Electoral Committee, 2010. E-Voting System - General Overview. http://vvk.ee/public/dok/General_Description_E-Voting_2010.pdf (accessed 11.30.16).

European Commission, 2015. eGovernment in Estonia.

Gates, S., Hegre, H., Nygård, H.M., Strand, H., 2012. Development Consequences of Armed Conflict. World Dev. 40, 1713–1722.

Gevorkyan, A.V., 2016. Development through Diversity: Engaging Armenia's New and Old Diaspora. Migr. Policy Inst. http://www.migrationpolicy.org/article/development-through-diversity-engaging-armenias-new-and-old-diaspora (accessed 12.11.16).

Gillespie, M., Ampofo, L., Cheesman, M., Faith, B., Iliadou, E., Issa, A., Osseiran, S., Skleparis, D., 2016. Mapping Refugee Media Journeys - Smartphones and Social Media Networks. The Open University and France Medias Monde.

Hansen, L., Nissenbaum, H., 2009. Digital Disaster, Cyber Security, and the Copenhagen School. Int. Stud. Q. 53, 1155–1175.

Harding, L., 2015. Hungarian police arrest driver of lorry that had 71 dead migrants inside. The Guardian. https://www.theguardian.com/world/2015/aug/28/more-than-70-dead-austria-migrant-truck-tragedy (accessed 12.4.16).

ICRC, 2015. Urban services during protracted armed conflict - A call for a better approach to assisting affected people (Report).

Kelkar, M., Viechnicki, P., Conlin, S., Frey, R., Strickland, F., 2016. Mission analytics - Data-driven decision making in government. Deloitte Univ. Press. https://dupress.deloitte.com/dup-us-en/industry/public-sector/data-driven-decision-making-in-government.html (accessed 12.9.16).

Kotka, T., Johnson, B., Cebul, T., Lovosevic, L., Liiv, I., 2016a. E-Government Services Migration to the Public Cloud: Experiments and Technical Findings, in: Electronic Government and the Information Systems Perspective. Springer International Publishing, pp. 62–76.

Kotka, T., Kask, L., Raudsepp, K., Storch, T., Radloff, R., Liiv, I., 2016b. Policy and Legal Environment Analysis for e-Government Services Migration to the Public Cloud, in: Proceedings of the 9th International Conference on Theory and Practice of Electronic Governance, ICEGOV '15-16. ACM, New York, NY, USA, pp. 103–108.

Kotka, T., Liiv, I., 2015. Concept of Estonian Government Cloud and Data Embassies, in: Kő, A., Francesconi, E. (Eds.), Electronic Government and the Information Systems

Perspective, Lecture Notes in Computer Science. Springer International Publishing, pp. 149–162.

Lopes, C., Theisohn, T., 2003. Ownership, leadership, and transformation: can we do better for capacity development? Earthscan Publications, London and Sterling, Virginia.

Lukosiunaite, A.A., 2014. History and activities of the UNHCR in Estonia and worldwide. Est. Hum. Rights Cent. https://humanrights.ee/en/2014/03/history-and-activities-of-the-unhcr-in-estonia-and-worldwide/ (accessed 12.9.16).

Manyika, J., Chui, M., Farrell, D., Kuiken, S.V., Groves, P., Doshi, E.A., 2013. Open data: Unlocking innovation and performance with liquid information. McKinsey Glob. Inst. http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/open-data-unlocking-innovation-and-performance-with-liquid-information (accessed 12.9.16).

McCluskey, M., 2015. Estonia redefines national security in a digital age. Al Jazeera. http://www.aljazeera.com/indepth/features/2015/03/estonia-redefines-national-security-digital-age-150318065430514.html (accessed 11.28.16).

Mekhennet, S., Booth, W., 2015. Migrants are disguising themselves as Syrians to enter Europe. Wash. Post. https://www.washingtonpost.com/world/europe/migrants-are-disguising-themselves-as-syrians-to-gain-entry-to-europe/2015/09/22/827c6026-5bd8-11e5-8475-781cc9851652_story.html (accessed 11.24.16).

Mell, P., Grance, T., 2011. The NIST Definition of Cloud Computing.

Microsoft, 2003. PKI Technologies: Public Key; Security Services. Microsoft TechNet. https://technet.microsoft.com/en-us/library/cc779826(v=ws.10).aspx (accessed 12.2.16).

Microsoft, MKM, 2015. 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.

Ministry of the Interior, 2016. Population Register. https://www.siseministeerium.ee/en/population-register (accessed 12.3.16).

MKM, 2014. Cyber Security Strategy 2014-2017.

MKM, 2013. Digital Agenda 2020 for Estonia.

OECD, 2002. E-government: Analysis Framework and Methodology.

Pierre, J., 2013. Diaspora. Oxf. Bibliogr. http://www.oxfordbibliographies.com/view/document/obo-9780199766567/obo-9780199766567-0091.xml (accessed 12.11.16).

Prettitore, P., 2016. The legal problems of refugees. Brook. Inst. https://www.brookings.edu/blog/future-development/2016/02/04/the-legal-problems-of-refugees/ (accessed 11.2.16).

Provost, F., Fawcett, T., 2013. Data Science and its Relationship to Big Data and Data-Driven Decision Making. Big Data 1, 51–59.

RIA, 2016. Introduction of X-Road. https://www.ria.ee/en/introduction-of-xroad.html (accessed 12.2.16).

RIA, 2014. Protocol for Data Exchange Between Databases and Information Systems - Requirements for Information Systems and Adapter Servers.

Riigi Teataja, 2008. Personal Data Protection Act, RT I 2007, 24, 127.

Riigi Teataja, 1996. State of Emergency Act, RT I 1996, 8, 165.

RIK, n.d. X-Road generator. Cent. Regist. Inf. Syst. http://www.rik.ee/en/other-services/x-road-generator (accessed 12.9.16).

Runnel, P., Pruulmann-Vengerfeldt, P., Reinsalu, K., 2009. The Estonian Tiger Leap from Post-Communism to the Information Society: From Policy to Practice. J. Balt. Stud. 40, 29–51.

Saparniene, D., 2013. From e-Government to e-Governance: e-Initiatives in Europe. Siauliai University, Lithuania.

Segue Technologies, 2013. The Three Stages of Disaster Recovery Sites. Segue Technol. http://www.seguetech.com/three-stages-disaster-recovery-sites/ (accessed 11.28.16).

Sertifitseerimiskeskus, 2016. ID-card and Digi-ID. ID.ee. http://www.id.ee/index.php?id=30500 (accessed 12.3.16).

Sertifitseerimiskeskus, 2003. The Estonian ID Card and Digital Signature Concept - Principles and Solutions. http://www.id.ee/public/The_Estonian_ID_Card_and_Digital_Signature_Concept.pdf (accessed 12.3.16).

Shabbir, N., 2014. Estonia offers e-residency to foreigners. the Guardian. http://www.theguardian.com/world/2014/dec/26/estonia-offers-e-residency-to-world-what-does-it-mean (accessed 5.27.15).

Spiegel, 2014. Europe's African Refugee Crisis: Is the Boat Really Full?. Spieg. Online. http://www.spiegel.de/international/europe/european-refugee-crisis-worsens-in-mediterranean-a-964304.html (accessed 11.26.16).

Thomas, C., 2015. What You Need to Know About Europe's Refugee Crisis: Q&A. Bloomberg.com. http://www.bloomberg.com/news/articles/2015-09-08/what-you-need-to-know-about-europe-s-refugee-crisis-q-a (accessed 11.26.16).

Thurnay, L., 2014. E-Governance and cyber security in Estonia (BA thesis). Budapesti Kommunikációs és Üzleti Főiskola, Budapest.

Tomkiw, L., 2015. European Refugee Crisis 2015: Why So Many People Are Fleeing The Middle East And North Africa. Int. Bus. Times. http://www.ibtimes.com/european-refugee-crisis-2015-why-so-many-people-are-fleeing-middle-east-north-africa-2081454 (accessed 11.26.16).

UNESCO, n.d. Displaced Person / Displacement. http://www.unesco.org/new/en/social-and-human-sciences/themes/international-migration/glossary/displaced-person-displacement/ (accessed 11.27.16a).

UNESCO, n.d. Migrant. http://www.unesco.org/new/en/social-and-human-sciences/themes/international-migration/glossary/migrant/ (accessed 12.4.16b).

UNHCR, 2016. Needs assessment for refugee emergencies (NARE) checklist.

UNHCR, 2015. Biometric Identity Management System - Enhancing Registration and Data Management.

UNHCR, 2014. Global Report 2014.

UNHCR, 2013. A New Beginning: Refugee Integration in Europe.

UNHCR, 2011. Handbook on Procedures and Criteria for Determining Refugee Status under the 1951 Convention and the 1967 Protocol relating to the Status of Refugees.

UNHCR, 2002a. Local Integration (No. EC/GC/02/6), Global Consultations on International Protection.

UNHCR, 2002b. UNHCR starts repatriating Namibian refugees in Botswana. http://www.unhcr.org/news/latest/2002/8/3d5935ac4/unhcr-starts-repatriating-namibian-refugees-botswana.html (accessed 12.10.16).

United Nations, 2016. E-Government survey 2016 - e-Government in support of sustainable development.

United Nations, 1963. Vienna Convention on Consular Relations.

United Nations, 1961. Vienna Convention on Diplomatic Relations.

United Nations, n.d. Human Development Index and its components. UNDP Open Data. https://data.undp.org/dataset/Table-1-Human-Development-Index-and-its-components/wxub-qc5k (accessed 3.25.14).

Vabariigi Valitsus, 2016. Infoühiskonna valdkonna arengukava "Eesti Infoühiskonna Arengukava 2020" rakendusplaan aastateks 2016-2019. https://valitsus.ee/sites/default/files/content-editors/arengukavad/infouhiskonna_arengukava_rakendusplaan_2016-2019.xlsx (accessed 11.28.16).

Van Hear, N., Bakewell, O., Long, K., 2012. Drivers of Migration.

Wæver, O., 1995. Securitization and Desecuritization, in: On Security. Columbia University Press, pp. 46–87.