Hardy, Alex

Article

Estonia's digital diplomacy: Nordic interoperability and the challenges of cross-border e-governance

Internet Policy Review

Provided in Cooperation with:
Alexander von Humboldt Institute for Internet and Society (HIIG), Berlin

Suggested Citation: Hardy, Alex (2024) : Estonia's digital diplomacy: Nordic interoperability and the challenges of cross-border e-governance, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 13, Iss. 3, pp. 1-31, https://doi.org/10.14763/2024.3.1785

This Version is available at:
https://hdl.handle.net/10419/300749

INTERNET POLICY REVIEW
Journal on internet regulation

Volume 13 **Issue** 3

RESEARCH ARTICLE

OPEN ACCESS

PEER REVIEWED

Estonia's digital diplomacy: Nordic interoperability and the challenges of cross-border e-governance

Alex Hardy *University of Liverpool*

DOI: https://doi.org/10.14763/2024.3.1785

Published: 22 July 2024
Received: 4 September 2023 **Accepted:** 22 December 2023

Funding: This research was funded by the author's doctoral grant from the Leverhulme Trust as well as the DORA Mobility Fund, Estonia.
Competing Interests: The author has declared that no competing interests exist that have influenced the text.

Citation: Hardy, A. (2024). Estonia's digital diplomacy: Nordic interoperability and the challenges of cross-border e-governance. *Internet Policy Review*, *13*(3). https://doi.org/10.14763/2024.3.1785

Keywords: Estonia, E-government, Digital diplomacy, Innovation, Cross-border e-governance

Abstract: Estonia has long been held as a leading example of e-Governance. Estonia's ubiquitous e-Governance is enabled by the X-Road, an open-source data exchange layer that allows the secure exchange of data. This paper explores the X-Road integration between Estonia, Finland, the Faroe Islands, the Åland Islands, and Iceland. Having been originally pioneered and implemented by Estonia and developed by the Estonian Information System Authority (RIA), X-Road is increasingly attractive to other nations drawn to the digital services it can enable. This paper argues that the cross-border implementation of the X-road, pioneered by Estonia, is a form of digital diplomacy – an opportunity to extend influence and shape e-norms among geopolitically like-minded partners. Prior conceptions of digital diplomacy have focused on citizen engagement – often specifically on the use of Twitter or other social media platforms for public outreach. This study suggests, however, that our understanding of digital diplomacy ought to extend beyond such undoubtedly important interpretations to also encompass the use of technology in developing closer diplomatic relations. The study utilises a series of semi-structured interviews with government officials and private sector actors to support its arguments around the diplomatic and geopolitical implications of e-Governance as a diplomatic tool.

Introduction

> It's crucial for Estonia to extend its system beyond the country because we've invested so much into it. (Research Participant, "Cybersecurity Solutions" Firm, Tallinn)

This paper represents an examination of contemporary Estonian e-Governance as a tool of foreign policy and digital diplomacy. In relation to Estonia and its neighbours, former Estonian President Kersti Kaljulaid has referred to the development of an "e-Nordic" region.

> We need to have all the Nordic circle countries connected to a single digital identity or at least have the ability to recognise digitally our digital signatures. We will strive to cooperate in this sphere and we are developing from e-Estonia to e-Nordic. (Kaljulaid, 2018)

President Kaljulaid was speaking about the event of Icelandic accession to the NIIS (the Nordic Institute for Interoperability Solutions).[1] The organisation, based in Tallinn, began as a collaborative agreement between the Estonian and Finnish governments. The focus of this institute is the development of cross-border, e-Governance solutions using the X-Road, a "digital ecosystem" software (NIIS, n.d.c). The institute supports the goal of increased cooperation in the realms of e-Governance, e-service development, and cooperative security. Estonia and Finland are the founding members of the NIIS whilst Iceland and the Faroe Islands are associates and are expected to become full members shortly. Full membership is contingent upon the implementation of the X-Road data exchange layer, with a focus on developing interoperable, cross-border services. President Kaljulaid did not explicitly name the countries of her "e-Nordic" vision, and so this paper henceforth refers to the signatories of the NIIS and their pursuit of Nordic interoperability.

This paper investigates the link between contemporary digital diplomacy literature and wider research on e-Governance, digitalisation, and the politics of digital technology. It offers this case study in an attempt to bridge the gap between these two fields of research, exploring some of the similarities and also differences in literature to data. The paper also offers some geopolitical observations building upon

1. Further information on the Nordic Institute of Interoperability Studies can be found on their website, see NIIS, n.d.a

the work of Buchanan (2020) who has offered insights into how technology increasingly shapes statecraft by providing increased opportunities for espionage and destabilisation. Schmidt (2023) conversely noted how digitalisation can be used to build national resilience, noting how Ukraine's rapid digitalisation of state infrastructure was particularly beneficial in maintaining the relationship between citizens and government in the early days of the 2022 Russian invasion of Ukraine. Robinson (2020) has argued that Estonia has already used technology to enhance the resilience of the state via the data embassy initiative (Robinson, 2020). The paper consequently focuses on the question of why Estonia is actively developing this initiative in collaboration with its Nordic neighbours and the socio-economic implications of this unique form of digital diplomacy.

Digital diplomacy

Before defining digital diplomacy, it may be prescient to define conventional diplomacy. The Oxford Dictionary defines diplomacy as "the profession, activity, or skill of managing international relations" (2001). It has been argued that diplomacy is the "institutionalised communication among internationally recognised entities through which representatives produce, manage, and distribute public goods" (Bjola & Kornprobst, 2018, p. 4).

Digital diplomacy has been a growing concern in recent years with an increased focus on semiotic/audience-based studies. This is said to be characterised by a fundamental shift involving the widespread digitalisation of Ministries of Foreign Affairs (MFAs) and a transformation in how diplomacy works in the 21st century (Bjola, 2016; Manor & Kampf, 2022). These are often focused on the messaging of governments using social media outlets to engage with the citizens of other countries and have been covered extensively by the likes of Bjola & Holmes (2015) whose edited volume outlines the policy and the institutional implications of digital diplomacy, largely focusing on foreign ministries. Bjola's (2016) State of the Art noted the "digital shift" of diplomacy moving towards interactions with nationals and non-nationals alike in the pursuit of foreign policy goals. While Adesina (2017) argues that there has been a revolution in diplomatic communication and emphasises how all nations, including African nations she is particularly concerned with, must adapt and learn to communicate their foreign policy in new, innovative ways. Manor (2019) explores digital diplomacy's impact on public diplomacy, using case studies to show technology's influence on diplomatic practices. He evaluates factors driving digitalisation and discusses its role in diplomacy. Manor's subsequent (2020) paper explores the use of humour in this public messaging. This focus on

public messaging characterises much contemporary digital diplomacy research to date, and has broadened to various case studies focusing on the online state communications of the United States, the EU, China (Bjola & Jiang, 2015), Russia (Manor, 2020), and beyond.

What tends to unite these studies is a focus on citizen engagement – often focused on the use of Twitter or other social media networks for public outreach. This study suggests, however, that Digital Diplomacy ought to extend beyond such undoubtedly important interpretations to also encompass the wider use of technology in developing diplomatic relations. Diplomacy is generally accepted to be an extension of, or a means to achieve foreign policy goals. Digital diplomacy should also be understood as a digital extension of more traditional forms of diplomacy, and thus an extension of a nation's foreign policy. There have been some tentative steps in this direction. Bjola & Manor allude to the possibility of broadening the study of digital diplomacy to work which "calls to attention a broader perspective of the role of digital technology in diplomacy, not only as an instrument or medium of communication and collaboration" (2024, p. 20). There has been some work in this regard. Kello (2024) focuses on cybersecurity as a matter of digital diplomacy and identifies "cyber diplomacy" as necessitating a reevaluation of traditional diplomatic frameworks to address evolving threats and stakeholders in the digital age. He also identifies a series of contemporary digital innovations that constitute major challenges such as the development of artificial intelligence and how careful digital diplomacy will be required to mitigate some of the threats it potentially poses. Bjola and Kļaviņš (2024) argue that states have begun to conduct digital diplomacy in a "hybrid" manner which involves both communication-based digital diplomacy but also the use of digital innovation to support conventional diplomacy, noting Estonia's use of an e-residency initiative in this regard.

This paper argues that our understanding of digital diplomacy can be further extended. While this study still involves the use of technology to conduct foreign policy and engage with the wider public, it does not encompass social media interactions, thus demonstrating the value of this case study, which is outlined below, and highlighting the broader potential of digital diplomacy. There is also a difference in the audience. While in public diplomacy-focused work the general public is the intended audience, in this more broadly-defined digital diplomacy, the audience is both the everyday citizen but also the more conventional subject of diplomatic relations – the governing elites of other nation states. Representation and

communication with foreign governments is noted to generally be the preserve of “traditional” diplomacy (Bjola & Manor, 2024) however, a digital diplomacy that engages with both the public and nation state governments is worthy of further research.

Methods

This article draws upon a dataset originating from a series of interviews conducted with individuals from various sectors of the Estonian tech industry, encompassing both public and private domains. This paper utilises data from ten of these interviews, and details of these interviews are included in the annex. These interviews were conducted as part of a broader investigation into Estonia's innovative approaches to e-governance and digitalisation, exploring how the country harnesses technological advancements to enhance governance practices and public service delivery. Moreover, these discussions were framed within the context of a larger project that scrutinises Estonia's strategic use of technology to expand its global influence, particularly in the realms of e-governance and cybersecurity. While interview participants' identities have been anonymized to safeguard confidentiality, detailed information is available in the annex accompanying this article for those seeking further insights. Furthermore, interviews were also conducted with professionals from Finland, offering valuable perspectives on the developments documented in this article, as Finland is an important neighbour and ally of Estonia and is directly impacted by the issues this paper addresses. Employing a semi-structured interview format, these interactions were transcribed and analysed to identify prevailing themes and nuances pertinent to the discourse on e-governance, digital transformation, and cross-cultural dynamics.

The geopolitics of Nordic interoperability

A vision of Nordic interoperability based upon a shared embrace of interoperable e-Governance represents a growing reality between Estonia, Finland, and Iceland. The chief goals of the NIIS include “enabling secure connectivity, searches and data transfers” (Sirviö, 2019). These are reflective of the principles of “confidentiality, integrity and availability” of data which is integral to most information security approaches. These principles have also been applied to e-governance approaches by Adeodate & Pournouri (2020) who note how the “X-tee” (the domestic e-governance ecosystem of Estonia) paid particular heed to the importance of these principles throughout X-tee’s development and implementation.

The sovereignty of data has also come under increasing scrutiny with critiques

covering the importance of geographical locations of digital infrastructure (Amoore, 2018) and the sovereignty of individuals' data (Pohle & Thorsten, 2020). Just as good e-Governance is guided by the principles noted above, it is also subject to geographical and indeed geopolitical forces. The NIIS vision of interoperable e-Governance represents a tentative example of enhanced, interoperable cooperation among willing partners (Sirviö, 2019; Krimmer et al, 2021). Yet it is simultaneously mindful of collective security concerns, both in terms of conventional security and cyber security, and particularly cautious of an increasingly assertive and revanchist Russia in the cyber domain (Dahl & Järvenpää, 2013; Pigman, 2018; Kurowska, 2020) and in the field of digital diplomacy where battles around identity and interpretation of the Soviet and post-Soviet past have become an online battleground in which the Russian Ministry of Foreign Affairs has been increasingly involved (Mälksoo, 2016; Manor, 2019).

The ongoing war in Ukraine is a particularly sensitive matter within the Baltic States who have long feared Russian domination and consistently warned the Western alliance against accommodating Russia before the 2022 full-scale invasion of Ukraine. Similarly, Russian foreign policy in the build-up to the invasion of Ukraine became increasingly focused upon the idea of "NATO expansionism" (Zubok, 2023). Consequently, it is important to acknowledge the environment in which NIIS and Nordic digital interoperability are a product. Namely, a tense geopolitical environment, defined by competing national security goals, where the threat of "hybrid" conflict looms large (for discussion on the geopolitics and competing identities of the region see Aalto, 2003; Berg & Ehin, 2016). Famously, Estonia was the target of malicious cyber attacks in 2007 targeting various public institutions including parliament, ministries, and state broadcasters. These cyber attacks were predominantly DDOS (distributed denial of service) attacks from a wide range of botnets. The incident was noted to be "hybrid" in nature and was supplemented by disorder on the streets from local Russian speakers (Hansen & Nissenbaum, 2009). The consequent fall-out of the 2007 attacks played out in a number of ways. Estonia's diplomatic response was swift, directly accusing the Kremlin of orchestrating the attacks and appealing to both the EU and NATO for assistance. In the aftermath, Estonian lobbying was integral to the establishment of the NATO Cooperative Centre for Cyber Defence in Tallinn. Estonia has also persistently argued that cyber attacks should be covered by Article 5 of the NATO charter, which serves as a mutual defence mechanism for all member states (Kerikmäe et al., 2019). The attacks also served as inspiration for Estonia to initiate the data embassy initiative; a programme which situates critical data storage in a geopolitically friendly nation, Luxembourg, and serves to protect that data in the event that

Estonia's territorial integrity is compromised (Robinson & Martin, 2017).

Actions such as those of 2007 involving both cyber and "real world" attacks have been argued to represent a form of "hybrid" conflict, although not without some cynicism that arguably all conflict is "hybrid" in the modern era (Mälksoo, 2018; Galeotti, 2016). Nevertheless, with the advent of "hybrid" threats, it is crucial to recognise that citizens hold security concerns brought about by the increasing digitalisation of the state and that this increasingly impacts on everyday lives of citizens. Existing critical research is often scathing of a contemporary security environment that increasingly places the burden of security upon citizens (such as Vaughan-Williams & Stevens, 2016), whilst the Estonian "cyber war" of 2007 has been critiqued from a perspective of securitisation (Hansen & Nissenbaum, 2009). Yet, despite these concerns, as well as concerns regarding the potential elite level of cyber security discourse as being inaccessible to average citizens (Dunn Cavelty, 2013), Estonia has continually embraced digital technology in delivering public services, with quantitative research indicating a continual growth of online service usage linked closely to public trust in delivering trustworthy services (Solvak et al., 2019); it has also been perceived as impressive enough by other states that they would like to replicate those services. Analysis of what is being adopted, where, and why, form the substantive analysis of the rest of this paper. Furthermore, this paper contends that Estonia has sought to use digital solutions as a long-term means of digital diplomacy with neighbouring countries such as Finland, who until recently did not share Baltic anxieties and adopted a more accommodating/neutral stance towards Russia (Sulg & Crandall, 2020). While utilising cross-border e-Governance as a digital diplomatic tool is relatively novel, it is not wholly unheard of for small states to adopt niche approaches to extend their international influence (Hardy, 2023). It has been observed that Latvia has very successfully specialised in counter-disinformation, successfully lobbying larger allies within the EU and NATO to take the threat of Russian propaganda seriously and helping to establish the NATO StratCom Centre of Excellence in Riga (Vériter, 2024). Lithuania, meanwhile, has been observed to offset its relatively small network of embassies by being particularly active online, especially in engaging with its diaspora and taking a combative approach to Russian messaging (Manor, 2019). These varied approaches are all broadly illustrative of the geopolitical priorities of those given states.

X-road: A geopolitical vision

Estonia claims to lead the world in e-Governance, with over 99% of government services available online. Every Estonian citizen has a citizen number and a secure

digital identity, and from the age of 16 has access to online services (e-Estonia, 2019). This all functions via the population register, which is connected to other systems and databases via the X-Road – a data exchange layer that supports secure, time-stamped data exchanges. The X-Road is an open-source data exchange layer with multiple instances and is available via Github (2024). The Estonian domestic X-Road instance is known as X-Tee (Tee meaning road in Estonian, however, this is now used to differentiate from the cross-border X-road instance this paper discusses in further detail). Finland operates a domestic X-Road instance Suomi.Fi-palveluväylä (Finland Gateway) and Iceland operates their own X-Road too, named Straumurinn (the stream). So while "X-Road" is a data exchange layer software of which there are multiple named instances, *the* X-Road is the international data exchange layer maintained by the Nordic Institute of Interoperability Studies (NIIS). This particular layer facilitates international data flows between separate X-Road instances. The NIIS is headquartered in Tallinn and is responsible for the ongoing development of the source code and assisting with the implementation of cross-border e-governance (NIIS, n.d.c).

However, X-Road adoption is not limited to the Nordic nations. Others have also adopted the Unified eXchange Platform (UXP) which is a privately developed and fully interoperable alternative to the X-Road (albeit based on the X-Road). This has been developed by the Estonian company Cybernetica and is utilised to provide a number of services and digital identities in several nations including Greenland, Ukraine, Benin, Namibia and more (Saputro et al., 2020; Cybernetica, n.d.). Greenland is a particularly curious case as an autonomous country of the Kingdom of Denmark, much like the Faroe Islands, who utilise X-Road and feature later in this paper. The Greenlandic adoption of the UXP system 'Pitu' and local experiences of digitalisation has been documented by existing research (Wendt, 2020; Jenson et al, 2020).

As with every case study outlined, local experiences are crucial. The Estonian experience of comprehensive e-Governance must be understood within the specific social, cultural and political environment in which it has been produced and implemented. The possibility of replicating e-Estonia beyond Estonia's borders has been subject to critique (Chadwick, 2003; Anthes, 2015; Hardy, 2022), and this has also recently spilt into popular media outlets including Wired, The New Yorker and the BBC (see Lufkin, 2017; Heller 2017; Sterling, 2017). These outlets have eulogised the efficiency, convenience, and economics of the Estonian model. This has been driven by many high-profile campaigns of the Estonian government, such as the e-residency initiative and the data embassy, which have successfully enhanced

the e-Estonia brand (Mäe, 2016; Robinson, 2020).

The ability of the X-Road to provide trackable, time-stamped, accountable data has generated much international interest as it is said to enhance accountability and prevent the misuse of personal data. Citizens access e-services with their secure digital identities, which are double-factor authenticated by the user via a variety of options. Contrary to common misconceptions, the X-Road is not blockchain technology, and the identity of both service providers and consumers is centrally maintained by the X-Road operator (Kivimäki, 2018). Therefore, the appropriate governmental departments in Estonia, Finland, and Iceland are responsible for their respective X-Road instances (X-tee, Suomi.Fi-palveluväylä, and Straumurinn, respectively).

Trust in the state to operate this benevolently is necessary and has been reasonably easy to find in a Estonian context. Existing research has argued that a consequence of the traumas of occupation by the Soviet Union and Nazi Germany and Estonia's perceived fragile independence has ensured increased levels of trust in public institutions within contemporary Estonia (Priisalu & Ottis, 2017). Nevertheless, despite local context, it is vital to build trust services for transparency and accountability.

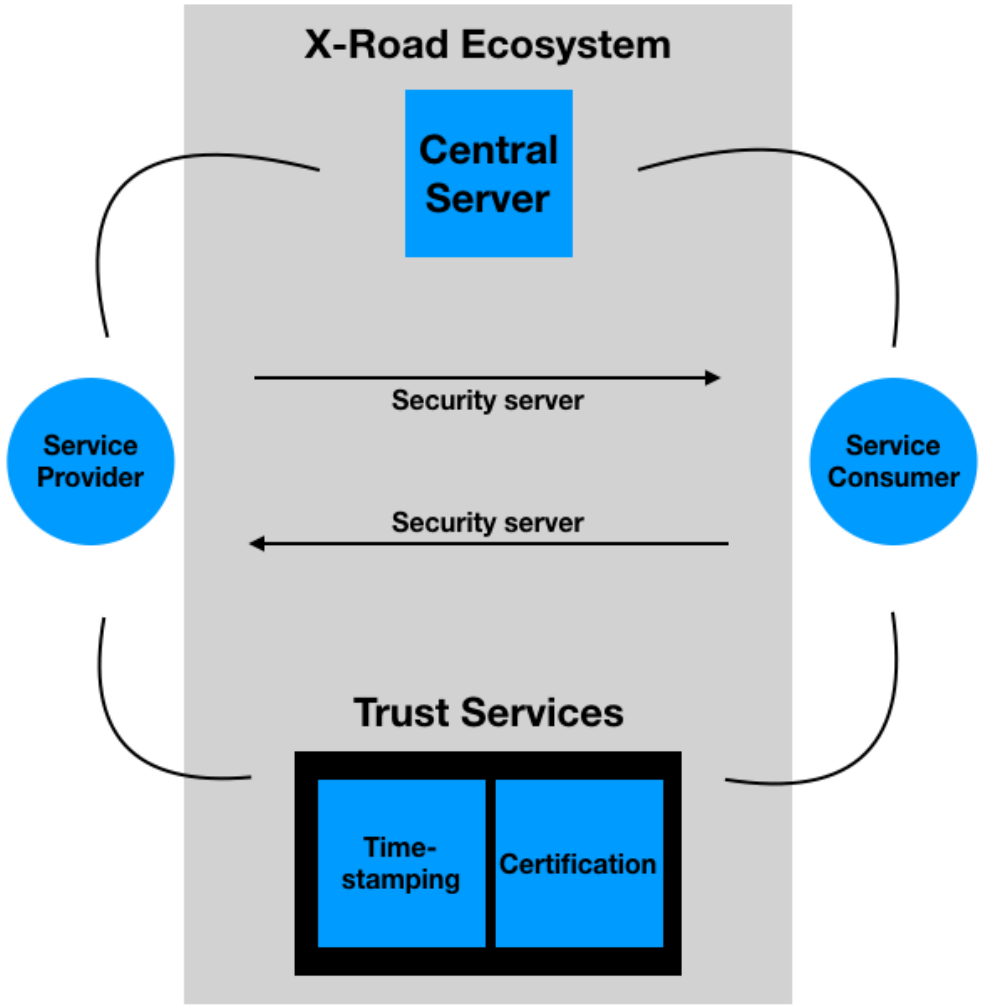

FIGURE 1: An overview of the X-Road Ecosystem (Hardy, 2022). For a highly detailed breakdown of the individual aspects of the Estonian X-Road Ecosystem including individual public and private service providers, see Vassil (2016).

As illustrated in Figure 1, an X-Road instance's key components include the central authority which maintains the central server, as well as associated trust services (including time stamping and certification services) and the security servers which permit communication between service providers and service consumers.[2] Service providers can be both public and private institutions. Trust services provide certification and time-stamping as part of the public key infrastructure (PKI). A combination of procedures, software, and hardware alike combine to implement securely-encrypted digital transactions. Service providers require the approval of the local

2. The diagram represents a simplistic overview of the X-Road. For further information on X-Road Architecture, see the NIIS (n.d.b).

government.

Interoperability, how Nordic interoperability works/will work, and why it matters to Estonia

Existing research on interoperability has been contributed by e-Governance and digitalisation scholars and has illustrated how interoperability projects affect institutional authority and accountability, as well as how domestic e-governance and interoperability among state institutions within one national jurisdiction is vital (Prins et al., 2012) It has also focused on the importance of "institutional reordering" and examined the integration of governmental information systems and how these raise concerns about privacy and surveillance while analysing technical and institutional implications to address power and accountability shifts (Pelizza, 2016). Other e-Governance research has identified legislation, institutional practices, and political agendas as significant challenges and noted that interoperability involves navigating intricate governance issues, with e-Governance projects often facing difficulties due to ambitious integration efforts and the need for societal changes (Hellberg & Grönlund, 2013). These studies have focused on various European nations including the Netherlands, Italy, and Sweden, and these challenges can also be evidenced in Estonia also. However, existing research on Estonia's domestic e-Governance has noted that the principle of interoperability is inherent to the development of national e-Governance services enabled by the X-Road and while not law, it is also an established principle in the country that all services should also ascribe to the Once Only Principle (OOP) to foster trust and enhance public convenience, which has been assessed as a great success domestically (Kattel & Mergel, 2019)

The success of Estonia's X-Road adoption can also be seen in existing quantitative research demonstrating a growing service uptake among the population (see Solvak et al., 2019). As previously mentioned, this has generated considerable interest overseas for X-Road-enabled governance. NIIS and the goal of Nordic Interoperability might be considered a progression of the success of X-Road in Estonia domestically. The goals of the institute are:

> To ensure the quality, sustainability, cross-border capability of core e-government infrastructure components; to save resources upon the development of digital society and cross-border co-operation. (Nordic Institute of Interoperability Studies, 2017)

Estonia has a long-running international reputation for punching above its weight in technological terms. However, existing research has suggested that X-Road's adoption in Estonia was driven predominantly by economic factors, helping to streamline public service costs, which could then be invested in other areas such as infrastructure and defence (Kalja, 2002). The Estonian development of services has often been carried out on an ad-hoc basis, thanks to the unique freedoms of immediate post-Soviet independence, which effectively meant Estonia could build a new government from scratch (Solvak et al., 2018). "e-Estonia" became as much a unique, soft power political tool as it did a technological solution. Many contemporary Estonians self-identify as Nordic rather than Baltic or Post-Soviet. "Soviet" is used as a negative cultural marker:

> I think being Digital means not being Soviet somehow… A lot of Estonians like to identify as Nordic now… (Interview Participant, Estonian e-Governance Academy)

> I think this is part of the Estonian identity these days… It's very much that they want to show themselves as being Nordic… for the other Nordic countries, it's very much about the information system architecture… for Estonia, it's a key part of their foreign and security policy also have close links with these countries… for the others, yes it's beneficial for everyone to cooperate too. (Interview Participant, Nordic Institute of Interoperability Studies)

However, while Estonian e-Governance has been argued to be somewhat identity-driven (Papp-Váry, 2018; Hardy, 2022) visions of Nordic interoperability cannot rely on post-Soviet freedoms and identities as perhaps the X-tee once did at its inception. Nevertheless, the Nordic nations have been observed to contain similarly high levels of trust in public institutions, as noted by Bergh & Bjørnskov (2011) who postulate that this has been shaped by sociocultural and historical factors. These high levels of trust, coupled with Estonian identity-driven political ambitions can be seen as contributory factors in the drive for Nordic interoperability in e-governance.

Below is a rough approximation of X-Road interoperability. So while domestically the X-Road requires public trust in the state to maintain a domestic X-Road instance, in the case of a cross-border interaction, trust will also be invested in the second partner-nation, as well as NIIS as guardians of the X-Road.

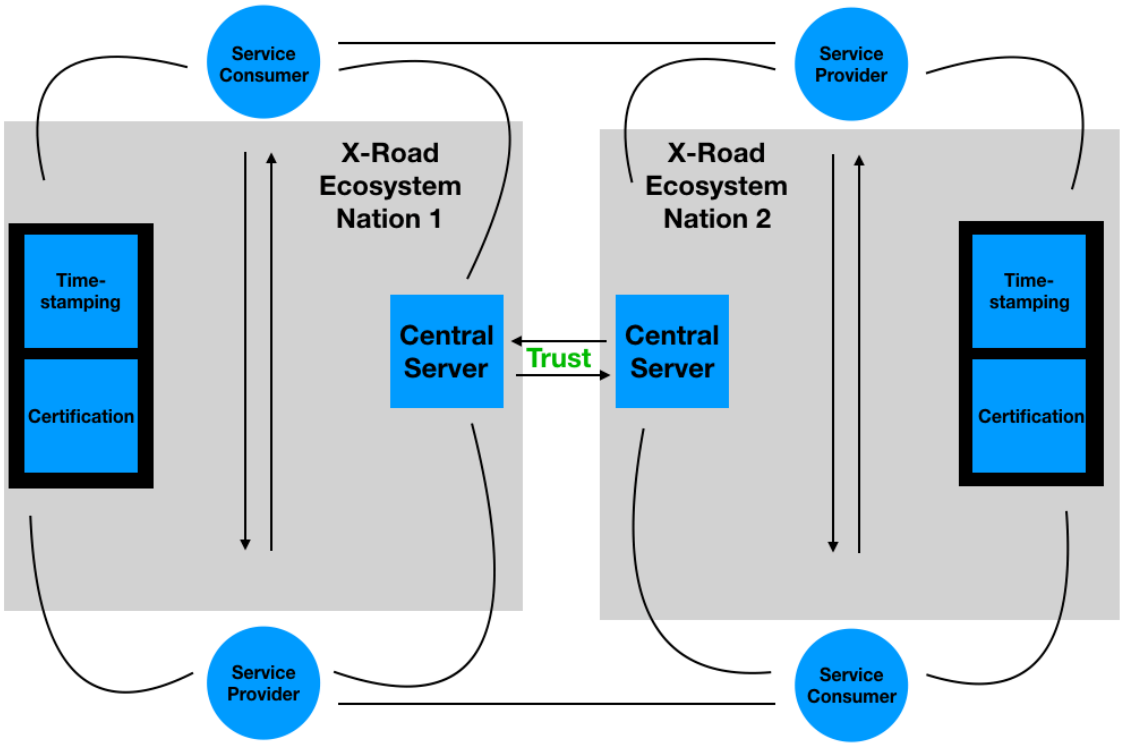

FIGURE 2: Integrated X-Road instance (Hardy, 2022).

One of the primary reasons to federate X-Road instances is to facilitate cross-border interactions between service consumers and service providers, and this is what NIIS – a non-profit organisation funded by the governments of signatories – hope to achieve (NIIS, n.d.c). While domestic X-Road instances are parallel to each other and are maintained by respective national authorities, federation means mutual international agreement. Trust is crucial and cross-border functionality requires a trust relationship between governing authorities and citizens alike.

Most citizens do not understand encryption, the X-Road, Public Key Infrastructure (PKI), or many other technicalities involved in developing secure digital services. Nevertheless, it falls upon the authorities to sell these digital solutions to the public. Harsher critics have suggested that Estonia sells a "fairy tale" which is a "façade" of good governance (Drechsler, 2018, p. 4) and that this creates in effect two tiers of citizens in Estonia: those who are good "e-citizens" (who securely consume the wealth of digital services available to them) and bad "e-citizens" who do not (Björklund, 2016). Research is in its relative infancy elsewhere. As Hjaltalin (2022) notes, Iceland has only recently begun to develop domestic services, albeit at pace. Following the 2017 agreement to join NIIS, Iceland implemented a citizen-facing service app in 2021, with services via the Digital Iceland website gradu-

ally increasing since 2018. Meanwhile, Finland is slightly further ahead of Iceland, implementing the Suomi.fi platform in 2017 after a four-year development process. Thus far, service development has thrived, with existing research noting the high levels of transparency and public trust in governance. Suomi.fi presently enables public service interactions between numerous stakeholders including public, private, and third sector actors in Finland, and external interactions with the Estonian Government and European Union, although the most common interactions are with branches of the public sector and Estonia. (Päivärinta et al., 2019; Abubakr & Kaya, 2021). Interactions between Estonia and Finland are underpinned by the so-called 'trust federation' between the two nations, an agreement that means members of the federated ecosystems can publish and consume services with each other as if they were members of the same ecosystem (NIIS, n.d.c).

Finland's collaboration with the Estonian government involves the integration of the data exchange layer, meaning that Finnish and Estonian citizens can mutually access digital services in either nation (this can be seen in figure 2, where service consumers and service providers can communicate across borders). This allows for the development of cross-border services such as concluding contracts, the sharing of medical data, and the mutual recognition of digital signatures (Petrone, 2022). Given that many Estonians live and work in Finland and account for more than 5% of all visits from Estonia to Finland (Silm et al., 2021), and an albeit smaller number of Finns live and study in Estonia (99% of all visits to Estonia from Finland are for tourist purposes [Silm et al, 2021]), these services provide a tangible human benefit (the lack of tangible benefits for ordinary citizens has been a common concern for critical researchers concerned with the increasing digitalisation of public services. For example, see Coles-Kemp et al., 2018).

> The goal is not necessarily to replicate e-Estonia, but we are capable of achieving their level of digital services and want to work collaboratively with them. (Research Participant, Development Manager, Finnish Population Registry [VRK])

The promotion of such citizen-oriented benefits has led enthusiastic foreign media outlets to encourage their nations to adopt this platform (See Thomson's, 2019 argument that Scotland should adopt the X-Road for such reasons). Indeed, as research participants noted, citizens benefiting from e-governance are crucial to the ongoing success of the project, while they are often less concerned with security.

> It is the services people care about. The state has provided a secure service, but security is not the citizen's primary concern. If you talk to most people… the average person on the street… they perhaps don't think about the security so much. (Research Participant, Senior staff, Private developer of X-Road software)

Undoubtedly, this is representative of the Estonian experience of e-Governance, which is notable for its relative lack of controversies and resistance to its implementation. Yet it does not account for the necessity of gradual introduction, familiarisation and trust building for citizens to engage with e-services. Indeed, this might explain Finnish opposition to e-voting despite comfortably having the expertise and system in place to quickly implement it (YLE News, 2017). Prior research has found that Finland abandoned plans for e-voting after poor trial experiences which garnered negative public reactions, particularly among those with poorer digital skills (Heimo et al., 2010). Those who extol the X-Road, such as the NIIS research participant interviewed, of course highlight this as an advantage, in that states can cater their approach to local concerns.

As of yet, the Faroe Islands have yet to link their domestic systems to the X-Road and have committed to do so in the future (their associate membership with NIIS is based upon progressing towards full interoperability in future). As an autonomous region of Finland, the Åland Islands connect interoperable services through Finland's 'Soumi.fi' platform. Iceland became a full member of NIIS in 2021, allowing the possibility of cross-border services (Digital Iceland, n.d.).

Significant drivers for increased digitalisation of governance and public services in such small states might be said to include demographics, mobility, economics, and efficiency. McBride (2019) explores the challenges of e-governance implementation in the Faroe Islands, highlighting barriers such as limited resources and networks. Despite aspirations, he concludes that digitalisation doesn't necessarily reduce bureaucracy or costs, but aims to promote economic growth and enhance economic independence from Denmark. Much like Greenland, the Faroe Islands are an autonomous and self-governing country of the Kingdom of Denmark. Seeking to pursue an alternative path of digitalisation to the mainland, Denmark has been a local political choice in both and both have embraced local customisations (McBride, 2019; Wendt, 2020). Saputro et al. (2020) identified the prerequisite conditions for X-Road adoption to include appropriate legal frameworks, political leadership, technological expertise, adequate funds, and the principle of a secure digital identity. New member Iceland comfortably meets this criteria, with a high GDP, as well as high levels of political and digital freedom. However, it has been

noted that Iceland faces challenges in innovating due to a "zero-error" local culture (Hjaltalin, 2022). This contrasts with Estonia, where innovation through trial and error helped with service development (Solvak et al., 2019). However, other crucial factors include public sector competencies, adequate funding, infrastructure (Kalvet, 2012), public-private partnership, and academia (Kattel & Mergel, 2019). In these areas, Iceland is well-placed, and digitalisation has received significant public support (Hjaltalin, 2022)

It is important to note that Estonia is not only providing e-government expertise in the Nordic world. Several nations in both the post-Soviet world and Africa have adopted either the X-Road itself or UXP. This international adoption has been enabled either through private enterprise, public diplomacy, or the "e-Governance Academy", an Estonian non-profit that supports digitalisation projects around the world. The most controversial user of the X-Road might be Azerbaijan, described by Freedom House (2020) as "not free" with "rampant corruption" and "little freedom of expression" for citizens, yet the Estonian government "assisted in the development of an information system similar to the X-Road in Azerbaijan" (EGA, 2014). However, unlike Azerbaijan, Finland, Iceland, Åland Islands, and the Faroe Islands may instead be considered to match Estonian aspirations and popular geopolitical visions of being identified as Nordic. The "why" of Nordic interoperability is interrogated further below.

Why develop Nordic interoperability?

This section analyses some of the reasons *why* Estonia is determined to develop and expand cross-border e-governance. This section argues that the reasons include security, mobility, services, economics, and digital diplomacy.

Security

One of the potential benefits of cross-border, interoperable e-governance is the possibility of enhanced security cooperation and the establishment of shared norms and procedures. Norm and subsequent international law building has been identified as a means to improve security (see Mačak, 2017). e-governance, for all the security which can be built into the process, creates vulnerabilities, which can be exploited by malicious state or non-state actors. It simultaneously secures data (for example, digital data stored properly on a distributed ledger is far more secure than paper documents which could be accidentally destroyed or misplaced through human error) but also creates additional attack vectors for would-be cyber attackers and criminals. This is particularly important as it has been noted in the

case of Estonia to create a "digital dependency" (Kattel & Mergel, 2019) which, as the 2007 cyber attacks proved, can grind the country to a halt. It can also represent a number of risks which the X-Road mitigates in various ways, including the use of the Once Only Principle (OOP) which means individuals must only have to provide data once to the authorities. Situations of requesting and sending data are points of risk for data protection as well as for data accuracy, so adherence to OOP is crucial from a security perspective (Nyman Metcalf, 2019).

A recurring pattern among interviews was the threat posed by Russia to its Nordic neighbours, and how decisions around digital innovation needed to be informed by geopolitical thinking:

> It takes guts and its political wisdom and courage to take a position that we should not use Kaspersky… it seems common sense you shouldn't use those if you consider Russia your primary security threat. (Research Participant, Private Consultancy & Former NATO CCDCOE)

Such comments can be seen as reflective of a popular geopolitical imagination (Koopman et al., 2021). This vision is of a menacing, malicious Russia – off and online (Pigman, 2018). This is a threat to the Nordic/Western way of life and chimes with other research which has noted non-conventional threats as a growing security concern, particularly for small nations (see Grigas, 2012; Galeotti, 2016; Mälksoo, 2018).

Existing research has also suggested that the digitalisation of public services often leads to the running down of in-person services, particularly in non-metropolitan areas (Aradau, 2010). As noted by two research participants, the movement of services online creates reliance and vulnerability in Estonia:

> The unique thing is that first, we do *everything* online… Estonians are really closed people…. so whenever you can avoid talking to other people… and we go crazy if things stop working. (Research Participant, Estonian Defence League Cyber Unit)

> It's totally changed life now, and people have a much easier life now… I don't know how people would cope without it… you'd have to go to places. (Research Participant, Senior, Digital Consultancy Firm)

These remarks speak to some of the cultural traits of Estonia but also highlight that total reliance on digital services can create insecurities. In sum, ubiquitous e-governance poses significant security challenges, which involves a complex series of relationships between public and private sector actors (Collier, 2018). The X-Road enables a consistent way to minimise risk, the ability to securely encrypt access to services and data, and the ability to maintain and update the system in an ongoing and streamlined manner (for more discussion on the security benefits of e-governance, see Zissis & Lekas, 2011; Pappel et al., 2012; Solvak et al., 2018). This is, however, balanced against risks such as dependency (Kattel & Mergel, 2019), and the potential for a breakdown of societal trust in the digital state (Nyman Metcalf, 2019).

Mobility and services

Cross-border interoperable e-governance may also represent a potential benefit for citizens. There is significant cross-border movement between Estonia and Finland. Improving access to services and amenities across borders is a strategic priority of NIIS signatories (NIIS, n.d.c). As illustrated earlier in figure 2, the cross-border federation of X-Road between Finland and Estonia now allows for service consumers in each nation to access service providers in the other. There are a number of challenges in federating X-Road instances and making them fully functional. These are both social and technical, as highlighted by Freudenthal & Willsensen (2017) and include differences in legislation, technical solutions, and best practices. This, they argue, could lead to an unclear state of possible disputes and that 100% alignment on all matters is extremely challenging if not impossible.

Nevertheless, cross-border X-Road federation and Nordic Interoperability represents both an ambitious and relatively novel undertaking. The EU has identified delivering cross-border services a strategic priority but delivery of such services so far has been limited. While alignment is improving it remains a major challenge (Large & Barasa, 2022) Estonia's desire to lead in this area is evident, rather than having non-local solutions imposed by the EU. Research participants were eager to emphasise needing a common approach while catering to local concerns is important, rather than being a copied and pasted version of Estonia's X-tee:

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

> want. (Research Participant, Nordic Institute of Interoperability Studies: NIIS)

A key challenge to rolling out the system across the wider region in the pursuit of Nordic interoperability lies in the geographical variability of public concerns. The shared values of these countries, as well as their close socio-cultural ties, make this easier but not without sensitivities. As the system grows, there could be concerns surrounding who maintains the X-Road exchange layer. However, the citizen-centric benefits of Nordic interoperability are a relatively easy case to make. Citizens like services to be easily accessible, adhere to the OOP, dislike bureaucracy, and interview participants further highlighted this.

> People don't want to go back to the old way of doing it. (Research Participant, Estonian Defence League & Private digital consultancy firm)

However, as the same participant consequently noted later in their interview, there is also a trust and security relationship involved. Public trust in Estonia is high, but this dynamic can alter when it involves trusting other states to uphold the same practices and procedures:

> Yeah, so apparently that's been an issue because the systems for these things are different a lot over Europe, so if other countries do their own e-citizenship systems, it's probably not so easy to make them work together, so connecting systems is probably the hardest part. We have that now between Estonia and Finland. The rest, who knows. (Research Participant, Estonian Defence League & Private digital consultancy firm)

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

> Finland just scored first place in human centricity in e-services, so in some areas we are already forerunners and not so much in a position where we need to replicate e-governance models. However, we of course do regular benchmarking and co-operation to learn from the best practices where applicable, as was the case with the X-Road concept a few years back. (Research Participant,

> Development Manager, Finnish Population Registry [VRK])

So whilst Estonia vocally takes the political lead, and has been essential to establishing the X-Road, other contributors should not be overlooked. In 2019, the national business registers and tax boards in Estonia and Finland agreed to cooperate and exchange data via X-Road (Sirviö, 2019) allowing both governments to track taxes collaboratively and potentially counter cross-border tax avoidance.

Economics and digital diplomacy

Aside from the ability to easily track cross-border taxes, one of the central arguments for ubiquitous e-governance on a domestic level is the money-saving aspect. e-Estonia (2020) estimates that Estonia saves roughly 2 percent of the national GDP from its use of digital signatures alone. They further estimate that voting online costs 1/20th of the cost as opposed to voting in person, based on the cost of vote counting, vote processes and voter identification (based on the study of Krimmer et al., 2018). For smaller nations such as Estonia and Iceland, the opportunity to make such savings is significant, as both operate with limited budgets due to their size. However, critics have noted that some savings are exaggerated by the Estonian authorities and that costs have simply been redistributed elsewhere. Drechsler (2018) notes that there are significant costs to digitalisation, which absorb some of the savings made by shrinking paper-based bureaucracy. This is further illustrated by McBride (2019) whose analysis of the Faroe Islands Digital Governance strategy suggested that digitalisation would not generate significant economic benefits (although the Faroe Islands is significantly smaller than the other nations involved in the NIIS). However, there was a hope that digitalisation could support the diversification of the economy. Estonia, Finland, and Iceland all have established tech sectors, which is also conducive to having a skilled population prepared to engage with e-government and the further development of potential cross-border services.

Monetary arguments aside, Estonian Foreign Policy since the resumption of independence has been explicitly pro-Western, NATO, EU, and pursued close ties to the Nordic sphere, using bilateral diplomatic platforms such as the Nordic-Baltic 8 (NB8). Since the restoration of independence, Estonia has continually emphasised its ties to the West and the North with a heightened sense of identity shaping Estonian Foreign Policy (Berg & Ehin, 2016). Estonia's Nordic interoperability goals can be conceived as a distinct extension of Estonian foreign policy, given Estonia's cultivation of a Nordic political identity – a position reinforced by interview partic-

ipants who noted the political/diplomatic nature of Nordic interoperability. This echoes other research that has noted how Estonia has used both technology and alliance-building multilateralism to enhance its diplomatic and political standing internationally (Adamson, 2019; Sulg & Crandall, 2020).

Other small nations have successfully inflated their influence and international standing through specialised expertise in digital technology, such as New Zealand (Burton, 2013). However, specialisation in interoperable, cross-border e-governance is unique. Estonia has sought to identify and exploit a niche for digital diplomatic purposes.e. It remains to be seen how this relationship develops, and who those partners will be in the future:

> It's about mentality and trust… we are conscious of what is happening at an EU level, with the development of services… we don't want a situation where our model becomes obsolete, so it's crucial for us to develop a critical mass… so it's demonstrable to Brussels, if it comes to a European level, that ours can work across borders. (Research Participant, Private Cyber Consultancy)

Estonia, as a small nation, has limited means to influence international politics, yet has already achieved influence and notoriety through digital innovations such as the data embassy and e-residency initiatives (Hardy, 2022). It has used its EU membership, and EU Presidency in 2018, among other bilateral agreements to push for the development of digital norms (Pápp-Vary, 2018; Adamson, 2019). The establishment of NIIS is not just a technical solution to the challenge of integrating e-governance platforms, but it is also a sociotechnical solution and a platform for enhanced digital diplomatic collaboration. This reflects some of the important work of interdisciplinary science and technology studies researchers who have noted the importance of paying attention to the sociotechnical minutiae of interoperability projects and the motivations of governments that implement them (Pelizza, 2016). Furthermore, Hellberg & Grönlund (2013) highlight the importance of local values in implementing cross-border services. The insights gleaned from these studies equally apply in this case study; as is noted by Saputro et al. (2020) X-Road adoption relies on political will and political support. Blake Jackson, Dreyling, & Pappel (2021) similarly conclude that the political and legal support afforded to the X-Road in Estonia for domestic development was crucial. The success or failure of Nordic interoperability will likely be decided by political support as much as technological expertise. An additional challenge is that the X-Road is resilient to EU-wide developments. Of note is the new eIDAS regulation, which legislates for functionalities and technical specifications of digital identity docu-

ments across the European Union (European Commision, 2014; European Commission, 2023). Estonia has maintained a critical stance to eIDAS and has encouraged private sector collaboration, and while it continues to aim to make a new application mRiik eIDAS 2.0 compatible, there have been a number of delays (Vihma, 2024; Koppel, 2024). While Estonia recognises the need to develop independent solutions and get other nations on board with its approach – actively seeking to do so in an act of digital diplomacy – it also recognises the geopolitical reality of its smallness and the need to work with rather than against the EU.

Challenges, conclusions and further research opportunities

The objective of this article has encompassed two main facets: firstly, it has sought to contribute to the expanding field of digital diplomacy, recognising the significance of this area of study and broadening the interdisciplinary scope of this field by exploring the use of e-governance as a diplomatic tool. Secondly, it seeks to provide a unique case study, addressing the scarcity of qualitative research on cross-border e-governance. This article refrains from adopting a purely supportive or critical stance, and endeavours to present a nuanced examination, suggesting digital diplomacy as a viable perspective to understand Estonia's motivations in seeking to expand the use of the X-road in the Nordic region. In acknowledging potential limitations, the article opts against an extensive discussion of positionality, given its pragmatic orientation and emphasis on practical socioeconomic implications, digital diplomacy, and geopolitical motivations rather than theoretical elaboration. However, to inject some reflexivity, while it is not the normative goal of this paper to state whether this Estonian model of digitalisation is desirable, it is challenging if not impossible to be fully impartial. The research was conducted over roughly a two year period spent living in Estonia, and while an outsider, I operated in a broadly privileged position as a British researcher from a reputable UK university. This enabled generous access to willing research participants and will also inevitably have informed how participants spoke about their experiences of digitalisation and e-governance – often with great pride. The article is somewhat Estonia-centric and further research can and should seek to interrogate these developments from a non-Estonia centred position in future. This article does not seek to suggest that all nations, even in the Nordic region, should pursue Estonia's strategy, but rather seeks to highlight that this is a unique cross-border development based on trust in a geopolitically significant region.

Much like domestic e-governance, cross-border interoperability requires trust and

political support to function, grow, and be attractive to private developers. In Estonia's domestic experience, that trust is a collaborative social contract formed between the government and populace over a significant amount of time. Interview participants hailed the Estonian government's role in building trust and use of digital technology and were optimistic that this approach could work beyond Estonian borders.

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

Sociotechnical cultures will likely be vital to the political and economic future of Nordic interoperability. While service provision, security, and financial benefits are touted as benefits, the political angle for all parties cannot be ignored. The financial incentives for integrating Finnish and Estonian e-governance (as well as the Åland Islands) are relatively clear cut, as there is economic activity between these close neighbours, but the financial and service-based cases for integrating Iceland and the Faroe Islands are less clear. It is, however, relatively easy to find evidence of digital diplomacy PR celebrating Iceland's use of X-Road (Digital Iceland, n.d.). Iceland, and other partners, get to celebrate collaboration with the internationally recognised "e-Estonia" image, and Estonia enhances its Nordic credentials while also building a reputation for cross-border solutions, through which it hopes to build international influence. Consequently, this paper concludes that Estonia's pursuit of nordic interoperability should be viewed as the latest Estonian use of digital innovation to extend their diplomatic and international reputation and a form of digital diplomacy. Further research might focus on cross-border service solutions as they mature and produce comparative studies of qualitative or quantitative nature. These could focus on the case studies in this article, or alternatives as they undoubtedly emerge across Europe. Likewise, future studies of digital diplomacy may continue to extend beyond the digital communications of statecraft and focus on how states, small and large alike, utilise digital technology to extend their in-

fluence.

References

Aalto, P. (2003). *Constructing post-Soviet geopolitics in Estonia*. Routledge.

Abubakr, M., & Kaya, T. (2021). A comparison of e-government systems between developed and developing countries: Selective insights from Iraq and Finland. *International Journal of Electronic Government Research*, *17*(1), 1–14. https://doi.org/10.4018/IJEGR.2021010101

Adeodato, R., & Pournouri, S. (2020). Secure implementation of e-governance: A case study about Estonia. In H. Jahankhani, S. Kendzierskyj, N. Chelvachandran, & J. Ibarra (Eds.), *Cyber defence in the age of AI, smart societies and augmented humanity* (pp. 397–429). Springer International Publishing. https://doi.org/10.1007/978-3-030-35746-7_18

Adesina, O. S. (2017). Foreign policy in an era of digital diplomacy. *Cogent Social Sciences*, *3*(1). https://doi.org/10.1080/23311886.2017.1297175

Amoore, L. (2018). Cloud geographies: Computing, data, sovereignty. *Progress in Human Geography*, *42*(1), 4–24. https://doi.org/10.1177/0309132516662147

Anthes, G. (2015). Estonia: A model for e-government. *Communications of the ACM*, *58*(6), 18–20. https://doi.org/10.1145/2754951

Aradau, C. (2010). Security that matters: Critical infrastructure and objects of protection. *Security Dialogue*, *41*(5), 491–514. https://doi.org/10.1177/0967010610382687

Berg, E., & Ehin, P. (Eds.). (2016). *Identity and foreign policy: Baltic-Russian relations and European integration* (1st ed.). Routledge. https://doi.org/10.4324/9781315587745

Bjola, C. (2016). Digital diplomacy – The state of the art. *Global Affairs*, *2*(3), 297–299. https://doi.org/10.1080/23340460.2016.1239372

Bjola, C., & Holmes, M. (2015). *Digital diplomacy: Theory and practice*. Routledge. https://doi.org/10.4324/9781315730844

Bjola, C., & Kļaviņš, D. (2024). The digital hybridization of ministries of foreign affairs: The case of the Nordic and Baltic states. In C. Bjola & I. Manor (Eds.), *The Oxford handbook of digital diplomacy* (1st ed., pp. 291–310). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780192859198.013.16

Bjola, C., & Kornprobst, M. (2018). *Understanding international diplomacy: Theory, practice and ethics* (2nd ed.). Routledge. https://doi.org/10.4324/9781315196367

Bjola, C., & Manor, I. (Eds.). (2024). *The Oxford handbook of digital diplomacy* (1st ed.). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780192859198.001.0001

Björklund, F. (2016). E-government and moral citizenship: The case of Estonia. *Citizenship Studies*, *20*(6–7), 914–931. https://doi.org/10.1080/13621025.2016.1213222

Buchanan, B. (2020). *The hacker and the state: Cyber attacks and the new normal of geopolitics*. Harvard University Press. https://doi.org/10.2307/j.ctv3405w2m

Burton, J. (2013). Small states and cyber security: The case of New Zealand. *Political Science*, *65*(2), 216–238. https://doi.org/10.1177/0032318713508491

Chadwick, A. (2003). Bringing e-democracy back in: Why it matters for future research on e-governance. *Social Science Computer Review*, *21*(4), 443–455. https://doi.org/10.1177/0894439303256372

Coles-Kemp, L., Ashenden, D., & O'Hara, K. (2018). Why should I? Cybersecurity, the security of the state and the insecurity of the citizen. *Politics and Governance*, *6*(2), 41–48. https://doi.org/10.17645/pag.v6i2.1333

Collier, J. (2018). Cyber security assemblages: A framework for understanding the dynamic and contested nature of security provision. *Politics and Governance*, *6*(2), 13–21. https://doi.org/10.17645/pag.v6i2.1324

Cybernetica. (n.d.). *Unified eXchange Platform (UXP)*. Cyber.Ee. https://cyber.ee/products/secure-data-exchange/

Dahl, A.-S., & Järvenpää, P. (Eds.). (2013). *Northern security and global politics: Nordic-Baltic strategic influence in a post-unipolar world* (1st ed.). Routledge. https://doi.org/10.4324/9780203725344

Digital Iceland. (n.d.). *Straumurinn (X-Road)*. Ísland.Is. https://island.is/en/o/digital-iceland/island-services/straumurinn

Drechsler, W. (2018). Pathfinder: E-Estonia as the β-version. *JeDEM - eJournal of eDemocracy and Open Government*, *10*(2), 1–22. https://doi.org/10.29379/jedem.v10i2.513

Dunn Cavelty, M. (2013). From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse. *International Studies Review*, *15*(1), 105–122. https://doi.org/10.1111/misr.12023

e-Estonia. (2020, August 19). E-Governance saves money and working hours. *E-Estonia*. https://e-estonia.com/e-Governance-saves-money-and-working-hours/

e-Governance Academy. (2014). *Estonia to construct secure data exchange X-Road layer for Namibia* [Press release]. https://ega.ee/news/estonia-to-construct-secure-data-exchange-layer-similar-to-X-Road-for-namibia/

European Commision. (2014). *Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity* (COM/2021/281). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2021:281:FIN

European Commission. (2023). *Commission welcomes final agreement on EU Digital Identity Wallet* [Press release]. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_5651

Freudenthal, M., & Willemson, J. (2017). Challenges of federating national data access infrastructures. In P. Farshim & E. Simion (Eds.), *International conference for information technology and communications* (Vol. 10543, pp. 104–114). Springer. https://doi.org/10.1007/978-3-319-69284-5_8

Galeotti, M. (2016). Hybrid, ambiguous, and non-linear? How new is Russia's 'new way of war'? *Small Wars & Insurgencies*, *27*(2), 282–301. https://doi.org/10.1080/09592318.2015.1129170

Github. (2024). *Nordic Institute—X-Road* [dataset]. https://github.com/nordic-institute/X-Road

Grigas, A. (2012). *Legacies, coercion and soft power: Russian influence in the Baltic States* (pp. 1–16)

[Briefing paper]. Chatham House. https://www.chathamhouse.org/sites/default/files/public/Research/Russia%20and%20Eurasia/0812bp_grigas.pdf

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International Studies Quarterly*, *53*(4), 1155–1175. https://doi.org/10.1111/j.1468-2478.2009.00572.x

Hardy, A. (2022). *Securing e-Estonia: Challenges, insecurities, opportunities* [Doctoral dissertation, Royal Holloway, University of London]. https://pure.royalholloway.ac.uk/en/publications/securing-e-estonia-challenges-insecurities-opportunities

Hardy, A. (2023). Digital innovation and shelter theory: Exploring Estonia's e-Residency, Data Embassy, and cross-border e-governance initiatives. *Journal of Baltic Studies*, 1–18. https://doi.org/10.1080/01629778.2023.2288118

Heimo, O. I., Fairweather, N. B., & Kimppa, K. K. (2010). The Finnish e-voting experiment: What went wrong. In M. Arias-Oliva, T. Ward Bynum, S. Rogerson, & T. Torres-Coronas (Eds.), *The "backwards, forwards and sideways" changes of ICT* (pp. 290–298). Universitat Rovira i Virgili. https://llibres.urv.cat/index.php/purv/catalog/book/131

Hellberg, A.-S., & Grönlund, Å. (2013). Conflicts in implementing interoperability: Re-operationalizing basic values. *Government Information Quarterly*, *30*(2), 154–162. https://doi.org/10.1016/j.giq.2012.10.006

Heller, N. (2017, December 11). Estonia, the digital republic. *The New Yorker*. https://www.newyorker.com/magazine/2017/12/18/estonia-the-digital-republic

Hjaltalin, I. T. (2022). Adopting digital government shared-services centers: A case from Iceland. *Proceedings of the 15th International Conference on Theory and Practice of Electronic Governance*, 140–145. https://doi.org/10.1145/3560107.3560132

Jensen, R. B., Coles-Kemp, L., Wendt, N., & Lewis, M. (2020). Digital liminalities: Understanding isolated communities on the edge. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–14. https://doi.org/10.1145/3313831.3376137

Jóhannesson, G. (2021). Iceland and Estonia: 30 years of friendly relations. *ERR News*. https://news.err.ee/1608318014/feature-iceland-and-estonia-30-years-of-friendly-relations

Kalja, A. (2002). The X-Road project. A project to modernize Estonia's national databases. *Baltic IT&T Review*, *24*, 47–48. http://www.ebaltics.lv/doc_upl/Kalja(2).pdf

Kalvet, T. (2012). Innovation: A factor explaining e-government success in Estonia. *Electronic Government, an International Journal*, *9*(2), 142–158. https://doi.org/10.1504/EG.2012.046266

Kattel, R., & Mergel, I. (2019). Estonia's digital transformation: Mission mystique and the hiding hand. In P. 't Hart & M. Compton (Eds.), *Great policy successes* (pp. 143–160). Oxford University Press. https://doi.org/10.1093/oso/9780198843719.003.0008

Kello, L. (2024). Digital diplomacy and cyber defence. In C. Bjola & I. Manor (Eds.), *The Oxford handbook of digital diplomacy* (pp. 121–137). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780192859198.013.7

Kerikmäe, T., Mölder, H., & Chochia, A. (2019). Estonia and the European Union. In *Oxford research encyclopedia of politics*. Oxford University Press. https://doi.org/10.1093/acrefore/9780190228637.013.1105

Kivimäki, P. (2018, April 26). There is no blockchain technology in X-Road. *NIIS Blog*. https://www.niis.org/blog/2018/4/26/there-is-no-blockchain-technology-in-the-x-road

Koppel, K. (2024, February 18). EU digital ID and mRiik app integration still unclear, both built in Estonia. *ERR News*. https://news.err.ee/1609256928/eu-digital-id-and-mriik-app-integration-still-unclear-both-built-in-estonia

Krimmer, R., Dedovic, S., Schmidt, C., & Corici, A. A. (2021). Developing cross-border e-Governance: Exploring interoperability and cross-border integration. *Electronic Participation: 13th IFIP WG 8.5 International Conference*, 107–124. https://doi.org/10.1007/978-3-030-82824-0_9

Krimmer, R., Duenas-Cid, D., Krivonosova, I., Vinkel, P., & Koitmae, A. (2018). How much does an e-Vote cost? Cost comparison per vote in multichannel elections in Estonia. In R. Krimmer, M. Volkamer, V. Cortier, R. Goré, M. Hapsara, U. Serdült, & D. Duenas-Cid (Eds.), *Electronic Voting Third International Joint Conference* (Vol. 11143, pp. 117–131). Springer International Publishing. https://doi.org/10.1007/978-3-030-00419-4_8

Kurowska, X. (2020). What Russia wants in cyber diplomacy. A primer. In D. Broeders & B. van der Berg (Eds.), *Governing cyberspace: Behaviour, power and diplomacy* (pp. 105–125). Rowman & Littlefield International. https://rowman.com/WebDocs/Open_Access_Governing_Cyberspace_Broeders_and_van_den_Berg.pdf

Large, O., & Barasa, H. (2022). *Digital government in Europe: In pursuit of cross-border functionality* [Briefing]. Tony Blair Institute for Global Change. https://www.institute.global/insights/tech-and-digitalisation/digital-government-europe-pursuit-cross-border-functionality

Lufkin, B. (2017, October 19). Could Estonia be the first 'digital' country? *BBC News*. https://www.bbc.com/future/article/20171019-could-estonia-be-the-first-digital-country

Mačák, K. (2017). From cyber norms to cyber rules: Re-engaging states as law-makers. *Leiden Journal of International Law*, *30*(4), 877–899. https://doi.org/10.1017/S0922156517000358

Mäe, R. (2017). The story of e-Estonia: A discourse-theoretical approach. *Baltic Worlds*, *1–2*, 32–44. https://balticworlds.com/the-story-of-e-estonia/

Mälksoo, M. (2018). Countering hybrid warfare as ontological security management: The emerging practices of the EU and NATO. *European Security*, *27*(3), 374–392. https://doi.org/10.1080/09662839.2018.1497984

Manor, I. (2019). A discussion of the digitalization of public diplomacy. In I. Manor, *The digitalization of public diplomacy* (pp. 323–352). Palgrave MacMillan. https://doi.org/10.1007/978-3-030-04405-3_10

Manor, I. (2020). The Russians are laughing! The Russians are laughing! How Russian diplomats employ humour in online public diplomacy. *Global Society*, *35*(1), 61–83. https://doi.org/10.1080/13600826.2020.1828299

Manor, I., & Kampf, R. (2022). Digital nativity and digital diplomacy: Exploring conceptual differences between digital natives and digital immigrants. *Global Policy*, *13*(4), 442–457. https://doi.org/10.1111/1758-5899.13095

McBride, K. (2019). Sailing towards digitalization when it doesn't make cents? Analysing the Faroe Islands' new digital governance trajectory. *Island Studies Journal*, *14*(2), 193–214. https://doi.org/10.24043/isj.93

Nordic Institute for Interoperability Solutions (NIIS). (n.d.a). *Digital society solutions and cross-border*

cooperation [Homepage]. https://www.niis.org/

Nordic Institute for Interoperability Solutions (NIIS). (n.d.c). *Strategy: The strategy of the Nordic Institute for Interoperability Solutions*. https://www.niis.org/strategy

Nordic Institute for Interoperability Solutions (NIIS). (n.d.b). *X-Road architecture*. https://x-road.global/architecture

Nyman Metcalf, K. (2019). Com construir la governança electrònica en una societat digital: El cas d'Estònia [How to build e-governance in a digital society: The case of Estonia]. *Revista Catalana de Dret Públic*, *58*, 1–12. https://doi.org/10.2436/rcdp.i58.2019.3316

Oxford Dictionaries. (2002). Diplomacy. In *The Oxford essential dictionary of the U.S. military*. https://www.oxfordreference.com/display/10.1093/oi/authority.20110803095719998

Päivärinta, T., Smolander, K., & Yli-Huumo, J. (2019). Towards stakeholder governance on large e-government platforms – A case of Suomi. Fi. *10th Scandinavian Conference on Information Systems*, *11*. https://aisel.aisnet.org/scis2019/11

Pappel, I., Pappel, I., & Saarmann, M. (2012). *Digital records keeping to information governance in Estonian local governments*. International Conference on Information Society (i-Society 2012). https://doi.org/10.13140/2.1.1435.6800

Papp-Váry, Á. F. (2018). A successful example of complex country branding: The 'e-Estonia' positioning concept and its relation to the presidency of the Council of the EU. *Acta Universitatis Sapientiae, European and Regional Studies*, *14*(1), 87–115. https://doi.org/10.2478/auseur-2018-0013

Pelizza, A. (2016). Developing the vectorial glance: Infrastructural inversion for the new agenda on government information systems. *Science, Technology, & Human Values*, *41*(2), 298–321. https://doi.org/10.1177/0162243915597478

Petrone, J. (2022, August 29). Tried and tested: Europe strives for crossborder patient data sharing. *E-Estonia*. https://e-estonia.com/european-crossborder-patient-summaries-effort-advances/

Pigman, L. (2019). Russia's vision of cyberspace: A danger to regime security, public safety, and societal norms and cohesion. *Journal of Cyber Policy*, *4*(1), 22–34. https://doi.org/10.1080/23738871.2018.1546884

Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, *9*(4). https://doi.org/10.14763/2020.4.1532

Priisalu, J., & Ottis, R. (2017). Personal control of privacy and data: Estonian experience. *Health and Technology*, *7*, 441–451. https://doi.org/10.1007/s12553-017-0195-1

Prins, J. E. J., Broeders, D., & Griffioen, H. M. (2012). iGovernment: A new perspective on the future of government digitisation. *Computer Law & Security Review*, *28*(3), 273–282. https://doi.org/10.1016/j.clsr.2012.03.010

Robinson, N. D. (2020). *Distributed denial-of-government: The Data Embassy and the geopolitical, diplomatic and legal implications of extraterritorial data storage* [Doctoral dissertation, Royal Holloway, University of London]. https://pure.royalholloway.ac.uk/ws/portalfiles/portal/44682853/2020_Robinson_N_PhD.pdf

Robinson, N., & Martin, K. (2017). Distributed denial of government: The Estonian Data Embassy Initiative. *Network Security*, *2017*(9), 13–16. https://doi.org/10.1016/S1353-4858(17)30114-9

Robles, G., Gamalielsson, J., & Lundell, B. (2019). Setting up government 3.0 solutions based on open source software: The case of X-Road. In I. Lindgren, M. Janssen, H. Lee, A. Polini, M. P. Rodríguez Bolívar, H. J. Scholl, & E. Tambouris (Eds.), *Electronic Government 18th IFIP WG 8.5 International Conference* (Vol. 11685, pp. 69–81). Springer International Publishing. https://doi.org/10.1007/978-3-030-27325-5_6

Saputro, R., Pappel, I., Vainsalu, H., Lips, S., & Draheim, D. (2020). *Prerequisites for the adoption of the X - Road interoperability and data exchange framework: A comparative study*. 216–222. https://doi.org/10.1109/ICEDEG48599.2020.9096704

Schmidt, E. (2023, February 28). Innovation power: Why technology will define the future of geopolitics. *Foreign Affairs*. https://www.foreignaffairs.com/united-states/eric-schmidt-innovation-power-technology-geopolitics

Silm, S., Jauhiainen, J. S., Raun, J., & Tiru, M. (2021). Temporary population mobilities between Estonia and Finland based on mobile phone data and the emergence of a cross-border region. *European Planning Studies*, *29*(4), 699–719. https://doi.org/10.1080/09654313.2020.1774514

Sirviö, V. (2019). Estonia and Finland – Digital forerunners in cross-border cooperation. *NIIS Blog*. https://web.archive.org/web/20201120033903/https://www.niis.org/blog/2019/10/2/estonia-and-finland-digital-forerunners-in-cross-border-cooperation

Solvak, M., Unt, T., Rozgonjuk, D., Võrk, A., Veskimäe, M., & Vassil, K. (2019). E-governance diffusion: Population level e-service adoption rates and usage patterns. *Telematics and Informatics*, *36*, 39–54. https://doi.org/10.1016/j.tele.2018.11.005

Sterling, B. (2017, August 26). Meanwhile, in Estonian e-residency. *Wired*. https://www.wired.com/beyond-the-beyond/2017/08/meanwhile-estonian-e-residency/

Sulg, M.-L., & Crandall, M. (2020). Geopolitics: The seen and unseen in small state foreign policy. *Journal of Regional Security*, *15*(1), 109–130. https://doi.org/10.5937/jrs15-24562

Tammpuu, P., & Masso, A. (2018). 'Welcome to the virtual state': Estonian e-residency and the digitalised state as a commodity. *European Journal of Cultural Studies*, *21*(5), 543–560. https://doi.org/10.1177/1367549417751148

Vassil, K. (2016). *Estonian e-Government ecosystem: Foundation, applications, outcomes* (World Cevelopment Report 2016 Digital Dividends, pp. 1–29) [Background paper]. http://citis.ut.ee/articles/articles/estonian-e-government-ecosystem-foundation-applications-outc

Vaughan-Williams, N., & Stevens, D. (2016). Vernacular theories of everyday (in)security: The disruptive potential of non-elite knowledge. *Security Dialogue*, *47*(1), 40–58. https://www.jstor.org/stable/26293584

Vériter, S. L. (2024). Small-state influence in EU security governance: Unveiling Latvian lobbying against disinformation. *JCMS: Journal of Common Market Studies*. https://doi.org/10.1111/jcms.13601

Vihma, P. (2024, February 14). Digital wallet and eIDAS 2.0: A boost for Estonian companies. *E-Estonia*. https://e-estonia.com/digital-wallet-and-eidas-2-0-a-boost-for-estonian-companies/

Wendt, N. S. (2020). *Digital self-determination: Everyday security through digitalisation and identity formation in Greenland* [Doctoral dissertation, Royal Holloway, University of London]. https://core.ac.uk/download/pdf/354516497.pdf

YLE News. (2017, December 20). Ministry working group says 'not yet' to online voting in Finland. *Yleisradio Oy*. https://yle.fi/a/3-9984736

Zissis, D., & Lekkas, D. (2011). Securing e-Government and e-Voting with an open cloud computing architecture. *Government Information Quarterly*, *28*(2), 239–251. https://doi.org/10.1016/j.giq.2010.05.010

Zubok, V. M. (2023). Myths and realities of Putinism and NATO expansion. In J. Goldgeier & J. R. I. Shifrinson (Eds.), *Evaluating NATO Enlargement* (pp. 145–159). Palgrave MacMillan. https://doi.org/10.1007/978-3-031-23364-7_5

Annex

Below is a list of those interviewed who have informed this paper as well as other publications including the author's doctoral thesis. Individual positions were collected by the author from the research participants at the time of the interview. The positions of those at private companies have been obscured slightly, as agreed with participants, mindful of ethical anonymisation and good academic practice. Descriptions of companies are included, but those companies' names have been obscured. Governmental institutions/departments are named.

- Participant 1: Works for a private firm involved in developing critical e-Government systems. Sales.
- Participant 2: As per participant 1. Senior research staff.
- Participant 3: Professor of e-Governance, Taltech University.
- Participant 4: Senior staff at the Ministry of Economic Affairs and Communications, Estonia.
- Participant 5: Technical volunteer at Küberkaitseliit (The Estonian Defence League Cyber Unit).
- Participant 6: Senior figure at the e-governance Academy, involved in creating and transferring knowledge and best practices in digital transformation.
- Participant 7: Researcher for the Government Office of Estonia specialising in e-governance and Cybersecurity.
- Participant 8: Senior figure at NIIS (The Nordic Institute of Interoperability Studies), involved in ensuring the development and strategic management of X-Road and other cross-border components for e-government infrastructure.
- Participant 9: Senior figure at the Finnish governmental department VRK (Väestörekisterikeskus), involved in cross-border e-governance collaboration with Estonia.
- Participant 10: CEO of Private IT Consultancy and Technical Solutions Firm, Estonia.

Published by

Alexander von Humboldt
INSTITUTE FOR INTERNET
AND SOCIETY

in cooperation with