EXPLORING ESTONIAN E-GOVERNMENT BEFORE, DURING, AND BEYOND COVID-19[*]

Logan Carmichael

University of Tartu
logan.emily.carmichael@ut.ee

[*] This work was supported in part by European Union’s Horizon 2020 research and innovation program under grant agreement No 857622 “ERA Chair in E-Governance and Digital Public Services — ECePS”.

Abstract

The outbreak of COVID-19 saw lockdowns imposed across the world, and traditionally in-person tasks and services shifted online. While this posed immense challenges in some governmental and institutional settings, in Estonia rigorous digital advancements dating back to the 1990s have made this learning curve markedly less steep, as many digital service provisions were widely available prior to the pandemic. This paper explores Estonia's e-government solutions pre-dating, during, and beyond the pandemic. It will examine mechanisms – e-ID, X-Road, the information authority, state portal, and e-learning – that existed prior to the pandemic, and others – new e-services, fully online learning, and contact tracing applications – that have emerged in direct response to the pandemic. Finally, this paper will examine how elements of Estonian e-government can, and have been, adopted in international settings, considering how cybersecurity, regulation, and accessibility are closely intertwined with such dialogues surrounding e-government. Throughout this paper, overarching analysis addresses how decades of digitisation in Estonia largely prepared the country for new realities of COVID-19, but some shortcomings exist that must be mitigated. Ultimately, this paper concludes that Estonian e-government must evolve with changing realities; continued growth and improvement is entirely necessary.

As COVID-19 swept across the globe in early 2020, lockdown measures banned in-person interactions, attempting to quell the spread of the virus. With in-person interactions restricted, the alternative was digitisation of these interactions to be conducted remotely; in some places, this rapid digital transition was accelerated by more than a decade, vis-à-vis what would have taken place under normal circumstances.[1] The result was a tremendous learning curve, as populations tried to understand and adapt to this new reality. In Estonia, deemed "a digital success story" long before the pandemic, this learning curve was not as steep, as the Baltic nation had spent decades undergoing a digital transformation that included digitising its government provisions.[2] As a result, in many capacities, Estonia was more prepared for the pandemic than other countries that had not experienced such extensive digitisation. However, it is inaccurate to say that Estonia was entirely prepared for the pandemic: the country indeed felt the impacts of COVID-19 itself, requiring the innovation of new systems, including in e-government.

The first case of COVID-19 in Estonia was found on 26th February 2020, in a returnee who had entered the country via a bus from Riga, Latvia.[3] The eventual spread of the virus in Estonia

[1] Liisa Past, "Securing Accelerated Digital Transformation: How to Best Survive the Global Pandemic," 27 January, 2021.

[2] Rainer Kattel and Ines Mergel, "Estonia's Digital Transformation: Mission Mystique and the Hiding Hand," *UCL Institute for Innovation and Public Purpose Working Paper Series* (2018): p. 7.

[3] ERR, "First Coronavirus Case Found in Estonia," 27 February, 2020.

prompted an emergency situation[4] to be declared on 12th March 2020, instituting lockdown measures across the country and imposing entry restrictions.[5] Though the emergency situation ended in May 2020, some restrictions continued throughout 2020 and into 2021, at times varying regionally. Measures instituted on 30th January 2021 harmonised restrictions nationwide; whereas measures had previously been in place in Harju and Ida-Viru counties, they were now renewed across the whole of the country.[6] These measures required mask-wearing indoors, the '2+2 rule' (groups of two people, maintaining a distance of two metres apart), and limitations on public gatherings, entertainment venues, catering establishments, and sporting events.[7] At time of writing, Estonia had experienced 45,663 cases of COVID-19, and 433 deaths, while vaccinating 30,158 people at least once, and 12,842 with a complete vaccination.[8] In line with the global situation, pandemic-related conditions in Estonia remain ongoing and changing.

This paper addresses how Estonia's e-government system has adapted and expanded during the pandemic by examining its historical development, the core components of its existing structure,

[4] It is notable that an emergency situation – undertaken in the event of a natural disaster, communicable disease, or other emergency – is not the same as a state of emergency, instituted only when there is a threat to Estonian constitutional order.

[5] ERR, "Estonian Government Declares Emergency Situation Against Coronavirus," 13 March, 2020.

[6] Riigiteataja, "Measures for Preventing the Spread of Coronavirus SARS-CoV-2," n.d.

[7] Kriis.ee, "The Government Approved Nationwide Restrictions on COVID-19 Control," 29 January, 2021.

[8] Republic of Estonia Health Board, "Coronavirus Dataset," 4 February, 2021.

and new implementations that have emerged since the onset of the pandemic. As well, it explores what prospects exist for exporting Estonian e-government practices globally, and what considerations must be evaluated for such a process to occur. The paper is divided into four key sections. The first section looks at the origins of both Estonian e-governance and e-government that provide the foundations for its current iteration, dating back to initiatives of the early 1990s. The second section examines the existing body of e-government provisions – electronic identification, X-Road, the information systems authority (RIHA), state portal, and education system – at the onset of the pandemic and its usefulness amidst lockdown restrictions and other pandemic-related realities. The third section will look at how Estonian e-government has evolved with COVID-19, with the expansion of e-services, the education system's move online, and provisions such as the HOIA contact tracing app, evaluating how effective these new mechanisms have been during the pandemic. Notably, this section encompasses the start of the pandemic around March 2020, until early February 2021, at time of writing. Lastly, this paper analyses the prospects for exporting elements of Estonian e-government to other states and international entities, as opportunities have arisen for Estonian technologies such as X-Road to be adopted by the likes of the World Health Organisation. The first, second, and third sections look at e-government in a domestic context, while the focus of the final section is international, examining applications beyond Estonia's borders. This paper does not argue that Estonian e-government have mitigated the COVID-19 pandemic itself, but rather, lessened some of the difficulties experienced with lockdown restrictions and the forced digitisation associated with these restrictions.

Methodology and Background

Methodologically, this paper is primarily an exploratory case study, while also utilising elements of policy analysis and discourse analysis. Using an exploratory case study allows for in-depth examination of a single case, Estonia, in gleaning increased understanding of a particular phenomenon, Estonian e-government preceding, during, and beyond COVID-19. This paper employs some of the Sage's handbooks approaches to the policy analysis process, asking questions including what problem exists, who it impacts, available policy options to address the problem, which policy option is most desirable, and what other variables should be considered.[9] However, there are limitations to this analysis, especially in the context of COVID-19, as some changes to Estonian e-government have come less as a result of contemplative policy-making, and more an urgent, reactive response to rapidly changing pandemic conditions. This paper also employs political discourse analysis, adopting van Dijk's delineation of political participants as those "elected or appointed, as the central players in the polity," but which would also encompass politically-engaged citizenry, political organisations, or

[9] Michael E. Kraft and Scott R. Furlong, "Policy Analysis: An Introduction", chapter 4 in *Public Policy: Politics, Analysis, and Alternatives* (5th ed.). Thousand Oaks, CA: Sage (2016), p. 117.

key commentators in academia and the media.[10] This includes both literature review and analysis of expert commentary from academics and practitioners, as well as news media, and organisational and government websites.

This paper seeks to build upon the body of literature outlined below, particularly surrounding Estonian e-government. It aims to provide an up-to-date overview of this system, considering how it has been formed over time, and how it has been impacted – as well as itself been impactful – amidst COVID-19. Furthermore, this paper seeks to contribute to broader e-government narratives globally, as it examines how Estonian e-government practices have already been adopted internationally and what considerations must be taken into account for this process to be undertaken. Estonia has often been held up as a case study, with various elements of Estonian digital government – from the platforms themselves, to the government provision of these services – studied in scholarly literature. Kerikmäe, Ramiro Troitiño, and Shumilo have examined public perceptions, in addition to myths and misconceptions, surrounding Estonian e-governance, concluding that this digitised model provides an 'ideal' for other countries to emulate, "looking at Estonia as a pathfinder to learn from."[11] They found that "perceptions of Estonian

[10] Teun A. Van Dijk, "What is Political Discourse Analysis," *Belgian Journal of Linguistics* 11 (1997), p. 13.

[11] Tanel Kerikmäe, David Ramiro Troitiño and Olga Shumilo, 'An Idol or an Ideal? A Case Study of Estonian E-Governance: Public Perceptions, Myths and Misbeliefs,' *Acta Baltica Historiae et Philosophiae Scientiarum* 7, no. 1 (2019), p. 77-78.

e-governance mostly reflect an ‘ideal’ mindset, which offers a tentative model of remarkably successful digital government” created under imperfect conditions, but whose benefits could be enjoyed elsewhere “as a possible cure to other countries’ inner public administration problems.”[12]

Solvak et al.’s comprehensive research on e-service adoption in Estonia explores how adoption rates have grown linearly over the 13-year period examined, with males and females adopting e-services at almost the same rate, though with some variation across age groups; overall, those aged 20-29 and 30-44 had the highest e-service adoption rates.[13] They found that some individuals “use more than 200 separate e-services a year… [while] the typical individual uses only a handful of unique services,” on a more frequent basis.[14] Note Solvak et al., “these findings indicate that the population in general does not face strong hurdles in uptake,” with seemingly no upper limit for the saturation of e-service usage.[15] More broadly, Kouremetis deemed Estonia “one of the most progressive adopters of information and communication technologies in all aspects of government, society and culture,” while examining components such as the ID-

[12] Ibid.

[13] Mihkel Solvak, Taavi Unt, Dmitri Rozgonjuk, Andres Vork, Marten Veskimae, and Kristjan Vassil. “E-Governance Diffusion: Population Level e-Service Adoption Rates and Usage Patterns,” *Telematics and Informatics* 36 (2019), p. 45-46.

[14] Ibid, p. 48.

[15] Ibid, p. 42, 49.

card and X-Road, and the country's cybersecurity practices.[16] As early as 2005, scholars deemed Estonian e-government as "best practice," emphasising its advanced, interconnected architecture, with X-Road as its 'backbone'.[17]

Furthermore, Czosseck, Ottis, and Talihärm have written about advancements in cybersecurity in Estonia after the country suffered a major cyberattack in 2007, including amending the Estonian penal code to raising public awareness of digital issues.[18] Herzog similarly examines changes to Estonian cybersecurity mechanisms in the ten years following the cyberattack, exploring both domestic and international cooperative endeavours.[19] Crandall and Collin designate Estonia as a cybersecurity "norm entrepreneur," vastly disproportionate to the country's small size.[20] A body of scholarly work has specifically focused on the applicability of Estonian digitisation to the United States. [21] Even in 2009, Alvarez, Hall, and

[16] Michael Kouremetis, "An Analysis of Estonia's Cyber Security Strategy, Policy and Capabilities (Case Study)," *Proceedings of the 14th European Conference on Cyber Warfare and Security, Hatfield, United Kingdom* (2015), p. 404.

[17] Ahto Kalja, Aleksander Reitsakas, and Niilo Saard, "eGovernment in Estonia: Best Practices," *A Unifying Discipline for Melting the Boundaries Technology Management,* Portland, USA (2005), p. 500-501.

[18] Christian Czosseck, Rain Ottis, and Anna-Maria Talihärm. "Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security," *European Conference on Information Warfare and Security*, Reading, UK (2018), p. 58-60.

[19] Stephen Herzog, 'Ten Years After the Estonian Cyberattacks: Defense and Adaptation in the Age of Digital Insecurity,' *Georgetown Journal of International Affairs* 18, no. 3 (2017), p. 72-75.

[20] Matthew Crandall and Collin Allan. "Small States and Big Ideas: Estonia's Battle for Cybersecurity Norms," *Contemporary Security Policy* 36, no. 2 (2015), p. 354

[21] See: Sharon L. Cardash, Frank J. Cilluffo, and Rain Ottis, "Estonia's Cyber Defence League: A Model for the United States?" *Studies in Conflict and Terrorism* 36, no. 9 (2013), p. 785; Cory Robinson, "Disclosure of Personal Data in

Trechsel asserted that Estonia's internet accessibility, legal structure, identification system, and "political culture […] supportive of Internet voting" is a model for countries that previously trialled e-voting, including France, the Netherlands, the United Kingdom, and the United States.[22] Meyerhoff Nielsen described Estonia's "political willingness to innovate, work with the private sector, and transform the public sector" as 'key' for creating a hospitable setting for successful e-government outcomes, while also attributing the country's political centralisation, and the availability, effectiveness, and efficiency of e-government provisions.[23] However, existing scholarly literature has not consisted exclusively of praise of Estonia. Kitsing has examined inconsistencies in the implementation and integration of e-government across Estonian government.[24] Paide et al have looked specifically at difficulties surrounding the X-Road data exchange platform, and a relative lack of adoption from private-sector entities.[25]

eCommerce: A Cross-National Comparison of Estonia and the United States," *Telematics and Informatics* 34 (2017): 569-570.

[22] R. Michael Alvarez, Thad E. Hall, and Alexander H. Trechsel, "Internet Voting in Comparative Perspective: The Case of Estonia," *PS: Political Science and Politics* 42, no. 3 (2009): p. 498-499.

[23] Morten Meyerhoff Nielsen, "eGovernance and Online Service Delivery in Estonia," Proceedings of the 18th Annual International Conference on Digital Government Research, New York, USA (2017), p. 302.

[24] Meelis Kitsing, "The Janus-Faced Approach to Governance: A Mismatch Between Public Sector Reforms and Digital Government in Estonia," *Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance, Galway, Ireland* (2018), p. 60.

[25] Karoline Paide, Ingrid Pappel, Heiko Vainsalu and Dirk Draheim, "On the Systematic Exploitation of the Estonian Data Exchange Layer X-Road for Strengthening Public-Private Partnerships," *Proceedings of the 11th International*

More broadly, scholarly work has examined the concepts of e-governance and e-government, deeming the distinction between these two terms as subtle, yet significant. In their study of the websites of American municipalities, D'Agostino et al distinguish the two: "e-government focuses on government services that are electronically provided to citizens. In contrast, e-governance assumes an interactive dynamic between government elites and the citizenry."[26] Bannister and Connolly have collated and analysed existing definitions of e-governance from an array of sources, including scholars and international organisations like UNESCO, drawing the conclusion that e-governance can be differentiated from e-government in that it changes the underlying, pre-existing model of governance, rather than simply being a digitised version of the previously analogue government service provision.[27] In his study of Estonia, Meyerhoff-Nielsen builds on the definition of e-governance, adding that it "refers to the governing bodies responsible for the successful introduction of eGovernment solutions like online public services."[28] Thus, this paper uses the term 'digital governance' or 'e-governance' to refer to the government – as well as the private sector entities with which it

Conference on Theory and Practice of Electronic Governance, Galway, Ireland (2018), p. 36, 38.

[26] Maria J. D'Agostino, Richard Schwester, Tony Carrizales, and James Melitski, "A Study of E-Government and E-Governance: An Empirical Examination of Municipal Websites," *Public Administration Quarterly* 35, no. 1 (2011), p. 3-4.

[27] Frank Bannister and Regina Connolly, "Defining E-Governance," *e-Service Journal* 8, no. 2 (2012), p. 12.

[28] Morten Meyerhoff Nielsen, "eGovernance and Online Service Delivery in Estonia," Proceedings of the 18th Annual International Conference on Digital Government Research, New York, USA (2017), p. 301.

works closely – provision of ‘digital government’ or ‘e-government,’ and its full array of digital services, to the Estonian citizenry.

Literature on various elements of COVID-19 is now beginning to emerge, as the pandemic’s reach has been wide, with long-term impacts to be examined in many disciplines of study. Much of the existing commentary on COVID-19 and digital government, specifically in Estonia, has emerged from mainstream media. Early reporting on the pandemic from *The New Yorker* posited that “Estonia may be the nation best prepared for the consequences of the pandemic,” on account of its wealth of digital services readily available as lockdown restrictions were imposed.[29] *The Atlantic*’s Nina Jankowicz similarly described the array of available e-services, before asserting that the United States should strive to learn from this model.[30] Additionally, some scholarly literature has emerged focusing on Estonia’s COVID-19 experience: Makarychev and Romashko compared Estonian and Finnish responses to the pandemic, determining that decision-making in Estonia was often decentralised and provided as guidelines, rather than legally-enforceable requirements.[31] Riemer et al. examined early contact tracing applications and their prospects for adoption and success; though pre-dating the Estonian contact tracing app, HOIA, this work

[29] Masha Gessen, “Why Estonia was Poised to Handle How a Pandemic Would Change Everything,” 24 March, 2020.

[30] Nina Jankowicz, “Estonia Already Lives Online – Why Can’t the United States?” 27 May, 2020.

[31] Andrey Makarychev and Tatiana Romashko, “Precarious Sovereignty in a Post-Liberal Europe: The COVID-19 Emergency in Estonia and Finland,” *Chinese Political Science Review* 6 (2021), p. 70-71.

provides a useful theoretical foundation for examining issues surrounding contact tracing apps.[32] Though primarily focused on Estonian e-government, this paper also contributes to the ostensibly fast-growing body of literature on COVID-19.

The Origins of Estonia's Digital Society

Examining the historical underpinnings of Estonia's e-government system over the past three decades is crucial to understanding how this system functions presently, along with the impacts felt during the pandemic. When Estonia regained its independence from the Soviet Union in August 1991, the country had immense possibilities to carve out a new path for itself. One key opportunity that Estonia seized was innovation in technology-related fields, an emerging space at the time. Kitsing notes that the Soviet banking system was largely analogue and cash-based, providing a 'blank slate' for Estonian banks to institute online banking and digitised systems largely free of "legacy costs and path dependencies of old banking systems."[33] High-quality services, with relatively early and widespread adoption, even vis-à-vis many Western countries, were already in place in the 1990s, when Estonia's two largest banks, Hansapank and Ühispank, offered their bank portal platforms to the

[32] Kai Riemer, Raffaele Ciriello, Sandra Peter, and Daniel Schlagwein, "Digital Contact-Tracing Adoption in the COVID-19 Pandemic: IT Governance for Collective Action at the Societal Level," *European Journal of Information Systems* 29, no. 6 (2020), p. 731.

[33] Meelis Kitsing, "The Janus-Faced Approach to Governance: A Mismatch Between Public Sector Reforms and Digital Government in Estonia," *Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance, Galway, Ireland* (2018), p. 63.

Estonian government for e-government purposes between 1999 and 2003.[34]

During this same era, indicators of Estonian ICT development rapidly increased. Accessibility of internet services and computers "took off" between 1997 and 1999, with Estonian computer ownership rising from 5% to 14%; this figure remained at 6% in Latvia and Lithuania.[35] Estonia's rapid adoption of technologies represented a deviation even from its Baltic counterparts. A uniquely Estonian endeavour was the launch of the Tiger Leap in 1997. The programme sought to "prepare the education system and the whole society for the Information Age" via digital literacy and computer skills taught in Estonian classrooms.[36] Tiger Leap, which received a generous budget (€10 million from the state budget and €9 million from municipalities), installed computers in all 560 Estonian schools, provided internet access to 75% of schools, and trained more than 10,000 teachers in technological education.[37] Though the programme officially only lasted four years, it paved the way for a generation of technologically-literate Estonians.

[34] Ibid, p. 63-64.

[35] Pille Runnel, Pille Pruulmann-Vengerfeldt and Kristina Reinsalu, "The Estonian Tiger Leap from Post-Communism to the Information Society: From Policy to Practice," *Journal of Baltic Studies* 40, no. 1 (2009), p. 31.

[36] Heli Aru-Chabilan, "Tiger Leap for Digital Turn in the Estonian Education," *Educational Media International* 57, no. 1 (2020), p. 63.

[37] Anu Toots and Mart Laanpere, "Tiger in Focus: A National Survey of ICT in Estonian Schools," *Educational Media International* 41, no. 1 (2004), p. 8; Michael Kouremetis, "An Analysis of Estonia's Cyber Security Strategy, Policy and Capabilities (Case Study)," *Proceedings of the 14th European Conference on Cyber Warfare and Security, Hatfield, United Kingdom* (2015), p. 404.

The new millennium signalled further digital advancements, including improved internet accessibility, the first public Wi-Fi space in 2001, and the first instance of e-voting in nationwide elections in 2005.[38] Despite the Estonia's technological savvy at that time, the country was struck by distributed denial-of-service (DDoS) cyberattacks in 2007, targeting the websites of the government, news media, banks, and other institutions. These cyberattacks were largely believed to originate from Russia as a politically motivated response to the relocation of a Red Army statue in Tallinn in April 2007.[39] Though the cyberattacks both debilitated and defaced major Estonian websites over several weeks, they represented another key opportunity in Estonia's digital progression. Estonia's cybersecurity was bolstered through policy changes and new measures enacted following the cyberattacks. A new cybersecurity strategy in 2009 outlined five key objectives: implementation of new systems, increasing competence, improved legal frameworks, further international cooperation, and increased general awareness, all in the field of cybersecurity.[40] It resulted in changes to the Estonian Penal Code, new cybersecurity entities within the government to accompany the existing Computer Emergency Response Team

[38] e-Estonia, "i-Voting," n.d.

[39] The government of the Russian Federation refused to cooperate with Estonia's investigation into the cyberattacks, though the pro-Kremlin youth group Nashi later claimed responsibility.

[40] Christian Czosseck, Rain Ottis, and Anna-Maria Talihärm. "Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security," *European Conference on Information Warfare and Security*, Reading, UK (2018), p. 58.

(CERT-EE), and the establishment of the Cyber Defence Unit of the Estonian Defence League (formerly the Cyber Defence League, CDL).[41] Longer-term changes have seen Estonia become a global 'norm entrepreneur' in cybersecurity, with NATO's Cooperative Cyber Defence Centre of Excellence (CCDCoE) housed in Tallinn, a sign of "the success of Estonia's norm-building efforts."[42] The country's enhanced cybersecurity in the wake of the 2007 cyberattacks meant increasing safety mechanisms to not only continue, but expand e-government provisions.

Core components of the e-government system were explored as early as the 1990s. The ID-card, initially an idea for both legal identification and an instrument for e-government services, evolved very closely with 1990s banking advancements. In 2001, Estonia's parliament, the Riigikogu, voted to establish the ID-card as a required identity document, the same year that Estonia's largest banks and telecommunications providers established AS Sertifitseerimikeskus (AS SK), which later formed a public-private partnership with the government as a certification centre for the ID-card.[43] The first ID-cards were introduced in 2002, in fulfilment of the *Digital Signature*

[41] Ibid, p. 60-61; Stephen Herzog, 'Ten Years After the Estonian Cyberattacks: Defense and Adaptation in the Age of Digital Insecurity,' *Georgetown Journal of International Affairs* 18, no. 3 (2017), p. 70.

[42] Matthew Crandall and Collin Allan. "Small States and Big Ideas: Estonia's Battle for Cybersecurity Norms," *Contemporary Security Policy* 36, no. 2 (2015), p. 354, 359.

[43] Meelis Kitsing, "The Janus-Faced Approach to Governance: A Mismatch Between Public Sector Reforms and Digital Government in Estonia," *Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance, Galway, Ireland* (2018), p. 66.

Act, as mandatory for all Estonian citizens[44] and "meant to be the primary document for identification in any (governmental, business or private) form of communication."[45] The ID-card has grown steadily in its use and scope since its debut almost two decades ago, but this has not come without difficulties. In 2017, Czech researchers uncovered vulnerabilities in 700,000 ID-cards, which were rectified before any damage could be done.[46] This indicates the potential for breaches and other shortcomings with e-government provisions, but also the efforts to which Estonia has gone to improve its e-government model. This has been a process of evolution, adaptation, and innovation, which has laid the groundwork for the e-governance structure in place in Estonia when COVID-19 struck.

Estonian E-Government Prior to COVID-19

This section will examine the e-government mechanisms in place in Estonia immediately preceding the onset of the COVID-19 pandemic. Furthermore, it will explore the usefulness of these services, systems, and practices after a nationwide emergency situation was declared due to the pandemic on 12th March, 2020. To do so, this paper adopts Solvak et al's four key infrastructural elements of Estonian e-government: electronic identification (e-ID),

[44] It is unclear the penalty for not holding this mandatory document; this has not been enforced.

[45] Marc Ernsdorff and Adriana Berbec, "Estonia: The Short Road to E-Government and E-Democracy." In: Paul G. Nixon and Vassiliki N. Koutrakou (eds.), *E-Government in Europe: Re-Booting the State.* Abingdon, UK: Routledge, 2007, p. 173.

[46] e-Estonia, "What We Learned from the eID Card Security Risk," May 2018.

the data exchange platform X-Road, the state information system (RIHA), and the state portal, eesti.ee.[47] The Estonian education system will also be examined as a central part of Estonia's digital transformation, an important case study in the resilience of, and challenges incurred by, Estonian e-government amidst rapid changes prompted by the pandemic. It is worth noting that the government does not provide all these services itself: the "public sector does not have the capacity to offer all services needed," and thus, must rely on public-private partnerships (PPPs) for some service provisions.[48] Instances of PPPs will be noted, where relevant.

Electronic Identification

As mentioned, the idea of e-ID in Estonia first emerged in the 1990s, and initially materialised via the ID-card in 2002, though its scope has expanded significantly over time. The current iteration of the ID-card provides legal photo identification, access to e-services and e-voting, public key encryption, and "definitive proof of ID in an electronic environment," including digital signatures.[49] Estonian ID-cards are not strictly a government service provision, but rather the result of cooperation with private sector entities, involved in various

[47] Mihkel Solvak, Taavi Unt, Dmitri Rozgonjuk, Andres Vork, Marten Veskimae, and Kristjan Vassil. "E-Governance Diffusion: Population Level e-Service Adoption Rates and Usage Patterns," *Telematics and Informatics* 36 (2019), p. 40.

[48] Karoline Paide, Ingrid Pappel, Heiko Vainsalu and Dirk Draheim, "On the Systematic Exploitation of the Estonian Data Exchange Layer X-Road for Strengthening Public-Private Partnerships," *Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance, Galway, Ireland* (2018), p. 36.

[49] e-Estonia, "ID-Card," n.d.

components of the ID-card, including authentication, encryption, and digital signatures. Approximately 98% of Estonians hold this mandatory document, while 67% use the ID-card regularly.[50] Notes Kitsing, this expansion can be traced to e-ID's origins with internet banking, which he says is "fundamental in explaining the early emergence of e-government services and the ID-card [and] have helped to diffuse the use of e-government services further."[51]

A slightly more recent development was the introduction of Mobile-ID, a mobile phone-based ID system intended to supplement the ID-card, in 2007. It requires a mobile device and a special Mobile-ID-compatible SIM card, available from service providers at an approximate cost of $12.[52] Mobile-ID offers the benefit of not requiring a card reader, as the ID-card does. While it was expected to take off with the advent of smartphones and tablets, it has not yet seen as widespread adoption as the ID-card, with only 16% of voters using Mobile-ID.[53] This is likely due to the ID-card being a mandatory document, required for all Estonian citizens over the age of fifteen, whereas Mobile-ID is not required. The ID-card and Mobile-ID together provide access to the vast portfolio of almost 5000 services, encompassing the public and private sectors, and national and

[50] Ibid.

[51] Meelis Kitsing, "The Janus-Faced Approach to Governance: A Mismatch Between Public Sector Reforms and Digital Government in Estonia," *Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance, Galway, Ireland* (2018), p. 66

[52] Ibid; ID.ee, "Application of Mobile-ID," n.d.

[53] E-Estonia, "Mobile-ID," n.d.

municipal levels of government.[54] As became the tagline of Estonia's e-government success, the only times an Estonian needed to interact with their government in-person was for marriages, divorces, and real estate transactions.

With lockdown restrictions in place from March 2020, the ability to access Estonian government services with e-ID was not only convenient, but entirely necessary as in-person interactions came to a halt. Especially compared with other countries operating on more analogue systems, Estonians could identify themselves and access e-services with relative ease. The full extent of Estonian e-ID's usefulness, especially in the context of the pandemic, has likely not yet been realised. Estonia has not had an election during the pandemic thus far, but if lockdown restrictions remain in place through an election,[55] e-ID and sixteen years of experience with e-voting mean that Estonia could circumvent many of the election challenges seen in predominantly analogue voting throughout 2020: issues with social distancing, voter line-ups, and allegations of 'rigging.' The use of e-ID to access one's e-prescriptions and medical records, by both the patient and medical professional, is also significant, especially as COVID-19 vaccinations unfold over the early months of 2021. It is vital to ensuring the Estonian government's vaccination plan is met,

[54] E-Estonia, "Estonia Introduced a New ID Card," January 2019; Meelis Kitsing, "The Janus-Faced Approach to Governance: A Mismatch Between Public Sector Reforms and Digital Government in Estonia," *Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance, Galway, Ireland* (2018), p. 67.

[55] The next election in Estonia will be municipal elections in October 2021.

and to ensure necessary information reaches e-service users and medical professionals alike.

X-Road

X-Road is the data exchange layer underpinning much of Estonia's e-government system, nicknamed the 'backbone' or 'busiest highway of e-Estonia'. The idea of X-Road emerged in the late 1990s, then developed as a pilot in 2000, before a project draft was submitted to the Estonian government in early 2001. Procurement for a PPP took place in April and May 2001, with AS Assert winning the contract and AS Cybernetica, one of its sub-contractors, developing X-Road before its implementation in December 2001.[56] In addition to connecting data registers with service providers, X-Road "establishes data exchange rules and communication security standards and monitors that users adhere to these."[57] Beginning in 2007, KSI blockchain was developed in Estonia, using a distributed public ledger to ensure the authenticity of data exchanged on the X-Road; the employment of blockchain technology "means that no-one – not hackers, not system administrators, and not even the government itself – can manipulate the data," while also retaining data privacy.[58] Paide outlines that the security of the X-Road is ensured by "authentication, log treatment

[56] X-Road, "X-Road History," n.d.

[57] Mihkel Solvak, Taavi Unt, Dmitri Rozgonjuk, Andres Vork, Marten Veskimae, and Kristjan Vassil. "E-Governance Diffusion: Population Level e-Service Adoption Rates and Usage Patterns," *Telematics and Informatics* 36 (2019), p. 40.

[58] E-Estonia, "KSI Blockchain," n.d.

features, authorisation, encrypted and time-stamped data traffic," however, it is notable that such provisions become more difficult to maintain consistently as data exchange systems are in place across borders, and legal and political jurisdictions, as will be explored later in this paper.[59]

Prior to the COVID-19 pandemic, the X-Road system had already been adopted for usage outside of Estonia, in places like Azerbaijan and Sweden, as part of a test project. The export of Estonian technologies and practices, including X-Road, is enabled by further public-private partnerships, such as the e-Governance Academy, discussed in greater detail in a latter section. Amidst lockdown restrictions that saw in-person interactions and services severely curtailed, X-Road provided the basis for digital service provisions to continue. Its role as a platform for effectively and securely connecting service providers with e-service users meant that Estonians did not face the same disruptions experienced in other parts of the world where government service provisions were perhaps not yet digitalised, or even digitised. While it has been noted that mainstream media took notice of Estonia's e-government model in the early days of the pandemic, so too did other states and prominent international actors, including the World Health Organisation

[59] Karoline Paide, Ingrid Pappel, Heiko Vainsalu and Dirk Draheim, "On the Systematic Exploitation of the Estonian Data Exchange Layer X-Road for Strengthening Public-Private Partnerships," *Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance, Galway, Ireland* (2018), p. 37; Kim Hartmann and Christoph Steup, "On the Security of International Exchange Services for E-Governance Systems," *Datenschutz und Datensicherheit* 39 (2015), p. 475.

(WHO), particularly surrounding the success of the X-Road. The reasons underlying this interest are explored in a later section of this paper.

Estonian State Information System (RIHA)

The Estonian State Information System (RIHA) is a semantic asset repository containing both the e-service catalogue and registry. Firstly, the RIHA's catalogue provides listings of the various information systems available in Estonia, along with pertinent information on their purpose, data they contain, and where and how that data can be found. Secondly, it allows for information systems to be added into the RIHA's catalogue for the purposes of informing agencies and developers of what data is held and how it can be used, while also ensuring the information system obeys the law and meets national-level IT requirements. Additionally, the RIHA provides the option to join X-Road, effectively delegating the data exchange security to X-Road, allowing use of the state information system's service, and user access to their data.[60] At the time of writing, the RIHA's catalogue presented 1301 information systems, representing various entities and levels of government across the country.[61]

The RIHA falls within the Information System Authority (RIA), under the Estonian Ministry of Economic Affairs and Communications, which "coordinates the development and

[60] Riigi Infosüsteemi Haldussüsteem, "Ülevadde Riigi Infosüsteemist," n.d.
[61] Riigi Infosüsteemi Haldussüsteem, "Infosüsteemid," n.d.

administration of information systems ensuring the interoperability of the state's information system, organises activities related to information security, and handles security incidents in Estonian computer networks."[62] The RIA is responsible for managing and protecting the state Internet network, secure e-elections, and the digital identity of Estonia globally.[63] Additionally, it manages the state portal, eesti.ee, examined below. Also within the scope of the RIA is cybersecurity initiatives including the Estonian Computer Emergency Response Team (CERT-EE), which provides assistance with cybersecurity incidents.[64] In the context of the pandemic, the RIHA provides similar benefits to X-Road, in providing continuity in e-service provision, a common place to catalogue available information systems, access to relevant data, and the ability for interested entities to join the X-Road. These functionalities are not only convenient, but wholly necessary during lockdown restrictions, as such functions can be carried out free of in-person interaction. Furthermore, the RIA's cybersecurity functions protect the security of the RIHA's systems, free of disruption or manipulation. This is exceptionally vital in the midst of the pandemic where, by several

[62] Republic of Estonia Information System Authority, "Information System Authority," n.d.

[63] Republic of Estonia Information System Authority, "Introduction and Structure," 28 May, 2020.

[64] Republic of Estonia Information System Authority, "CERT-EE," 24 January, 2020.

benchmarks, global levels of cyberattacks have increased significantly.[65]

State Portal

The state portal, www.eesti.ee., is landing place for e-service users in Estonia. By logging into the state portal using electronic identification for secure authentication, users can "view [their] personal information, use e-services and read messages sent by government."[66] Both streamlining and uniformity are key components of the state portal. Every ID-card holder in Estonia has been issued an email address by the Republic of Estonia, following the format 'firstname.surname@eesti.ee,' used as the main channel of communication between the state and person.[67] As of March 2020, approximately coinciding with the onset of the COVID-19 pandemic, more than 128,000 people, almost 10% of the Estonian population, had such an email address.[68] Additionally, the state portal utilises the 'only once principle' (OOP), which dictates that a piece of information only needs to be provided to the state once. According to Krimmer et al., OOP provides myriad benefits, including "reducing the administrative burden on users and businesses," like the time and

[65] See: World Economic Forum, "The Global Risks Report 2021," 19 January, 2021; Shannon Williams, "Cyberattacks up 400% Compared to Pre-COVID-19 Levels," 2 October, 2020.

[66] n.a., "eesti.ee," n.d.

[67] ID.ee, "@eesti.ee E-mail Address," n.d.

[68] ID.ee, "@eesti.ee E-mail Addresses are Becoming More and More Popular," 20 March, 2020.

cost of collecting information.[69] Under normal circumstances, these streamlining efforts are tremendously convenient, but amidst a pandemic, they are essential. These measures allow citizens and the state to focus their attention elsewhere, avoiding chasing up non-uniform email addresses, information already provided to the state, or other administrative tasks that may arise. Furthermore, the state portal offers a comprehensive, forward-facing portal, a 'face', in essence, of Estonian digital government. While it is important that this portal remain accessible to its existing users, it is perhaps even more critical that its comprehensiveness and usability extends to new users being forced online amidst the pandemic.

Education System

The Estonian education system is comprised of non-compulsory early childhood education, then primary and lower secondary school, and secondary school, over the ages of 3 to 19. Students may attend university, or technical or vocational college. Says Lees, "one of the aspects that gave [the] Estonian education system a good starting point in 1990s, when the independence was regained, was that Estonia had permission to deviate from Soviet Union requirements" including the Soviet structure and duration of education, and the curriculum.[70] As with Estonian banks in the 1990s, the end of the Soviet system

[69] Robert Krimmer, Tarmo Kalvet, Maarja Olesk, and Aleksandrs Cepilovs, "Exploring and Demonstrating the Once-Only Principle: A European Perspective," *Proceedings of the 18th Annual Conference on Digital Government Research*, Staten Island, USA (2017), p. 1.

[70] National Center on Education and the Economy, "Estonia: Learning Systems," n.d., p. 4.

effectively provided a 'blank state' whereby an entirely new education system could be crafted. The Tiger Leap programme of the 1990s signalled significant advancement of digital literacy and ICT knowledge in Estonian classrooms. The 2007 cyberattack also provided an impetus for further digital education; measures were largely undertaken to enhance national cybersecurity, through targeted awareness and education.[71] These opportunities ranged from new Master's programmes at Estonian universities training more experts in the field, to expanding the public's understanding of ICT in everyday applications. Between 2006 and 2015, e-learning developments included the newsletter *e-Oppe Uddiskiri* exploring issues "such as the quality of e-courses [...] new technological solutions, teaching and learning methodologies," and an annual e-learning conference.[72] At this time, e-learning was predominantly used "as a support for classroom learning," while there was also special funding for ICT studies in universities.[73]

Preceding the COVID-19 pandemic, the Estonian Ministry of Education and Research adopted the *Estonian Lifelong Learning Strategy 2020* in 2014, an agenda for providing continued learning opportunities for all Estonians throughout their lives, in formal education and beyond. This agenda features "a digital focus in

[71] Christian Czosseck, Rain Ottis, and Anna-Maria Talihärm. "Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security," *European Conference on Information Warfare and Security*, Reading, UK (2018), p. 58, 62.

[72] Heli Aru-Chabilan, "Tiger Leap for Digital Turn in the Estonian Education," *Educational Media International* 57, no. 1 (2020), p. 65.

[73] Ibid, p. 64-65.

lifelong learning," aiming to integrate new digital infrastructures – personal digital devices, interoperable information systems, open linked data, cloud computing, and more – in a "new approach to learning and an increase in the quality of education."[74] Its five very detailed strategic measures for achieving this goal include the development of a "digital culture" in education, enabling digital learning resources for schools, increasing accessibility of digital infrastructure, assessing digital competence, and providing "learning opportunities for adults to acquire digital competences."[75] Immediately preceding the onset of the pandemic, teaching at various levels of the Estonian education system was still largely undertaken in-person. This meant that a move online amidst the lockdown prompted a more marked change than with other government provisions already offered as e-services. However, the exploration of e-learning opportunities, the teaching of ICTs, and other measures predating the pandemic meant that there was some preparedness for the move to fully online education.

Estonian E-Government Amidst the Pandemic

This section will examine new developments in Estonian e-government that have taken place since the onset of COVID-19 in March 2020, until February 2021. Such developments, prompted by new pandemic-related realities, emerged almost immediately after the

[74] Republic of Estonia Ministry of Education and Research, "The Estonian Lifelong Learning Strategy 2020," 2014, p. 14.
[75] Ibid, p. 15-16.

emergency situation was instituted in Estonia in March 2020, and have continued to date. Estonia has since seen an expansion of e-services, beyond the existing body of approximately 5000 services, with many developments related directly to the pandemic. Initial lockdown restrictions saw Estonian education move to exclusively remote learning, although with the end of the emergency situation in May 2020, the provision of education has varied between hybrids of in-person and remote learning. The HOIA contact tracing app was an entirely new provision to emerge from the pandemic, necessitated by the need to identify infected persons and attempt to stop the spread of COVID-19. There were additional developments involving international adoption of Estonian e-government practices, however, its international applicability will be considered in the following section.

Expansion of E-Services

At the onset of the pandemic, there were already a broad array of e-services in place and readily available in Estonia. However, especially with the specific needs of Estonian citizenry that arose from the pandemic, there emerged an opportunity to expand the body of e-services, uniquely tailored to new COVID-19-related realities. One such responses was fully online 'hackathons,' whereby participants – typically with some knowledge or expertise of digital services – collaborate to brainstorm and develop potential solutions. For 48 hours from 13-15 March, 2020, the *Hack the Crisis* hackathon was jointly hosted by Tallinn-based hackathon platform Garage48 and Enterprise Estonia. At this event, teams generated solutions to mitigate various impacts of the pandemic. Among the hackathon's ideas that ultimately came to fruition is Koroonakart, a live map and compilation of up-to-date COVID-19 statistics in Estonia, collated from the Estonian Health Board, Land Board, and Statistics Estonia.[76] Further e-services developed at the hackathon include statebots or chatbots, designed to answer pandemic-related questions in Estonian and English, based on information from state authorities, the World Health Organisation, and Johns Hopkins University.[77] *Forbes'* Robert Walcott applauded the hackathon: "what is truly breathtaking is *how fast everyone mobilised*," he said, crediting Estonia's advanced digitisation and existing digital infrastructure.[78] It is notable that the hackathon began the day after the emergency situation was declared in Estonia.

Early media coverage of Estonia's digital government, and its effectiveness amidst COVID-19, pointed out that the only government service provisions that could not be completed online were marriage, divorce, and real estate transactions; this has changed since the onset of the pandemic. Previously, meetings with notaries were required to sign off on necessary documents for real estate transactions, an interaction that became impossible with lockdown restrictions. The solution to this issue came via remote authentication

[76] Koroonakart, "Koroonakart," 9 February, 2021; e-Estonia, "Digital Solutions from e-Estonia to Combat COVID-19 Crisis," n.d.

[77] Accelerate Estonia, "Hack the Crisis: From Idea to Execution in Just 6 Hours," n.d.

[78] Robert Wolcott, "Hack-The-Crisis: 6 Lessons From Estonia's Coronavirus Response," 15 March, 2020.

and facial recognition: Estonia-founded international identity verification platform, Veriff, uses remote verification to confirm the identity of the involved parties: notaries, the bank, and buyers and sellers.[79] This technology was originally developed for Estonia's e-residency programme, but was repurposed to help avoid face-to-face meetings during the pandemic. It is an important distinction that this service is not obligatory; it is at the discretion of notaries to determine whether they will use remote authentication. However, this now means that remote authentication to verify identity, then perform notarial acts, can be conducted either by notaries or in an Estonian embassy.[80] This represents an expansion of e-services, prompted by the pandemic, to include real estate transactions, as well as transactions of shares in a limited company and the authentication of power of attorney, but does not include the certification of a contract of marriage or divorce.

Education

As discussed previously, Estonian education had been a predominantly in-person endeavour before the pandemic. While digital and ICT-based education had been a part of Estonian classrooms dating back to the 1990s, and e-learning opportunities had been explored as early as the 2000s, the latter was largely supplementary to classroom-based learning. It is also notable that

[79] e-Estonia, "Digital Solutions from e-Estonia to Combat COVID-19 Crisis," n.d.
[80] Notarite Koda, "Remote Authentication and Facial Recognition," 3 September, 2020.

Estonian education provision is not uniform – with the different levels and types of education outlined previously – nor linear, with the state of emergency and lockdown restrictions varying over time since the onset of the pandemic. When the emergency situation was declared in March 2020, Estonian educational institutions had a turnaround of about four days before moving online. The ministry did, however, provide a catalogue of potentially useful software, applications, and other resources that institutions and educators could select from.[81] Estonian platforms such as e-Kool, a school management platform for teachers, students, and parents, whose use was already widespread before the pandemic, saw even further growth in their usership.[82] In addition to existing educational platforms in e-learning, the move online with COVID-19 prompted much innovation in Estonia. From the aforementioned hackathons emerged e-learning solutions such as Tutor.id, a platform connecting students with tutors for private online tutoring sessions in 220 subjects.

Makarychev and Romashko point out that many of COVID-19-related provisions, including in the field of education, were suggested rather than enforced legally, with the goal of establishing new norms, but this did not always materialise.[83] There is a great deal of disagreement surrounding the success of Estonia's move toward

[81] See the ministry's database of e-learning resources at https://docs.google.com/spreadsheets/d/1ls-q_RksZ89JxXxQ_M5-XJ9UPIYspNJVmmXq_yCYpVQ/htmlview#gid=0

[82] Tanel Keres, "Organising School Life in Modern Times," 12 September, 2020.

[83] Andrey Makarychev and Tatiana Romashko, "Precarious Sovereignty in a Post-Liberal Europe: The COVID-19 Emergency in Estonia and Finland," *Chinese Political Science Review* 6 (2021), p. 70-71.

remote learning amidst COVID-19, and the verdict of its overall body of e-learning, both pre-dating and since the start of the pandemic. One camp argues that Estonian education has been able to "successfully handle the coronavirus crisis," given that "Estonian schools managed to adapt to new situations quickly.[84] Aru-Chabilan says this is because "long-lasting focus on integrating technology into learning has paid off," while Urmo Uiboleht of the Tartu Private School Board attributes this success to the high digital competencies of Estonian teachers.[85] At the end of the emergency period, the Ministry of Education and Research provided data to suggest that there had not been any spike in students missing primary or secondary studies.[86]

Conversely, critics have argued that "[Estonian schools] were not up for the task, nor had the needed services for a complete switch to online distance learning. Teachers and schools were left on their own to decide which systems and services to use."[87] Essentially, the education ministry's laissez-faire approach was detrimental, as more directive was needed in an uncertain and unprecedented emergency situation. Further concerns were raised about the accessibility of devices – laptops, tablets, desktop computers – for e-learning, as well

[84] Kadi Raal, "What Helped Estonian Schools Successfully Handle the Coronavirus Crisis," 14 September, 2020.

[85] Quoted in Ibid.

[86] ERR, "Distance Learning has not Caused Spike in Number of Kids Missing Education," 17 May, 2020.

[87] Keegan McBride, "Image of 'Digital Baltics' Cracks Under Weight of Pandemic – Analysis," 2 February, 2021.

as Internet connection.[88] Despite claims that pen and paper could still be used in the event that a student did not have Internet access, there were instances of equipment being rented out or donated to students otherwise unable to obtain them.[89] In April 2020, the e-Kool platform suffered a cyberattack, further compounding concerns about the feasibility and reliability of e-learning services, from a security standpoint.[90]

An education ministry directive from 2015 indicated a €40 million investment to "ensure that by 2020 it will be possible, where desired, for all teaching and learning in schools to take place digitally [...] e-study materials will be developed and made more widely available and a gradual transition will be made to completely paper-free e-exams."[91] With the onset of COVID-19, lockdown restrictions meant that a move to e-learning was not a matter of 'where desired,' but a necessity in the midst of a pandemic. By most measures, this goal was not achieved; a move to full e-learning only took place with the onset of the pandemic, and this transition was undertaken very quickly. This showcased Estonia's existing digital infrastructure and the e-learning mechanisms already in force, which placed it far ahead of more traditionally analogue education systems. Simultaneously, it exposed the shortcomings of the Estonian e-learning environment: its

[88] Aivar Pau, "Kõik Eesti Õpilased Siirduvad Homsset Koduõppele – Kuidas See Tehniliselt Välja Näeb," 16 March, 2020.

[89] ERR, "More than 1,000 Computers Donated to Help Pupils, but More Needed in Tartu," 10 April, 2020.

[90] Eesti Ekspress, "eKool Langes Küberrünnaku Alla," 15 April, 2020.

[91] Argo Kerb, "Minister Ligi: All School Studies Digital by 2020," 24 July, 2015.

excessive flexibility and lack of definitive directive, accessibility issues, and cybersecurity risks. The shift toward e-learning is a relatively new and demanding undertaking; the consensus from both critics and proponents of this process is that the improvement of e-learning practices in Estonia must continue.

HOIA Contact Tracing App

HOIA is a COVID-19 contact tracing and notification application, unveiled on 20th August, 2020, and owned by the Estonian Health Board within the Ministry of Social Affairs. The app uses Bluetooth low energy technology (BLE), whereby devices with the app installed pick up Bluetooth signals from other nearby devices, collecting and storing anonymous data codes; users who become infected with COVID-19 can notify the HOIA app, which then notifies those who have been in close contact.[92] The Estonian Health Board's website maintains that "using the app is private and secure," as well as in accordance with the EU's GDPR.[93] By February 2021, less than five months after its release, the HOIA app had been downloaded more than 261,000 times.[94] The website of the Estonian Health Board, along with other government websites and news media outlets have widely encouraged Estonians to download the HOIA app

[92] Justin Petrone, "Estonia's Coronavirus App HOIA – The Product of a Unique, Private-Public Partnership," September 2020.

[93] Republic of Estonia Health Board, "Phone Application 'HOIA' Privacy Policy," n.d.; however, this website notes that it is not possible to implement some Chapter III rights.

[94] Republic of Estonia Health Board, "Coronavirus Dataset," 8 February, 2021.

as a means of stopping the spread of COVID-19, with a common rhetoric of protecting "ourselves and our closest ones."[95]

The HOIA app was the result of a PPP between the Estonian government and a consortium of 12 companies. Approximately 30 experts worked on the app's creation, across disciplines – design, software development, security, and marketing – to deliver the app to the Estonian Health Board free of charge.[96] The Estonian creators of the HOIA app "did not build [their] application from scratch," but rather, "built on the analysis and work of internationally recognised teams."[97] The first instance of BLE contact tracing was the Singaporean government's *TraceTogether* app, released in March 2020. However, this app did not have a sufficient level of privacy protection to be adopted in Estonia, so the Swiss model of decentralised privacy-protecting proximity tracing (DP-3T) was incorporated into the HOIA app. At the time of HOIA's release, then-Minister of Social Affairs Tanel Kiik called the app an "effective tool for all of use to reduce potential infectious contact."[98] Liisa Past, of Cybernetica AS, one of the 12 companies involved in creating the

[95] Republic of Estonia Health Board, "HOIA," n.d.

[96] Harri Kirik, "Creating HOIA – The Story of Estonian Coronavirus Contact Notification Application," n.d.

[97] Quoted in Justin Petrone, "Estonia's Coronavirus App HOIA – The Product of a Unique, Private-Public Partnership," September 2020.

[98] Eva Lehtla, "The Estonian Coronavirus Mobile Application is Now Available for Download," 20 August, 2020.

app, applauded HOIA as contract-tracing done in a "truly privacy-preserving way."[99]

However, not all Estonians shares this enthusiasm for HOIA. Ratings for the app on Apple's App Store and Google Play complain that HOIA is confusing, difficult to use, or does not work properly on their device.[100] A *Delfi* op-ed from Raimo Poom criticised HOIA as "too voluntary, too complicated."[101] Because the app is not mandatory, the onus falls on users to declare a positive COVID-19 test; infected persons often will not do so, whether due to the stigma of contracting COVID-19, or difficulties with the app itself. As of February 2021, of more than 45,000 cases of COVID-19 in Estonia since the start of the pandemic, only about 3000 cases had been reported in the HOIA app.[102] These concerns are echoed in scholarly literature on early COVID-19 contact tracing apps pre-dating HOIA. Riemer et al emphasise that "proximity tracing [using Bluetooth technology] will only be effective and achieve its intended health, economic and societal benefits if a significant user base adopts and

[99] Liisa Past, "Securing Accelerated Digital Transformation: How to Best Survive the Global Pandemic," 27 January, 2021.

[100] Reviews for the HOIA app can be viewed in their entirety on the Apple App Store (https://apps.apple.com/app/id1515441601) and Google Play Store (https://play.google.com/store/apps/details?id=ee.tehik.hoia&hl=en).

[101] Raimo Poom, "HOIA Äpp ei Täida Eesmärki. Parandused on Vaidlutesse Takerdunud," 18 January, 2021.

[102] Republic of Estonia Health Board, "Coronavirus Dataset," 8 February, 2021; it is worth noting that the HOIA app was not in place until August 2020, but Estonia had cases of COVID-19 from February 2020, so there is not a direct alignment of these timelines.

uses the service."[103] They note that a populace may resist the adoption of a contact tracing service due to privacy concerns, effort or difficulty with installing the app, or perception that they can benefit without adopting the app.[104] In the Estonian case, the second of these factors seems the greatest impediment to HOIA's adoption, and thus, its effectiveness. Beyond the effort of installing the app, difficulties that arise in using the app create an additional barrier.

Notably, unlike other digital service provisions examined in this section, HOIA is an entirely new provision. It is not an expansion of existing e-services, nor a field where digitisation was previously explored, even if not adopted in full, like education. HOIA's newness stems from the urgency of the pandemic and a need to adapt amidst new social realities. Thus, it is perhaps logical, as Poom writes, that the PPP responsible for creating HOIA is particularly slow at remedying the issues that Estonians have identified with the app.[105] It remains unclear if and how these issues may be addressed by the involved consortium. In late 2020, it was announced that work to ensure HOIA's compatibility across European borders would begin in December, after Latvia's COVID-19 contact tracing app, *Apturi*

[103] Kai Riemer, Raffaele Ciriello, Sandra Peter, and Daniel Schlagwein, "Digital Contact-Tracing Adoption in the COVID-19 Pandemic: IT Governance for Collective Action at the Societal Level," *European Journal of Information Systems* 29, no. 6 (2020), p. 731.

[104] Ibid, p. 731-732.

[105] Raimo Poom, "HOIA Äpp ei Täida Eesmärki. Parandused on Vaidlutesse Takerdunud," 18 January, 2021.

Covid, was functional Europe-wide, but it has yet to be seen how these functionalities may be applicable cross-border.[106]

Estonian E-Government Beyond Estonia's Border

For as long as Estonia has been innovating digital solutions, it has never sought to keep these advancements to itself, but rather, endeavoured to share them with the world. Estonia has provided a model for a data exchange platform, electronic identification and ID-cards, cybersecurity, and more, which entities have emulated and adopted. One such prominent example is the X-Road, which was trialled in places like Sweden and Azerbaijan pre-dating COVID-19. Several mechanisms exist for facilitating this cooperation: among them are the eGA, a non-profit organisation, and e-Estonia, a former non-profit now part of Enterprise Estonia. Both the eGA and e-Estonia tailor their purview and services depending on the needs of the interested entities. In Tonga, for example, this has meant developing foundations for eventual e-goverment architecture, cybersecurity consultations, and advising on national ID.[107] In Ukraine, eGA assistance was much broader, advising the Ministry for Digital Transformation on national- and local-level e-services, and establishing a Ukrainian iteration of the X-Road data exchange platform, called Trembita.[108] In October 2020, the World Health Organisation (WHO) signed a memorandum of understanding with

[106] ERR, "Development Work to Make Estonia's COID App Cross-Border Starts Next Month," 6 November, 2020.
[107] eGA, "Cyber Security Consultancy for Tonga,"n.d.
[108] eGA, "E-Government in Ukraine," n.d.

Estonia's then-Prime Minister Jüri Ratas in October 2020. This cooperation tasked Estonia with creating a "reliable and transparent cross-border exchange of vaccination data," based on the existing X-Road platform and KSI blockchain technology.[109] Even more recently, the Mexican state of Quintana Roo launched its own iteration of X-Road, Xacbé, to provide a backbone for state-level digital government.[110]

This prompts the question of why Estonian e-government has garnered so much attention, as it is not the only country pioneering in the e-government space, or even innovating data exchange layers. There is the availability, effectiveness, and efficiency of Estonian e-government, noted by Meyerhoff Nielsen, but this alone does not offer sufficient explanation. What sets Estonia apart from its counterparts is a combination of variables: Meyerhoff Nielsen's benchmarks, the effective branding of e-Estonia and the eGA, their highly tailored international outreach, and continual strategic assessment of Estonian e-government by government ministries or office of the Chief Information Officer (CIO). These factors are now compounded with COVID-19 and the need for rapid digitisation of government provisions. Thus, those seeking to adopt or expand their e-government have looked to the Estonian model, which has enjoyed success, offering opportunities for the expansion of Estonian e-

[109] ERR, "Estonia and World Health Organization Digitally Sign Cooperation Agreement," 6 October, 2020.

[110] Silver Tambur, "Estonia's X-Road Solution Launched in Mexico," 2 February, 2021.

government practices globally. As the European Union introduced its new digital strategy and regulation on data governance in 2020, there is the potential for Estonia to share its best practices, whether in the EU's transition toward a digital economy, introduction of e-services, cybersecurity, or other related fields.[111] However, if Estonian e-government practices are exported, there are contingencies on how and to what extent this can happen.

As Estonian e-government practices are put into practice in international settings, they must not be a copy-and-paste solution whereby Estonian processes are simply duplicated in full. Rather, several considerations, including local needs and intricacies – cultural, political, infrastructural, for example – must be taken into account. Estonian President Kersti Kaljulaid further raised that 'rushing online' during COVID-19 without sufficient security or interoperability "has a big risk for discrediting the idea of government digital service provision and damaging citizens' trust."[112] Former Estonian President Toomas Hendrik Ilves notes that Estonians typically trust their government in the provision of digital services, but that this trust may not be shared in other countries.[113] There is also the issue of adoption, both by people – the users of e-governance's services – and ministries, businesses or other entities, as the service

[111] European Commission, "The European Digital Strategy," n.d.; European Commission, "European Data Governance," 25 November, 2020.

[112] Kersti Kaljulaid, "Europe's Vision for Technology Leadership," 30 September, 2020.

[113] eGA, "Securing Elections in the Digital Era: Conference and Table-Top Exercise," 2 December, 2020.

providers. Solvak et al, and Paide et al have explored these concerns in their respective research; the former found some disparities across demographics, including gender and age group, in the adoption of e-services, while the latter detailed concerns from some private sector organisations that the accession process to the X-Road, specifically, was too bureaucratic, time-consuming, and complex.[114] If such concerns exist within Estonia, where e-government is comparatively well-established, then similar concerns would almost certainly arise in other settings.

Alongside public attitudes and adoption of digital government, concerns of underlying security must be addressed. One particular security concern expressed in scholarly work is trans-jurisdiction international data exchange; as X-Road, or variations of this platform, are adopted in cross-border settings, the integrity of data must transcend multiple jurisdictions.[115] Furthermore, "data stored at different locations may result in loss of transparency and hence generate inconsistencies," and thus, databases must include further mechanisms to detect and remove inconsistencies. The effective

[114] Mihkel Solvak, Taavi Unt, Dmitri Rozgonjuk, Andres Vork, Marten Veskimae, and Kristjan Vassil. "E-Governance Diffusion: Population Level e-Service Adoption Rates and Usage Patterns," *Telematics and Informatics* 36 (2019), p. 48-49; Karoline Paide, Ingrid Pappel, Heiko Vainsalu and Dirk Draheim, "On the Systematic Exploitation of the Estonian Data Exchange Layer X-Road for Strengthening Public-Private Partnerships," *Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance, Galway, Ireland* (2018), p. 38.

[115] Kim Hartmann and Christoph Steup, "On the Security of International Exchange Services for E-Governance Systems," *Datenschutz und Datensicherheit* 39 (2015), p. 475.

consideration of the aforementioned factors – local intricacies, trust in government, adoption, and security – increases the chances that the adoption of e-government practices goes smoothly, especially as rapid digitisation is being undertaken in various international settings as a response to the pandemic. Thus, the potential applications of Estonian e-government practices globally are immense.

Conclusion

By several of the benchmarks outlined throughout this paper, scholarly, think tank, media reporting, and other dialogues have indicated the success of Estonian e-government predating the pandemic, and the effectiveness of this structure since the onset of COVID-19. Its key components were well-established prior to the pandemic and have mitigated numerous challenges seen elsewhere, where digitisation had not progressed to the same extent. It has been commended for its availability, effectiveness, and efficiency, paired with effective branding and outreach, sparking great interest beyond Estonia's borders. What Estonian e-government is *not*, however, is the 'idol' that Kerikmäe, Ramiro Troitiño, and Shumilo describe, a model to be blindly revered as a 'one-size-fits-all' for other entities to adopt in full. It is not a perfect system, as has been evident both before and amidst new pandemic-related realities, but offers a compelling case study to learn from and emulate.

Responding to the realities of COVID-19, Estonian e-government experienced further innovation: an expansion in scope or nature of existing e-services, or entirely new platforms, as was the case with the HOIA app. Criticisms have emerged of various elements of this system, pertaining to new provisions, like HOIA, or the effectiveness of existing services amidst pandemic conditions, like education or certain e-services. Such is to be expected, as Estonian e-government is an imperfect system, albeit a very successful and globally recognised one. This does prompt questions of how this model can be improved, both inside of Estonia, and internationally, as elements of Estonian e-government expand into global settings. This paper has outlined considerations, both surrounding e-government inside of Estonia, and also around the exportation of Estonian digital government practices, related to the intricacies of security, adoption, and public opinion. Both proponents and critics of various elements of Estonian e-government have voiced a similar sentiment: that this model *must* keep improving. Estonian e-government has successfully mitigated numerous challenges associated with the pandemic, but improvement and adaptation must continue. Strategic assessment of e-government's performance, as well as the consideration of new intricacies and realities that arise, should be undertaken and implemented to ensure the continued success of Estonia's e-government system beyond COVID-19.

Logan Carmichael is a PhD Student in Political Science and Junior Research Fellow in E-Governance at the Johan Skytte Institute of Political Studies at the University of Tartu in Estonia. Her research focus is on e-governance, cybersecurity policy, and national security in the Baltic neighbourhood. She previously completed a Masters of Conflict and Terrorism Studies degree at the University of Auckland and worked as a professional tutor and guest lecturer at UoA, as well as in cybersecurity in the New Zealand private sector.