The Potential of the Estonian e-Governance Infrastructure in Supporting Displaced Estonian Residents

Lőrinc Thurnay[1(✉)], Benjamin Klasche[2], Katrin Nyman-Metcalf[1], Ingrid Pappel[1], and Dirk Draheim[1]

[1] Tallinn University of Technology, Akadeemia tee 15a, 12618 Tallinn, Estonia
thlorinc@gmail.com,
{katrin.nyman-metcalf,ingrid.pappel,dirk.draheim}@ttu.ee
[2] Tallinn University, Narva mnt 25, 10120 Tallinn, Estonia
benjamin.klasche@tlu.ee

Abstract. This paper examines the possibilities of using the Estonian e-Governance infrastructure in an innovate manner to help displaced Estonian residents in a hypothetical national emergency. We 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. On this basis we analyze how the Estonian e-Governance infrastructure can be used in a refugee emergency. We provide a definition of intangible e-Governance infrastructure. We identify the key component of the existing Estonian e-Governance infrastructure as well as the proposed Governmental Cloud and Data Embassy initiatives. We analyze linkages where the utilization of the infrastructure could potentially counter the challenges of displaced persons and aid organizations. To realize these linkages, we propose a policy to make certain refugee-related, otherwise restricted governmental datasets accessible to international aid organizations. Additionally, we introduce a legal framework for the policy, analyze the technological requirements of its implementation, and discuss its communicational and technology export-related implications.

Keywords: Data embassy · Displacement · e-Governance infrastructure · National emergency · Policy recommendation · Refugee · UNHCR

1 Introduction

Estonia can be considered a pioneering country in ICT and e-Governance solutions [17,18]. In the last 25 years, Estonia introduced a number of unprecedented new technology-driven solutions in the public sector, such as Internet voting [7], nation-wide digital signatures [20] and the e-Residency program [12]. 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

A. Kő and E. Francesconi (Eds.): EGOVIS 2017, LNCS 10441, pp. 236–250, 2017.
DOI: 10.1007/978-3-319-64248-2_17

services would remain functional even if the country's territorial integrity was breached [15]. The idea of the Data Embassy initiative is 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. This is a new element of the idea of exile governments. It is not the aim of this work to assess the likelihood of such a scenario. However as the Estonian Government has made this topic a relevant matter of national security it does not need further explanations from our side.

The main questions that we will discuss in this paper are if and how displaced persons with Estonian digital identities can be supported by the Estonian e-Government infrastructure and what the challenges are that displaced persons and organizations aiding them face. In this discussion, we will identify what are the components of the Estonian e-infrastructure that are relevant to the challenges of displaced persons and aid organizations and what steps could be taken to enable the relevant components to be used to counter the challenges. This discussion will be of wider interest than just for Estonia, as many countries are inclined to build an e-Governance structure based on the Estonian e-Governance model. To answer these questions, we use qualitative data analysis methods and data sets. This is mostly, due to the lack of large quantitative datasets available on several of the subject matters, and most notably on the topic of Data Embassies [15], which is a project in its early pilot phases. All results in this paper are outcome of the research conducted for a Master Thesis by Thurnay [23].

In Sect. 2, we look at the challenges that displaced persons and aid organizations face throughout different stages of displacement. Following that, Sect. 3 discusses components and features of the Estonian e-Governance infrastructure. In Sect. 4, we attempt to define linkages between the infrastructural features and the challenges of displaced persons and aid organizations discussed in the previous sections. Based on this, we make a policy recommendation to realize the potential benefits identified in Sect. 5. Finally, we make some concluding remarks in Sect. 6.

2 Challenges of Displaced Persons and Aid Organizations

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 other non-traditional security threats, such as the weather. We 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.

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 conflict is resolved. The first set of challenges they face is during the flight away from their homes to safety. The most prominent challenges that displaced persons might face are:

- 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 [9]. Up-to-date and reliable information is vital for refugees in planning their journeys, which are often dangerous [9].
- 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 [8], large numbers of people who 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.
- Communication. During their time in transit, refugees have the need to communicate: with authorities; 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 [9].

The challenges that refugees face during flight are many. 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 deal with. We 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 arriving at a place that is safe and stable enough for aid organizations to be able to offer help in people's displacement.

2.2 Emergency Response of Aid Organizations

Just as every region, refugee crisis and every individual refugee faces different challenges during flight, also organizations aiding refugees 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 [24]. 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 the refugees pose, and to suggest actions based on these assessments. The checklist is designed to be general enough, and customizable so it could be applied effectively in any refugee scenario. The NARE checklist suggests using several methodologies to assess the nature and severity of refugee crises. Based on the content of and the methodologies suggested by the NARE checklist, we 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 (water, sanitation, hygiene, 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 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.

We 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.

2.3 Legal Integration into Host Societies

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 and 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 only use up resources. If we consider the goal of integration as being included in the host society, the purpose of the legal process leading to integration is to have similar legal status or rights that the members of the host community have.

Integration presupposes certain legal steps, primarily in order to determine the identity of persons based on which a clear legal status for the displaced person can be established. This can best be achieved with the help of documents, proofs and certificates that verify the identity and provide a basis for any claims made. Re-establishing and preserving identities is key to ensuring protection and solutions for refugees [25]. The lack of documents due to losing them during transit or the inability to carry them around is a critical issue in establishing a clarified legal status [27]. Host states enforce the identification of incoming refugees and displaced persons because taking in people with unclear identities carries risks. Missing legal documents, proofs, and certificates make legal proceedings in the host country challenging, since supplementing them is often impossible due to the disruption of the home state and lost identities of the displaced persons. These people fleeing persecution are often unable to contact home state authorities. These challenges are further aggravated by the fact that the legal requirements might differ significantly between the home country and the host country. Apart from having to prove their identity, legal issues displaced persons face can typically be, but are not limited to, family-related issues (marriage, children), issues related to ownership, labor-related issues and certifications, health problems, or criminal cases. Legal proceedings in such situations can be problematic if the legal history of the involved parties is missing [27].

3 Estonian e-Governance Infrastructure Components

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 that face end users are based. In this work, we chose to study infrastructure in the non-tangible sense. This decision was made based on 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 striking distinction of the Estonian e-Governance are found in the intangible components. The key components are:

– X-Road is a distributed, secure, unified web-services based inter-organizational data exchange framework [1], 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 [1].
- Public Key Infrastructure. In the Estonian national PKI, every e-Citizen[1] 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.
- eID. Every e-Citizen 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 citizen's personal code, therefore the personal code is also a basis of the citizens' digital identities, or electronic identities (eID).

In addition to the key components, we also identified the Government Cloud and Data Embassies project [15] 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 a considerable role in the infrastructure. Many European countries, including Estonia, have concluded that features of cloud computing such as rapid elasticity, continuous operation, location independence could be used as the infrastructural basis of their e-Government services [15]. However, the assessment of the possibility of implementing governmental cloud in Estonia shows that the ubiquitous service portfolio, the advanced Estonian 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 [15]. These peculiarities of the Estonian e-Government system were the basis of the Concept of the Estonian Government Cloud and Data Embassies [15], which considers three main technological components, i.e., 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 [6].
- Public clouds – 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

[1] Throughout this work the term e-Citizen is used to refer to people who hold Estonian digital identification and profile: Estonian citizens, residents of Estonia, and Estonian e-residents.

to better guarantee their availability, e.g., the website of the President or the Government [13,16]. The possibility of migrating sensitive data to public cloud services – despite the inherent security risks – which would allow to guarantee digital continuity in case the territorial integrity of the country is breached, is also discussed [15].
– Data embassies – to combine the benefits of a territorial cloud infrastructure, i.e., exclusive control over the cloud infrastructure, with the benefits of using multinational private cloud providers – i.e., 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 [15].

4 Estonian e-Government Infrastructure Components Relevant to Issues of Refugees and Aid Organizations

4.1 (Re-)Establishment of Identities of Displaced Persons

In Sect. 3 we 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 displaced persons who lost their identity document provide 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[2] of e-Citizens have the potential to be used to re-establish the identities of displaced e-Citizens who have lost their identification documents.

Even if the identification document of the displaced person in question is available, the possibility of performing biometric identification provides an 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 [25]. Being able to use the already established

[2] Digital profiles of e-Citizens maintained by the state differs from digital profiling carried out by social media providers such as Facebook, the latter not having the potential to be used to re-establish identities of displaced persons, since they are not verified by the state and carry no legal authenticity.

biometric identity of an e-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, it 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 Sect. 2 we found that in order 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, the home and host country's population, geography, economy, as well as qualitative data from interviews and focus groups and field reports are needed. The Estonian e-Governance has a high degree of maturity, and most state and public registers and databases as well as documents are managed in digitized, standardized formats, linkable by X-Road. In theory, these databases could be sources for rich, quantitative data of demographics with information on the population health and education that could support aid organizations in their efforts to understand the complex challenges they are facing.

Given that the identities of displaced persons' normally 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 community could be used to create detailed profiles to help in identifying not only community key informants and ideal focus group discussion participants, 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 concerns. With conventional methods, 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.

4.3 Supplementing Missing Documents

Above, we identified the legal dimension of local integration as a challenge that displaced persons are likely to face during their long term displacement. The prerequisite of legal integration into the host society is a clear legal status. Displaced persons are often unable to carry certificates and proofs – documents that should be the basis of their cleared legal status in the host country – or lose them during the displacement. 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, the electronic availability of 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 [4], which might help them to 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 [5] and records related to benefits, 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.

4.4 Continuous Operation

In time of an armed conflict, conventional government services are often severely disrupted, or even seize to be offered completely [11]. Assuming that the Data Embassy initiative would be fully implemented and operational, e-Government services migrated to the government cloud could remain operational even during a severe impairment of other governmental functions [15]. Services that require the active, manual involvement of a 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.

The Estonian e-Governance infrastructure has the technical potential of helping e-Citizens in re-establishing their identities, clarifying their legal status, and the potential of supporting the work of aid organizations by providing rich data sources to analyze. However, in practice, the technical realization of such potential would require the continuous operation of the underlying infrastructural components. The Data Embassy concept is proposed specifically to guarantee continuous operation in scenarios that are likely to trigger the displacement of people, i.e., the Government's loss of control over the territory of Estonia [15]. Therefore, we consider the full implementation of data embassies to be a prerequisite of the realization of the potential identified above and classify data embassies as a key component of the Estonian e-Governance infrastructure in a refugee emergency scenario.

5 Policy Recommendations

As concluded above, 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. Therefore, our policy recommendations are the following:

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

This policy would have benefits similar to open data initiatives. Open data has the widely accepted benefit of enabling well informed, data-driven management and decision-making in organizations [2]. The United Nations specifically encourages the increased publishing and use of open data for helping people in vulnerable situations [28]. However, unlike usual open data policies, the implementation of our 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.

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. The conditions in which aid organizations could be granted access to restricted databases should be codified in 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, compare with [22], Sect. 1. In other words, this Act already addresses the question of what a 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. Similar legislation exists in most countries, which is why our recommendations can be relevant in the future also elsewhere, in countries that may develop similar e-governance to Estonia.

An alternative approach of determining the conditions in which access could be granted to restricted databases could be using the national security model proposed by Kotka et al. [14] to determine the operation modes of Data Embassies, i.e., the infrastructural components that are a prerequisite of this policy recommendation. This model makes a 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.

The possibility of granting international aid organizations access to personal data without the explicit agreement of the citizens in question should be examined in the context of section 14 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 or directly applicable legislation of the Council of the European Union or the European Commission, compare with [21] section 14. Estonia, as a member state of its Executive Committee, has international agreements with UNHCR [26], 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, UNHCR could be an ideal aid organization to whom access could be granted to restricted refugee-related datasets in case of emergencies. The possibility of granting UNHCR the right to further share these datasets with other organizations could also be discussed – based on their involvement and the relevance of their work assessed by the NARE checklist in the context of a concrete refugee emergency. It is not unusual that explicit consent is not needed for data use provided it is for the purpose of carrying out a task of public interest or in the interest of the individual, which is set out in law or in other form – such as an international agreement.

As explained in Sect. 4, aid organizations might also benefit from the use of 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, compare with [21], section 4, and as such cannot be granted access to based on section 14 of the Personal Data Protection Act, compare with [21], section 14. Instead, sensitive personal data of individual displaced persons could be collected on the condition of their explicit consent, compare with [21], section 12, supporting the efforts of aid organization in providing better individualized services to displaced persons. In exceptional circumstances there may be a possibility to collect data also without explicit consent, but this issue will not be further discussed here as it is a major topic in its own right and not necessary for the main argument of this article.

5.2 Technological Considerations

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 our 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 [19], 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 [3]. The Java codebase is accessible to anyone under the European Union Public Licence, and offers documentation. 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.

5.3 Communication and Export Implications

As argued earlier, the relevance of this work lies not in the likelihood of a national emergency, but in 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 [15]. 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 [10], and might be interpreted as a sign of increased risk, potentially causing unwarranted public unease or panic. Therefore, we think it is worth taking this into 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 organizations such as the UNHCR – just as the precedent setting national cyber defense achievements cemented the country's position in NATO. 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 are some of the e-Governance-related products that Estonia exports abroad. X-Road is being implemented in a number of states and territories. 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 do Namibia and Palestine – countries that have implemented or are in the process of implementing features of the X-Road, with Estonian help. 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.

6 Conclusion

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, we think that it is also worth taking a look at whether there are some other, more practical implications of these key governmental functions that could be taken advantage of during a worst case scenario.

This paper 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 like the concept of Data Embassies – the very concept enabling this suggestion – was turned into a policy, and is being implemented.

References

1. Cybernetica: X-Road eGovernment Interoperability Framework (2013). https://cyber.ee/uploads/2013/03/cyber_xroad_NEW2_A4_web.pdf
2. Davies, T.G., Bawa, Z.A.: The Promises and Perils of Open Government Data (OGD). J. Commun. Inform. **8**

3. EduCloud Alliance: Joint X-Road REST Gateway Development (2016). https://github.com/educloudalliance/xroad-rest-gateway
4. https://www.eesti.ee/eng/services/citizen/haridus_ja_teadus/isikukaart_eesti_ee_portaali
5. https://www.eesti.ee/eng/services/citizen
6. ENISA: Good Practice Guide for Securely Deploying Governmental Clouds. European Union Agency for Network and Information Security (2013)
7. Estonian National Electoral Committee: E-Voting System - General Overview (2010). http://vvk.ee/public/dok/General_Description_E-Voting_2010.pdf
8. Gates, S., Hegre, H., Nygrd, H.M., Strand, H.: Development consequences of armed conflict. In: World Development, vol. 40 (2012)
9. Gillespie, M., et al.: Mapping Refugee Media Journeys - Smartphones and Social Media Networks. The Open University and France Medias Monde (2016)
10. Hansen, L., Nissenbaum, H.: Digital disaster, cyber security, and the Copenhagen School. Int. Stud. Q. **53**, 1155–1175 (2009)
11. ICRC: Urban services during protracted armed conflict - a call for a better approach to assisting affected people. International Committee of the Red Cross (2015)
12. Kotka, T., del Castillo, C., Korjus, K.: Estonian e-residency: benefits, risk and lessons learned. In: Kő, A., Francesconi, E. (eds.) EGOVIS 2016. LNCS, vol. 9831, pp. 3–15. Springer, Cham (2016)
13. Kotka, T., Johnson, B., Cebul, T., Lovosevic, L., Liiv, I.: E-Government services migration to the public cloud: experiments and technical findings. In: Kő, A., Francesconi, E. (eds.) EGOVIS 2016. LNCS, vol. 9831, pp. 62–76. Springer, Cham (2016). doi:10.1007/978-3-319-44159-7_5
14. Kotka, T., et al.: Policy and legal environment analysis for e-Government services migration to the public cloud. In: Proceedings of ICEGOV 2015–2016 - 9th International Conference on Theory and Practice of Electronic Governance. ACM (2016)
15. Kotka, T., Liiv, I.: Concept of Estonian Government cloud and data embassies. In: Kő, A., Francesconi, E. (eds.) EGOVIS 2015. LNCS, vol. 9265, pp. 149–162. Springer, Cham (2015). doi:10.1007/978-3-319-22389-6_11
16. Microsoft, MKM: Implementation of the Virtual Data Embassy Solution - Summary Report of the Research Project on Public Cloud Usage for Government. Microsoft Corporation, Estonian Ministry of Economic Affairs and Communications (2015)
17. MKM: Cyber Security Strategy 2014–2017. Estonian Ministry of Economic Affairs and Communications (2014)
18. MKM: Digital Agenda 2020 for Estonia. Estonian Ministry of Economic Affairs and Communications (2013)
19. RIA: Protocol for Data Exchange Between Databases and Information Systems - Requirements for Information Systems and Adapter Servers. Republic of Estonia Information System Authority (2014)
20. Sertifitseerimiskeskus: The Estonian ID Card and Digital Signature Concept - Principles and Solutions (2003). http://www.id.ee/public/The_Estonian_ID_Card_and_Digital_Signature_Concept.pdf
21. Riigi Teataja: Personal Data Protection Act, RT I 2007, 24, 127 (2008)
22. Riigi Teataja: State of Emergency Act, RT I 1996, 8, 165 (1996)
23. Thurnay, L.: The potential of the Estonian e-Governance infrastructure in supporting displaced estonian residents in national emergencies. Master thesis, School of Information Technologies, Tallinn University of Technologies, December 2016

24. UNHCR: Needs Assessment for Refugee Emergencies (NARE) Checklist. United Nations High Commissioner for Refugees (2016)
25. UNHCR: Biometric Identity Management System - Enhancing Registration and Data Management. United Nations High Commissioner for Refugees (2015)
26. UNHCR: Global Report 2014. United Nations High Commissioner for Refugees (2014)
27. UNHCR: Refugee Integration in Europe. United Nations High Commissioner for Refugees (2013)
28. United Nations: E-Government Survey 2016 – e-Government in Support of Sustainable Development (2016)