8

Estonia's Digital Transformation

Mission Mystique and the Hiding Hand

Rainer Kattel and Ines Mergel

A Digital Success Story

In 2017, *The New Yorker* published a story titled 'Estonia, the Digital Republic' (Heller 2017). The article's subtitle was 'Its Government is Virtual, Borderless, Blockchained, and Secure. Has this Tiny Post-Soviet Nation Found the Way of the Future?' It summarizes the buzz around Estonia's digital transformation: from the outside, at least, it is seen as a major success and has been lauded in mainstream media such as the *New York Times*, *Financial Times*, and *Forbes* (Scott 2014; Crouch 2015; Gaskell 2017). In these, Estonia's success in digital government is frequently described in parallel with its thriving ICT industry, best exemplified by Skype which originated and is still primarily based in Estonia and which was subsequently acquired by Microsoft.

The Estonian e-government infrastructure and its success rest on two main pillars, both introduced in 2001, that essentially create a digital state and digital citizens: the data infrastructure X-Road and a compulsory national digital ID (Kalvet and Aaviksoo 2008; Kalvet 2012; Margetts and Naumann 2016). X-Road is an interoperability platform for existing decentralized databases and a data exchange layer that can be used by public and private sector actors. It is independent of platforms and architectures and provides secure interoperability for data exchanges and identification of trusted actors in digital service delivery. The digital ID makes it possible for citizens to be identified digitally and to use digital signatures. Together, X-Road and the digital ID make it possible to digitally sign any contract, access essentially any public service such citizens' digital medical history, order prescriptions, file taxes, vote, and so forth. More than 2,300 public and private services use X-Road, and the digital signature has been used almost

350 million times by Estonia's population of 1.3 million. The digital ID penetration is close to 100 per cent; 30 per cent of votes are cast digitally (in both local and national elections); almost all personal income tax declarations and medical prescriptions are done online, and most medical records held by hospital and family doctors are accessible online. The Estonian government claims that its e-government infrastructure has annually led to savings of about 2 per cent of GDP and more than 800 years in working time for public and private sector in a calendar year.[1]

According to the EU's Digital Economy and Society Index (DESI) for 2017, Estonia is the leading nation in Europe in digital public services (it dropped to second place in 2018). However, in most other e-government rankings, Estonia's digital success is less evident. In DESI's overall ranking, Estonia is featured in the ninth spot for 2018, and it is ranked only sixteenth globally, according to the UN's 2018 e-government survey.[2] This mismatch—high praise and leadership position in global news outlets vs. relatively middling rankings in overall digital transformation indexes[3]—reflects the nature of Estonia's digital success: Estonia is ranked high for its digital public service *infrastructure*, universally available and mandatory, as an integral backbone of public service delivery. Estonia's digital success, however, is *not* about other digital offerings such as digital democracy, citizen engagement, or digitally transforming public services such as the welfare state.

The specific nature of Estonia's digital achievement and at the same time the disconnect between technological infrastructure and degree of digital penetration are often overlooked in international coverage. Domestically it has become a crucial political and policy issue over the past few years. For instance, Kaja Kallas who heads the Reform Party since April 2018 (the Reform Party is one of the largest and most popular parties which has led various coalition governments over the past fifteen years until 2016 when it was forced into opposition) referred to the abovementioned less than stellar rankings in global indexes and argued that much of the e-government infrastructure is outdated and called for fundamental reforms in Estonian e-government (Kallas 2018). With the decision to focus its digital development on X-Road only, Estonia has effectively created its own legacy system—a move that the initial thinkers wanted to avoid. This realization comes amidst increasing domestic criticism of the so-called e-residency programme, launched in 2014 and highly lauded in international media, which essentially opens some of the X-Road and digital ID-based services globally (Tammpuu and Masso 2018).[4]

In order to assess Estonia's digital transformation along the three dimensions deployed in this book—programmatic, policy and political success—it is important to note that Estonia's case is a success of a national strategy rather than of a single policy or even a bundle of programmes. Indeed, Estonia's digital initiative does not arise from a documented foundational policy or strategy, or even

documented discussion and debate. The government's e-government strategy document, *Principles of Estonian Information Policy* (1998) approved by the Estonian parliament in 1998, which was seen as the critical scene-setter for digital transformation in the 1990s (Kalvet 2007), does not mention any of the fundamental principles or developments that took place just a few years later. It can therefore be argued that the Estonian digital transformation is characterized by 'development-driven strategies' rather than by 'strategy-driven development' (Kalvet 2007: 11).[5]

Furthermore, Estonia has never had a central office for digital transformation like other countries that have set out on the digital transformation journey, such as the UK's Government Digital Service (GDS), despite the fact that such a central agency was initially envisioned to manage (among other things) vital public registries (Estonia's Roadmap to Information Society 1994). Nor is there a formally designated and empowered state official for digital enablement: the current government Chief Information Officer position exists only in English translation, and only informally.[6]

Estonia's digital transformation has been an extended and ongoing process over three decades, starting in the early 1990s when Estonia regained its independence and continuing to the present day. It was informed by successive debates and developments, and multiple policy initiatives. Much of this process has been ad hoc and informal. For example, many strategic policy documents for digital transformation have followed the rhythms of European (structural) funding periods rather than responding to domestic challenges and planning processes.[7] Similarly, various overlapping and mostly self-managed public–private networks provided the informal dynamic capacity and capability for change, few of which have been institutionalized or formalized.

However, a fundamental constant in Estonia's digital transformation has been widespread cross-party support for the digital agenda. Starting with the first independent government in 1992, ICT development in society was seen as delivering competitive advantage, as a symbol for leaving the Soviet past behind, and as an indicator for opening the Estonian society and economy towards the West. Digital transformation as a vision was part of a broader political consensus at the time that included the agreement to join the European Union and NATO. To this day, the digital agenda enjoys widespread political support. It has become part of Estonia's official image and branding as evidenced by the e-Estonia showroom (https://e-estonia.com), almost a mandatory stop of any official state visit.

In the following, we review past events and decisions to untangle the essential elements and distinctive features of Estonia's digital government success. We examine whether the success factors and drivers of the past decades can be relied on to ensure this success endures and delivers the next generation of digital transformation policies in Estonia.

Contexts, Challenges, Agents

History and the Hiding Hand

In 1990, Estonian state-owned electronics companies employed 26,000 people—this is more than today despite electronics being one of the principal and highly successful export articles over the past twenty years (Ubar 1993; Tamkivi 2017). Yet Estonia's electronics industry, and its transformation from the Soviet legacy systems into an integral part of Scandinavia's global value chains, has almost nothing to do with Estonia's digital government. So why and how did digital government emerge as a paradigm next to and competing with electronics and industry in general? In other words, why did not digital transformation follow the path of the 'invisible hand' of free-market reforms—a set of ideas so dominant in Estonia from the 1990s onward?

Two crucial political circumstances in the 1990s provide the answer. First, after regaining independence in 1991, the first free elections in Estonia brought to power political forces that were intent on cutting ties to Soviet legacies in all aspects of society. Some developments were inevitable: as the Soviet planning system collapsed, so did export markets to the east, and companies needed to transform themselves into privately owned entities relying on domestic (and mostly Western) markets (Reinert and Kattel 2004). Others came from political will, such as consciously embracing recent Western technologies, products, and services rather than attempting to upgrade inherited Soviet technical, production, and service systems (Drechsler 1995). This resulted, for instance, in changes to the funding and governance of R&D, the privatization of state-owned companies, and transformation of the finance sector—all following a guiding political principle of transition by replacement (Kattel 2012). This proved particularly crucial for ICT because it encouraged a focus on new IT solutions as opposed to large-scale centralized legacy systems in both private and public sectors, also excluding Western legacy systems available in the form of development aid.

Transition as replacement was complemented with a political idea underpinned by the same ideological principle: namely, to 'leapfrog' the West's technology. Here the success of Finland and Nokia became one of the guiding political reference points: 'What is our Nokia?' asked Lennart Meri, Estonia's first president after Estonia regained independence in 1991, a question that has remained a popular catchphrase. As Estonia seemed to lack the political will and economic capacity to build its own significant industry, the focus turned to develop what might be labelled as a general purpose technology. In other words, rather than developing specific IT and electronics industries, the political focus was on developing IT as a general purpose socio-economic skill to be shared by as many citizens as possible.

These twin ideas laid the groundwork for three critical features of Estonia's digital transformation that are still dominant today:

1. Focus on future-oriented and almost utopian solutions—the realm of 'crazy ideas', as expressed by Mart Laar, prime minister from 1992–4 and 1999–2002.

2. Public digital architecture should be universal in nature.

3. Decentralized digital agendas (including databases) of line ministries.

Thus, in its purest form, Estonia's digital transformation can be seen as a strategy to leapfrog rather than just catch up with the West (Burlamaqui and Kattel 2016). In this view, widely shared among the emerging policy networks in the early 1990s, the Soviet occupation that lasted over five decades is seen as a lost time. This implied a particular glorification of what can be called the first republic, which lasted from 1918 until 1940. Following its independence, Estonia not only reissued the *kroon*, its currency from the interwar period, but also based its new constitution on its previous constitutions from 1920 and 1938—indicating its reliance on traditional values. The digital initiative epitomized the other component of the new republic's dual ambition: to be the state and the society that it was in the interwar period *and* to leapfrog the West in development.

However, two significant differences exist between Estonia in the 1930s and the 1990s: the ethnic composition of its society and its economic structure. In 1934, 88 per cent of inhabitants were Estonian, and this increased to 97 per cent after mass emigration during the Second World War. In subsequent decades this trend reversed as people, mostly ethnic Russians and Ukrainians, were encouraged by the Soviet government to move to Estonia from the Soviet Union. By 1989 the share of native Estonians dropped to as low as 62 per cent; in north-eastern Estonia, the percentage of Estonians decreased to 13 per cent in 1989 (from 65 per cent in 1934) (Estonian Statistics n.d.). These shifts in the population were associated with rapid industrialization, particularly in north-eastern Estonia, that created a long-standing high demand for labour (Rajasalu 2002). Plans for even more investment into resource-intensive heavy industry and mining—and fears of new waves of immigration—played a crucial role in galvanizing the popular independence movement in the late 1980s around environmental protection issues (Manning 2007).

This confluence of industrialization with ethnic tensions explains why Estonia, despite being one of the most economically and technologically advanced countries within the Soviet Union, chose not to upgrade the inherited economy and instead sought to do something completely different. As an emerging general-purpose technology, ICT offered an almost perfect solution, particularly given the availability of R&D skills in this sector. 'The digital' thus came to express Estonia's—or more precisely, its elite's—ambitions, and explains why to this day, the 'digital elite' is almost entirely ethnically Estonian.

The role of 'crazy' ideas was initially also part of Estonia's economic policy. For example, Estonia introduced a relatively unique currency board to manage its currency, and a flat income tax rate (both rare in Western or other economies).

The first prime minister after regaining independence, Mart Laar, was openly radically neoliberal, citing Milton Friedman and counting Margaret Thatcher among his friends. Also, the success of these reforms brought international recognition and gave Laar and others confidence to pursue further radical ideas. This contributed largely to Estonia's rise as the extreme and successful reformer in the eyes of the international community—and as the main disciple of Adam Smith's famed 'invisible hand'-led economic policies whereby free markets provide the best economic outcomes. The implementation of 'invisible hand' infused policies by the first Laar government in 1992–4 relied upon the enthusiasm of amateur politicians, who drew at least part of their risk-taking courage from their naïvety. This process is well described by Albert Hirschman (1967), whose principle of the 'hiding hand' notes that policy-makers sometimes take on tasks without realizing the risks involved, and this may result in unexpected creativity and success. Hirschman argues the hiding hand works through ignorance of ignorance, and Laar agrees: 'I was 32, I was young and crazy, so I didn't know what is possible and what's not, so I did impossible things' (Laar 2010). In digital government, this did not lead to free-market based solutions, but rather to visionary policies that relied on charismatic leadership, small tight networks, and constant renewal of both leadership and networks.

External Influences and Skills

The academic elite played a vital role in the early genesis of Estonia's digital transformation. Mart Laar recalls how one of the first things that came onto his desk as prime minister was a memo by Raimund Ubar, professor of computer engineering at Tallinn University of Technology, titled 'Targeted program for Estonian electronics and computer technology' (Ubar 1993). The purpose of the memo was to convince the government to establish an R&D programme in electronics and computer engineering to upgrade Estonia's industry. While Ubar's memo focused on industry and applied research, what seemed to have impressed Laar was Ubar's insistence on avoiding the legacy trap he had observed in Western countries and encouraging a policy of investment in future-oriented emerging technologies rather than in legacy technology. Laar recalls: 'Ubar wrote that it is not sensible to overreact and start immediately by buying things. He was the first person who told us not to buy anything old.'

The avoidance of this legacy trap allowed the policy-makers to avoid large-scale investments into ICT as budgetary means were scarce and capacity to develop centralized IT systems was low. Later, during Laar's second government (1999–2002) this became the unspoken *principle of frugality*: rather than buying large-scale solutions from established vendors, government departments and agencies were encouraged to find open-source solutions. This also enforced departments and agencies to develop their own digital agendas.

In the initial decision-making processes, academics played a vital role as part of the first formal advisory body on ICT, the Informatics Council, established in 1990. The focus on cyber security, a prominent feature of the X-Road, can be traced back to the Informatics Council, as many of its members had a connection with the Estonian Academy of Sciences Institute of Cybernetics.[8] From this institute, Cybernetica AS was founded, one of the companies that delivers many of the public digital solutions, including X-Road. Academics were also the first to establish actual internet connections with the West through networks with Swedish colleagues (Högselius 2005).

Proximity to Scandinavia played an essential role in building the ICT landscape in Estonia. The Estonian government reorganized the Ministry of Communications into two state-owned companies, Eesti Telekom and Eesti Post in 1991, decoupled from Soviet telecommunication networks and created a mobile joint-venture with Swedish and Finnish counterparts called Eesti Mobiiltelefon. This company initially used the NMT and not the GSM standard for mobile technology (as did the Nordic countries at the time). Eesti Telekom, in turn, acquired the monopoly rights for Estonia's fixed telephony until 2000, but the concession agreement left out mobile and data communications—and this proved critical in the years to come. Another joint venture between Estonia and the two Nordic countries, Eesti Telefon, was an important early investor into Estonia's digital infrastructure modernization (Högselius 2005: 81–91).

The R&D programme in electronics, proposed by Ubar to Laar, never materialized, but ICT gained importance as a cross-party policy goal throughout Laar's first administration. During Laar's second administration, between 1999 and 2002, many of the critical elements of Estonia's ICT policy coalesced into a more or less coherent framework and were quickly translated into swift and radical actions. Key to this development was Linnar Viik, a serial entrepreneur and later founder of the e-Government academy, as the ICT adviser to the prime minister. Viik became an influential adviser with a wide-reaching portfolio, more important and powerful than many of the ministers (Laar 2010).

As the digital experiment—and the modern republic—matured, political leadership in ICT became less about ideas and policies and more about recruiting talented IT people to work for the government. This was much helped by the fact that the Estonian civil service is designed as an open system: almost all positions can be filled through open competitive calls. Thus, for instance, Taavi Kotka, former CEO of Nortal, one of the largest domestic ICT companies, was hired as government 'Chief Information Officer' in 2013. Lack of legal and public barriers arising from the large-scale support of digital transformation helped attract talent from the private sector, as Kotka (interview) states:

> The good part was that in ICT there [were] very few legislation initiatives. It was mostly about inspiration, it was mostly about fixing investment processes, getting toward the right resources and strategies in place. It was more like organizing

work than working the policy or the legislation. ICT and cyber security are not regulated at all, basically. It's a very lightly regulated effort.

If the hiding hand style of strategic leadership was provided mostly by politicians in the 1990s, then in the 2000s it was provided increasingly by strategic advisers and recruits from some of the most prominent Estonian ICT companies.

Design and Choice

Following Ubar's guidance a fundamental principle of Estonia's digital transformation efforts was the idea of no legacy. As mentioned earlier, government ICT projects could not afford to build massive systems run by large vendors. Instead, the government was encouraged to embrace a distributed architecture of IT systems to cater to the different needs of each government agency. This became an explicit strategy from 1999 onwards: ministries were asked to build their IT systems according to their specific needs but ensuring frugality and interoperability across government. The resulting distributed architecture created the need for a software layer that allowed these distributed IT systems and databases to exchange data with each other.

Laar's second government rapidly expanded X-Road as a layer for secure data exchange for distributed public IT systems and databases, followed shortly after by digital signature and e-ID based on the unique personal code. Viik and others were able to tap into personal networks in the public and private sectors, for example with the banking sector, which helped develop competency in cyber security (Kerem 2003). In this way, the public ICT infrastructure—with its fundamental principles of governance: distributed data architecture and strategy, central strategic guidance and financial controls, decentralized implementation—worked with public–private networks to access competencies and increase legitimacy.

Despite this seemingly coherent strategic move, Estonia has never had a central digital agency, nor does it have centralized or even unified public databases. Instead, politicians and civil servants have relied on cross-sectorial networks to receive strategic advice in pushing their digital transformation agenda forward. Viik (interview) notes:

> The overall ICT policy coordination and formation were carried out by the, I would say as a central group of some 10 to 15 people, and the broader group involved some maybe 20, 25 persons who twice a year, sometimes three times a year had seminars and reviews on what we should do next.

This is highly unusual in the Estonian political and bureaucratic culture. Most neoliberal political cultures mistrust close-knit networks or the heavy influence of private sector actors on public sector representatives and are acutely sensitive

when it comes to corruption and erosion of accountability associated with such networks. In the Estonian ICT sector the networks and exchanges between the private sector and government operations rely heavily on each other's advice and guidance—and build the trusted backbone of its digital transformation efforts. As a matter of fact, belonging to these networks is more important than having a formal government role. This is even more remarkable in the Estonian context where in all other policy fields one of the key complaints is lack of cooperation and weak coordination structures (Randma-Liiv and Savi 2016).

Despite the potential accountability threat the ICT sector has remained relatively scandal-free over the past two decades, with little evidence of corruption, influence, or accountability issues. The most critical moment occurred in 2007 when Estonia became the first nation-state to fall victim to a coordinated Distributed Denial of Service (DDoS) cyber-attack in 2007 (Lesk 2007). The continued attacks led to the establishment of NATO's cyber security centre in Tallinn. Following the initial attack, the country had to repair its services by disconnecting from the internet for four weeks, and a strategic intent emerged that focused on collective rather than on individual actions. According to Andres Kütt, a principal adviser to the Estonian Information System's Authority:

> Strategically this is from where [the network] emerged. The ideology from it actually stems from what our former Director General Jaan Priisalu called the collective brain. Which is primarily behind the cyberwar ideology of Estonia. The doctrine is that in cyber conflict, the party who can amass the biggest collective brain wins. Because in the internet world, everything is interconnected, and no one single organization can withstand attacks or can sort of execute attacks en masse alone. You need to have that sort of collective brain. And the collective brain being distributed needs to work together, there needs to be trust between parties in that brain, so that network stems from that sort of ideology.

The close-knit network among high-profile politicians and their private sector IT advisers also emerged as a natural development from the fact that public–private partnerships initiated significant IT investments and digital services as joint ventures with Scandinavian state-owned companies and then mainly by the banking industry. With electronic banking proliferating in the late 1990s, banks were at the forefront in rolling out the national e-ID (initially bank offices issued e-IDs). Through the educational Tiger Leap and Look@World programmes in the late 1990s and early 2000s, the banks financed IT education in schools and for the broader population so that citizens could use their online services. In essence, the banks took over the task to train and inform citizens who might not be naturally drawn to conduct online transactions and preferred physical bank branches:

> The bank's self-interest was to not have a bank branch everywhere. They embraced electronic banking. So what they did for a while was to teach people in rural areas, especially older people, how to use computers.

The banks deployed training kiosks across the country to bring their clients online. Also, Hansapank, the leading bank at the time, built up the data infrastructure and hired cyber security specialists to protect the banking system. Some of the top cyber security people moved from banks to the government, which proved vital in responding to the DDoS attack in 2007 and paved the path for continuous personnel movement between sectors.

Delivery, Legitimacy, and Endurance

Estonia's early focus on integrating IT education with general school education was an essential factor in enabling digital transformation. Funded by both public and private sector organizations, the Tiger Leap programme was initiated by Jaak Aaviksoo and Toomas Hendrik Ilves in 1996: a first step was to bring all Estonian schools online. Private sector companies became involved in a co-sponsored public–private partnership called Look@World. Both programmes had an immediate effect on Estonian youth and led to the emergence of a vibrant IT start-up sector and arguably to improvements in government operations in recent years, as one official notes:

> The last several years, when I went around visiting Estonian start-ups, I always asked them why did they end up in technology, and they would say 'Oh, well I was a Tiger Leap child.' So now people in their mid-30s, are people who were 14 or 15 [when they] got online.

The subsequent success of IT start-ups such as Kazaa and Skype provided further stimulus:

> What really transformed young people's attitude was the success of Skype. Basically, there were four, at that time, young Estonians who after they managed to avoid doing prison time in the United States for inventing Kazaa, which was a file-swapping program, like Napster, and of course it violated copyright laws. And then the same group of four, because the technology concept's fairly similar, invented Skype. And the idea that in this sort of far away provincial, cold, rainy, backward backwater, which is kind of the concept young Estonians had of where they lived. You could send the career—some, some people who were good at math and science, would invent a worldwide brand, and become rich was an enormous motivating factor to get people interested in technology.

In particular, the Tiger Leap programme can be seen as a blueprint for how digital transformation was delivered. The programme was initiated in 1996 through a legally private foundation in which government was one of the founding members and key funders, alongside eleven IT companies. It created competitive grants and encouraged schools and local governments to submit applications for the

rather limited government funding for IT education programmes. In essence, this governance structure created a highly agile environment, where those willing to invest their time and energy could be easily engaged either as funders or participants, and it did not matter whether they belonged to the public or private sectors. Above all, such fluid structures allowed private actors—notably banks—to be heavily engaged in the Tiger Leap programmes. Importantly, foundation based structures allowed public–private networks to operate outside of government without much red tape—and without much institutionalization or formalization.

The networked cooperation between the public and the private sector occurred as a natural evolution: CEOs, non-profit managers, or academics are moving between different sectors, accept short-term appointments in government, or are asked to serve as strategic advisers to the Prime Minister and the President. The phenomenal success of Estonian IT start-ups, like Skype, gave rise to another powerful network of Estonians with ICT skills and members of its local start-up ecosystem (the 'Skype mafia'), mostly developers and entrepreneurs with shared values and ideas (see http://skypemafia.com). Thus, layers of trusted network relationships have evolved between public and private organizations that focus on exchanges and strategic planning initiatives. Many of those incorporate prominent Estonian IT companies, such as Cybernetica, Nortal, or Skype which are active in the cyber security, e-government, and banking industries.

Movement between sectors is not one-directional. Government agencies have, for example, signed a memorandum of understanding with Nortal, which allows the company to request government officials to work on international client projects abroad. Frequently, public managers are sent on leave to work on international projects, for example in Oman, lending deep public administration expertise and understanding of government systems to the private sector.

Another layer—beyond the consultative layer—is the information exchange and networking layer of cyber security experts who regularly meet as an informal group. Their goal is to exchange knowledge and good practices to protect the country's infrastructure against cyber-attacks. Ties among participants are extremely strong and take on a regulative function since the informal network members include representatives across all industry sectors. For instance, failing to fall in line with what is decided in terms of processes and technologies can lead to exclusion from the network. This has a real impact, as one of the network organizers explains:

> It is a small community, but it [can] still to an extent deliver. In the sense that, it is acknowledged that the formal mechanisms can get you that far, but true cooperation between parties only happens via personal contact. We need to have some level of personal rapport with people. Yes, at the end of the day, you can whack somebody with a piece of law, or regulation, or a process, yes, you can do that. But, it only works very limited. Has very limited effect.

The design principles of the Estonian digital transformation are a result of the strong political decision-making and networked governance. Some of these are ingrained in the policymaking culture, others in the explicit legal codex. The most influential design principles are not, however, codified in law or regulation; instead, they are followed by those in leadership positions in government. They bear the hallmarks of what can be dubbed a civic hacker culture that fuses start-up agility with design thinking. The once-only principle—designed to reduce the bureaucratic burden (Wimmer et al. 2017)—is a case in point. Citizens and businesses provide their information to government one time only and thereafter this information is available to all other government actors. In Estonia, this is a principle, not a law. As Kotka explains:

> It's not a law. People think it's a law, it's not a law, it's a principle. So, there's no law saying that the government can ask only once information from the people. This is so in the case of companies, but about the people it's a principle.

Similarly, the high level of interoperability made possible by components such as the X-Road data platform and its connected applications are also not mandated by law: 'Or the saying [that] an ICT system has to be interoperable with other systems. That's, again it's a principle. There's no legally binding regulation.'

Nor is it a rule that the Estonian public sector should not use IT technologies that are more than thirteen years old or avoid off-the-shelf IT systems offered by large international vendor companies. Instead, such principles emerged from early thinking typified by the Ubar memo, and are a reflection of the start-up culture of that time, of which Skype and its later alumni—'Skype mafia'—are examples.

This development of informal networks can be summarized as a specific kind of 'mission mystique' that spans organizational boundaries: a set of institution-strengthening characteristics and institutional charisma Goodsell (2011: 477–8). In the Estonian ICT sector, such mission mystique transcends organizational institutions and strengthens networks that are driven by common values and held together by (digitally savvy) charismatic leadership. Such mission mystique is essential for the hiding-hand principle by creating legitimacy for risk-taking and experimentation.

Analysis and Conclusions

At the core of Estonia's digital transformation is the idea of a digital citizen who accesses public and private services through a digital platform that ensures the interoperability of diverse and decentralized information systems. This relies on ideas that are counter-intuitive to free-market thinking and follow a principle characterized as the 'hiding hand' rather than the invisible hand. Two elements

were essential: first, the adoption by politicians and policy-makers of a culture of risk-taking and bold ideas; second, the formation of multiple overlapping small networks to promote early success and build momentum. These phenomena became mutually enforcing and enabled rapid adoption of innovative solutions.

To summarize, Estonia's digital transformation and its success rest on three key factors. First, a confluence of a number of contextual factors; second, on a set of agreed upon governance principles; and third, on a set of design principles:

Contextual Factors

- The Soviet legacy had left Estonia with an outdated industrial structure and widespread dislike of industrialization. More positively, it left Estonia with a wealth of R&D talent in ICT through various Academy of Sciences institutes, such as the Institute of Cybernetics (established in 1960) and other similarly highly advanced academic institutions. As their funding collapsed in the early 1990s, much talent poured into emerging private companies, in particular, various joint ventures with Scandinavian telecoms and other companies.

- Geographical vicinity to Scandinavia. In the 1990s, Nordic countries had one of the fastest developing telecommunications sectors globally. Opening up both policymaking processes (through advice and joint ventures) and markets (through privatization and regulations) to Scandinavian partners brought know-how and investment.

- Small size and population concentration. Estonia has 1.3 million inhabitants, almost one third in the capital, Tallinn. This clustering of population facilitated agile networks that were able to gain quick and lasting political support, and which required low initial infrastructure investment.

Governance Principles

- Government ministries and their agencies had direct responsibility for their ICT strategies, investments, and data—and information architecture and departmental ICT strategies were decentralized.

- A critical coordinating and guidance function in negotiating ICT investment decisions and the formulation of crucial design principles was performed in the centre. During the 1990s the prime minister's office played this vital role, and it is now coordinated by the Ministry of Economic Affairs and Communications.

- There was a deliberate focus on public–private networks rather than on individual organizations. Estonia's e-government landscape consists of a number of organizations (agencies such as Information System Authority, or departments within ministries such as Department of State Information Systems) and cross-organizational networks that are sometimes formalized (such as the Estonian Defence League's Cyber Unit[9]).

Design Principles

- No legacy principle: public digital infrastructure should not use technological solutions that are older than 13 years.
- Build-vs.-buy principle: particularly in the early stages of digital transformation, the priority was to build systems from scratch rather than buying 'off-the-shelf' software systems from ICT vendors.
- Once-only principle: businesses and citizens have to supply information for government authorities only once and data is available through the data exchange layer X-Road across government agencies.
- Interoperability and security principle: rather than seeking to create unified databases and information system, the focus is on secure interoperability of data systems.

Together, the coordination of strategy, social conditions and policy combined with a uniquely talented, motivated and relatively young workforce resulted in the creation of a public digital infrastructure that is recognizably world-class.

The rapid pace of change and the focus on digital citizen and identity nonetheless highlighted anomalies. In the first place, despite the statement of a strategic intent of participatory governance, innovation—and in fact the drive for digital initiatives—has come from a tight-knit elite network of politicians, business leaders, and civil servants and few ideas have emerged through co-creative processes with citizens. The recent e-residency programme is one of the only initiatives that places a strong focus on user feedback. Second, while e-ID and other advances have changed aspects of the user experience of crucial public services such as electronic tax declaration, the services themselves have remained remarkably unchanged. Third, while many digital services have brought efficiency gains to citizens and businesses in Estonia, citizen satisfaction with crucial services such as healthcare and education has remained low. As an example, according to OECD rankings in 2014, Estonia ranked fifth from bottom in satisfaction with health services (in 2007 it ranked the lowest), and second from bottom in satisfaction with education system (in 2007 it ranked third lowest). Further, Estonia performs poorly on some critical social indicators: for example, in 2016 it had the highest gender pay gap in Europe, and a higher than EU average Gini index (Eurostat). While citizen satisfaction is not the only

measure of the quality of public services—and digital infrastructure only one component in the provision of sophisticated services such as health and education—it is indicative that there is a little-measured improvement in the provision of core public services.

While decentralized digital agendas of line ministries provided needed agility, it also created uneven digital capabilities across different departments and agencies. This reliance on bottom-up departmental initiatives seems to necessitate stronger and perhaps more formalized coordination structures than are currently present. Furthermore, while e-voting is increasingly popular, other aspects of digital democracy such as civic engagement have remained weak (with a notable exception of the so-called Citizen Assembly between 2012 and 2014 that, however, eventually failed to deliver any significant results; see Jonsson 2015).

Finally, while distributed IT architecture is at the heart of Estonian digital transformation, the central X-Road layer represents a dependency: 'It's the X-Road or no road.' While Estonia has already successfully exported this proven infrastructure to other European countries, like Finland, there are alternative paradigms that do not rely on it (e.g. the UK's domain and platform focused approach).

Estonia's focus on ICT as general-purpose technology proved to be one of the critical success factors as it enabled the creation of digital infrastructure that is universal in nature. Yet, relying on decentralized and mostly informal networks in building this infrastructure, Estonia now faces a challenge to build capacities and capabilities within the public sector to take advantage of the public digital infrastructure. In sum, perhaps the most significant question faced by Estonian digital government is whether the main reasons for its success—particularly its charismatic leadership-based informal networks and civic hacker culture—provide it with enough endurance to sustain its early success and with the institutional capacity to harness the potential of Estonian digital infrastructure for more inclusive public services and society.

Additional version of this case

The case study outlined in this chapter is accompanied by a corresponding case study from the Centre for Public Impact's (CPI) Public Impact Observatory—an international repository of public policies assessed for their impact using CPI's Public Impact Fundamentals framework. CPI's framework provides a way for those who work in or with government to assess public policies, to understand why they were successful, so key lessons can be drawn out for future policy work. The case can be easily located in the CPI repository at www.centreforpublicimpact.org/observatory.

Notes

1. E-Estonia facts, https://e-estonia.com/wp-content/uploads/updated-facts-estonia.pdf.
2. For details, see https://ec.europa.eu/digital-single-market/en/desi and https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2018 respectively.
3. Drechsler (2018) offers an excellent discussion on the hype around Estonia's digital success.
4. E-residency programme homepage and live dashboard can be found here: https://e-resident.gov.ee. As of August 2018, there are more than 40,000 e-residents. As the main service e-residents can currently use is setting up a company, this has had unintended consequences as it has drawn the attention of money laundering regulators in some countries.
5. Thus, for instance, the data exchange layer called 'X-Road'—introduced in 2001 and fundamental to Estonian e-government—is not mentioned in the 1998 strategy document at all, either by name or principle. A subsequent 2004 strategy document, 'Basics of Information Policy' mentions it once; a follow-up strategy in 2006 (*Development Plan for Information Society* 2013) discusses X-Road twice; and the current strategy (*Development Plan for Information Society* 2020, adopted in 2013) mentions it eight times—even though the X-Road has not changed significantly since 2001.
6. The position is formally called Deputy Secretary-General for Communications and State Information Systems, and it is part of the typical management level in Estonian ministries and not a stand-alone office; see https://www.mkm.ee/en/ministry-contact/management.
7. Starting with the 2004 strategy, the timings of adoptions of the strategies reflect EU structural funding periods (2004–6; 2006–13; 2014–20).
8. For a detailed discussion of the vital importance of Institute of Cybernetics, established in 1960, and its R&D capabilities in the evolution of Estonian ICT sector, including involvement in 'Soviet Arpanet', see Högselius (2005).
9. See http://www.kaitseliit.ee/en/cyber-unit.

References

Basics of Information Policy. 2004. https://www.mkm.ee/sites/default/files/infopoliitika_pohialused_2004-2006.pdf [in Estonian].

Burlamaqui, L. and R. Kattel. 2016. 'Development as Leapfrogging, Not Convergence, Not Catch-up: Towards Schumpeterian Theories of Finance and Development'. *Review of Political Economy* 28(2), 270–88.

Crouch, D. 2015. 'How Estonia set the Pace on the Way to Digital Government'. *Financial Times*, 5 June. https://accounts.ft.com/login?location=https%3A%2F%2Fwww.ft.com%2Fcontent%2F7459bdd4-fd66-11e4-9e96-00144feabdc0 [gated].

Development Plan for Information Society 2013. 2006. https://www.mkm.ee/sites/default/files/eesti_infouhiskonna_arengukava_2006.pdf [in Estonian].

Development Plan for Information Society 2020. 2013. https://www.mkm.ee/sites/default/files/elfinder/article_files/eesti_infouhiskonna_arengukava.pdf [in Estonian].

Drechsler, W. 1995. 'Estonia in Transition'. *World Affairs* 157(3), 111–17.

Drechsler, W. 2018. 'Pathfinder: e-Estonia as the β-version'. *Journal of e-Democracy and Open Government (JeDEM)* 10(2), forthcoming.

Estonia's Roadmap to Information Society. 1994. Estonia's Informatics Council [in Estonian].

Estonian Statistics (n.d.). *Rahvaarv 1881–2000* [in Estonian].

Gaskell, A. 2017. 'How Estonia Became the Digital Leader of Europe'. *Forbes*, 23 June.

Goodsell, C. T. 2011. 'Mission Mystique: Strength at the Institutional Center'. *American Review of Public Administration* 41(5), 475–94.

Heller, N. 2017. 'Estonia, the Digital Republic: Its Government is Virtual, Borderless, Blockchained, and Secure. Has this Tiny Post-Soviet Nation Found the Way of the Future?' *The New Yorker*, 18 and 25 December.

Hirschman, A. O. 1967. 'The Principle of the Hiding Hand'. *National Affairs* 6 (Winter), 10–23.

Högselius, P. 2005. *The Dynamics of Innovation in Eastern Europe: Lessons from Estonia* (Cheltenham: Edward Elgar Publishing).

Jonsson, M. E. 2015. 'Democratic Innovations in Deliberative Systems: The Case of the Estonian Citizens' Assembly Process'. *Journal of Public Deliberation* 11(1). http://www.publicdeliberation.net/jpd/vol11/iss1/art7.

Kallas, K. 2018. 'Eesti Digiriigi Allakäik'. https://kajakallas.ee/postitus/eesti-digiriigi-allakaik/.

Kalvet, T. 2007. 'The Estonian Information Society Developments since the 1990s'. PRAXIS Working Paper 29. http://www.praxis.ee/fileadmin/tarmo/Toimetised/toimetised_29_2007.pdf.

Kalvet, T. 2012. 'Innovation: A Factor Explaining e-Government Success in Estonia'. *Electronic Government: An International Journal* 9(2), 142–57.

Kalvet, T. and A. Aaviksoo. 2008. 'The Development of e-Services in an Enlarged EU: e-Government and e-Health in Estonia'. *JRC Scientific and Technical Reports.* http://publications.jrc.ec.europa.eu/repository/bitstream/JRC40679/jrc40679.pdf.

Kattel, R. 2012. 'Eesti Taasiseseisvumisjärgne Majanduspoliitika'. In R. Vetik (ed.), *Eesti Poliitika ja Valitsemine 1991–2011* (Tallinn: Tallinna Ülikooli Kirjastus), pp. 38–56.

Kerem, K. 2003. *Internet Banking in Estonia.* Praxis Centre for Policy Studies. http://unpan1.un.org/intradoc/groups/public/documents/UNTC/UNPAN018529.pdf.

Laar, M. 2010. Interview with Stephen J. Dubner, for 'Freakonomics Radio' podcast, 24 March.

Lesk, M. 2007. 'The New Front Line: Estonia under Cyberassault'. *IEEE Security & Privacy* 5(4), 76–9.

Manning, N. 2007. 'Patterns of Environmental Movements in Eastern Europe'. *Environmental Politics* 7(2), 100–33.

Margetts, H. and A. Naumann. 2016. *Government as a Platform: What Can Estonia Show the World?* (Oxford: Oxford Internet Institute).

Principles of Estonian Information Policy. 1998. https://www.riigiteataja.ee/akt/75308 [in Estonian].

Rajasalu, T. 2002. 'Eesti Majandus 1940–90'. http://entsyklopeedia.ee/artikkel/eesti_majandus_1940–901 [in Estonian].

Randma-Liiv, T. and R. Savi. 2016. 'Managing the Public Sector under Fiscal Stress'. In G. Hammerschmid, S. Van de Walle, R. Andrews and ,P. Bezes (eds), *Public Administration Reforms in Europe: The View from the Top* (Cheltenham: Edward Elgar Publishing), pp. 231–43.

Reinert, E. S. and R. Kattel. 2004. 'The Qualitative Shift in European Integration: Towards Permanent Wage Pressures and a "Latin-Americanization" of Europe?' *PRAXIS Working Paper*, no. 17.

Scott, M. 2014. 'Estonians Embrace Life in a Digital World'. *The New York Times*, 4 October.

Tamkivi, S. 2017. 'Speech to the Parliament of Estonia'. *Parliament of Estonia*. http://stenogrammid.riigikogu.ee/et/201705091000—PKP-20849. Accessed 9 May 2017.

Tammpuu, P. and A. Masso. 2018. 'Welcome to the Virtual State: Estonian e-Residency and the Digitalised State as a Commodity'. *European Journal of Cultural Studies* 21(5), 543–60.

Ubar, R. 1993. 'Elektroonika ja Arvutustehnika Vabariiklik Sihtprogramme'.

Wimmer, M. A., E. Tambouris, R. Krimmer, J. R. Gil-Garcia, and A. T. Chatfield. 2017. 'Once Only Principle: Benefits, Barriers and Next Steps'. 18th Annual International Conference on Digital Government Research, Staten Island, NY, USA, 7–9 June.