Network Security Article
Title: Distributed Denial-of-Government: The Estonian Data Embassy Initiative
Authors: Nick Robinson, Prof. Keith Martin

Current word count: 2541

In an age of increasing and evolving cyberattacks and disruption, recent events have shown us that threats to critical national infrastructure and vital government services are both genuine and effective. In light of this, what measures might a government be willing to take in order to safeguard its critical infrastructure and ever-expanding 'digital ecosystem'? One small country in the Baltics, with a recent history of dealing with such threats, may just have the answer: to 'backup' the nation-state. To protect itself from cyberattacks (but also legitimate concerns of military occupation), the Estonian government is planning to open 'data embassies' around the world, ensuring the state can endure and continue to function, even outside its own borders.

The dramatic rise in cyberattacks, particularly those emanating from states (or state-sponsored groups), is of great concern and anxiety for many governments around the world. The recent UK National Cyber Security Strategy (2016-2021) underlined the "political, diplomatic, technological, commercial and strategic advantage" for state and non-state actors to utilise such tactics, with "government, defence, finance and telecommunications sectors" becoming primary targets for those seeking to disrupt, destabilise or exploit a potential adversary[1]. Within an ever-changing threat landscape, and against an increasingly complex and volatile geopolitical backdrop, states are having to think of new and creative ways to mitigate against emerging cyber threats: from coordinated DDoS attacks against vital organs of the state, to new forms espionage and the onset of 'information warfare' and 'fake news'.

What happens, for example, when a targeted DDoS attack brings a state's financial sector to its knees? Or if vast troves of citizens' healthcare records are effectively wiped from existence or encrypted in a ransomware attack? The recent WannaCry ransomware virus, which crippled the UK's National Health Service, has shown that state institutions and their vital services are still vulnerable and extremely susceptible to ever-growing cyber threats. Doomsday scenarios are often envisaged by those in the media or information security circles, but can every government be certain that its defence and mitigation strategy is up to the job?

Governments around the world have increasingly utilised cloud-based services in order to improve accessibility and reduce costs of some functions of the state. However, by virtue of redundancy and geographical distribution, cloud-based services can also be used to improve the availability and overall security of government data. Taken to extreme, just as individuals increasingly secure their personal lives (photos, documents, etc.) in the cloud, a nation-state could choose to outsource to the cloud its entire digital function (land and business registries, tax and healthcare records, etc.). In this way a government, even if forced into disarray or exile,

[1] **HM UK Government.** 2016. *National Cyber Security Strategy 2016 to 2021*, Cabinet Office, London.

could potentially continue to function from beyond its own borders. This might seem a fantastical idea, but it could soon become a reality.

e-Estonia: All Roads Lead to the X-Road

Estonia is a country that is continually trying to reimagine itself *virtually*, above and beyond its own physical limitations. Whether this is through the recent decision to store every citizens' healthcare records on an immutable, verifiable blockchain; or the rather bold attempt of amassing 10 million *e-Residents* by 2025, Estonia's status as a *digital vanguard* is rarely disputed. The journey Estonia has taken since regaining independence from a collapsing Soviet Union in 1991 has been nothing short of remarkable – and in many ways, it was this collapse, and the opportunity to 'start again' with no political legacy, that was ardently seized by a youthful, forward-thinking government. The introduction of project Tiigrhüpe (Tiger Leap) in 1996 is often seen as a catalyst in this regard, as large-scale improvements in both infrastructure and education oversaw a period of enormous social, economic and political change. A powerful post-Soviet vision emerged that recognised technology as *the* facilitator for streamlining cumbersome, bureaucratic government institutions and nurturing innovation, in a tiny nation otherwise bereft of any infrastructure or resources. A 'conveyor-belt' like period of innovation soon followed with the introduction of an eID system (2002), i-voting (2005), and e-Health (2008), offering huge benefits for the everyday Estonian with efficient, secure e-services. They soon adopted the now renowned prefix 'e-Estonia' – a visible brand and message the Estonian government are keen to present to the rest of the world.

In Estonia today, you can vote online, tax returns are completed digitally within minutes, and almost all health prescriptions are issued electronically reducing administrative burdens on its health service[2]. Citizens elsewhere rarely have a one-stop shop for all of their government services: Estonia is certainly an exception to this rule. Estonians often joke that the only thing you *can't* do online today is get married or divorced. All of this is kept fully functioning by, unsurprisingly, yet another Estonian creation: X-Road. Understood to be the backbone of today's e-Estonia, X-Road provides vital cryptographic services and infrastructure, enabling data to be securely exchanged between different information systems, registries and databases; but also allowing *all* of Estonia's e-services to link up and operate in harmony across a seamless, decentralised network. Services are efficient, interoperable, and most importantly, secure.

But the Estonian government also recognises that many of its databases, registries and services (e.g. Land or Population Register) only exist in digital form. It is this lack of a paper trail - considering the evidential value each register or database holds - that is the cause of great anxiety for the Estonian government. Could its government continue to effectively function in the event of a large-scale cyberattack? What if Estonia's territorial integrity and independence was suddenly under threat? History has taught Estonians that such eventualities are legitimate and valid.

[2] **e-Estonia.** 2015. *e-Estonia: The Future Is Now*, Enterprise Estonia, Tallinn.

Backing up the nation-state

In 2013, the Estonian government began pursuing the *Data Embassy Initiative* (DEI): an ambitious (but also timely) solution to the plausible scenario that its government would be required to sustain its numerous digital services and functions of the state outside its own borders. Its desideratum, as outlined by the Estonian government, is to ensure *digital continuity*: "the capacity of a state to maintain its services and digital data relevant for the functioning of the state, regardless of any adverse changes or interruptions"[3]. This, in the case of Estonia, would ensure the state – its numerous databases, registries and digital services – would continue to function, "even in the direst of scenarios"[4], which, they say, includes the loss of territory.

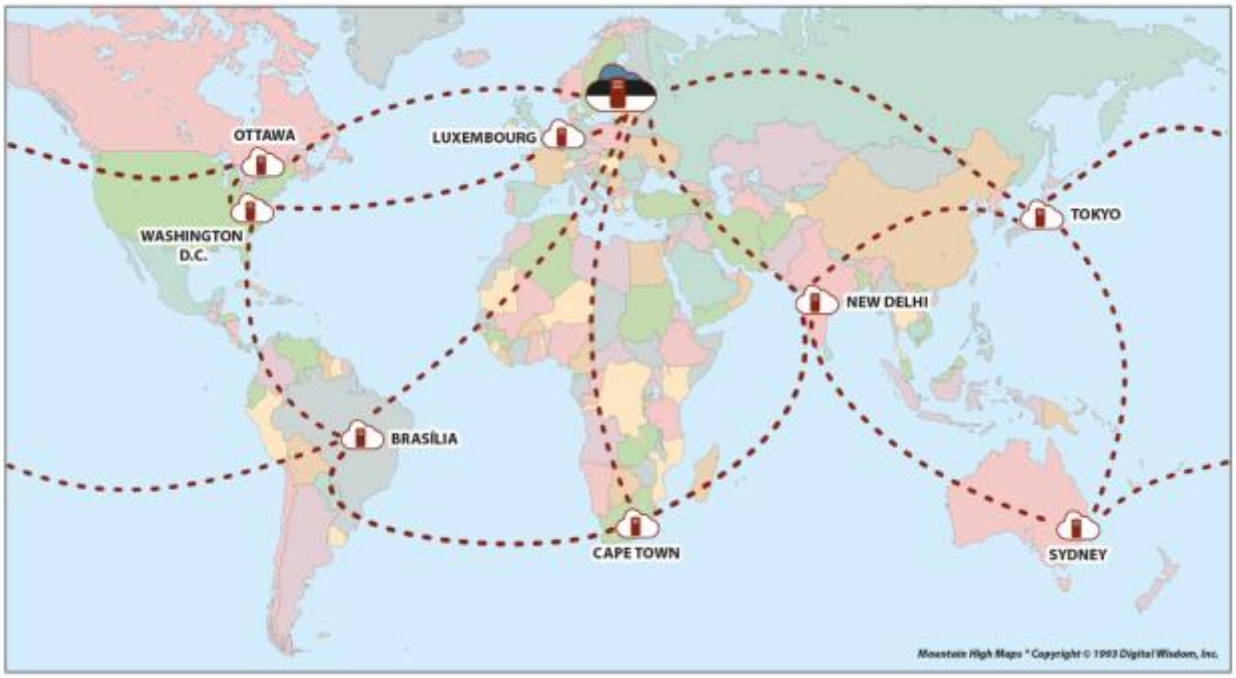
To ensure *digital continuity*, the DEI consists of three fundamental approaches. First, and not too dissimilar to other governments' cloud strategies, purpose-built data centres located within Estonia's own borders will allow for improved maintenance of regular data backups and live services. Next, the Estonian government will look to migrate its so-called "digital monuments" – websites and other non-sensitive resources that hold national symbolic significance – to an international public cloud service (such as Amazon's AWS or Microsoft Azure). Resources such as the State Gazette - the online depository for all Estonian legislation since 2010 - do not hold sensitive information, but are part of the state's critical national infrastructure and could be significant targets for disruptive attackers and require full availability at all times for Estonian citizens.

The final (and perhaps most novel) step the Estonian government is now proposing, will see the creation of a network of 'data embassies' around the world in an effort to backup its more critical and sensitive data. Located outside of Estonia's own borders, it offers an effective solution for housing backups of Estonian registers and databases, whilst still being under full control of the Estonian government. In the first instance, this will involve the continued utilisation of Estonian embassy buildings in different cities around the world. Many Estonian embassies have been used this way for the last decade or so, but will now see more systematic backups as previous quarterly/twice-annual backups were not sufficient enough in ensuring 'digital continuity'.

There are, however, obvious drawbacks to this proposal - namely the lack of technical competence within each embassy to offer support during times of emergency; but also, that it is patently clear that embassies are not constructed to the correct standards and data security requirements expected within a (regular) data centre. Because of this, the Estonian government have proposed a supplementary solution: to procure additional data centre resources through bilateral agreements with so-called 'friendly' governments across the globe. The Estonian government would, in effect, 'rent' server space within existing data centres, with Estonian jurisdiction being deemed applicable within these agreed spaces. Under such an agreement,

[3] **MEAC.** 2016. *Transforming digital continuity: Enhancing IT resilience through cloud computing*, Ministry of Economic Affairs & Communications and Microsoft, Tallinn.
[4] **MEAC.** 2015. *Implementation of the Virtual Data Embassy Solution*, Ministry of Economic Affairs & Communications and Microsoft, Tallinn.

the data centre will operate in a similar capacity to a physical embassy, where diplomatic immunities will be applicable under the Vienna Convention on Consular Relations (1963). Together, these two solutions will present a robust, distributed network of data embassies (see, Fig. ?) that the Estonian government believe will not only be costly and exhaustive to attack, but also improve data security, integrity and availability of services in the event of a crisis.



(Fig. ? - How a network of 'data embassies' might look when in full operation - author's own image)

On June 20th 2017, it was announced that the first data embassy would be located in Luxembourg after a bilateral agreement (the first of its kind) was signed by both heads of state. Whilst the data embassy is not expected to be fully operational until 2018, the historic agreement lays out each country's necessary rights and obligations, along with ten priority databases being chosen to be backed up in the data embassy's secret location. It may be a little while longer, however, until we see a fully operational data embassy network. Future locations remain undisclosed, whilst the uncertainty surrounding Brexit negotiations appear to have stalled any plans for a data embassy in London.

The team tasked with implementing this ambitious project have also admitted that certain technological and legal hurdles still need to be overcome. Decisions are yet to be made over what kind of scheme will be used for distributing the data across multiple embassies - but, like many Estonian innovations, the government will look towards the private sector for answers as companies such as Cybernetica and Guardtime play critical roles in the design, development and upkeep of Estonia's flourishing ecosystem.

From a legal perspective, questions remain over how governments should respect the integrity and sovereignty of other government's data when stored in the cloud? Or, how to legally ensure that government data held in the cloud has immunity from being tampered with or copied? In a recent joint research report with Microsoft[5], it was acknowledged that minor revisions to domestic Estonian law may be required; but with no form of legal precedent to guide us, and no data embassies tested under international law, further investigation as to how diplomatic and international protections can be applied is essential.

Distributed Denial-of-Government?

The *Data Embassy Initiative* may raise plenty of questions within the information security community, namely: why is any of this even necessary? Such an initiative will ultimately carry a hefty financial burden upon the state, with some governments maybe questioning whether the potential risks even outweigh the benefits. So, under what circumstances (or indeed pressures) does a government like Estonia's feel that it is imperative to utilise such a bold strategy as 'backing up' the nation-state?

Mentioned already, Estonia's reliance upon its digital ecosystem could ultimately become its own downfall. Despite its many benefits, the aforementioned 'paperless' vision of a digital society can lead to obvious vulnerabilities and weaknesses[6]. As the government outlines, scenarios whereby "digital signatures do not work for days at a time, or the data in the Land Register is corrupted"[7] are not acceptable in today's Estonia. With the recent introduction of e-Residents into the equation, the onus is even higher on the Estonian government to ensure that all databases, registries and services are secure and available 24/7.

The Estonian government has also learnt lessons from its own recent history. In 2007 Estonia was victim to what is widely considered to be the first instance of a state-sponsored cyberattack (allegedly Russian-orchestrated), as its government institutions, media and news portals, banks and telecommunications infrastructure were subject to a significant DDoS attack. Although damage was minimal, and 'normal service' was resumed in a matter of days, it was deemed a wakeup-call not only in terms of attitudes towards cyber security, but in asking vital questions of *how* (and *where*) should its databases, registries and services be held and secured. Around this period a comprehensive cyber security strategy (2008-2013) was published[8], whilst NATO strategically placed its Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn.

---

[5] **MEAC.** 2015. *Implementation of the Virtual Data Embassy Solution*, Ministry of Economic Affairs & Communications and Microsoft, Tallinn.

[6] **Pernik, P**. 2016. *e-Residency and Data Embassies: A Country Without Borders*, European Cybersecurity Journal, 2(1), 54-61.

[7] **Kotka, T. and Liiv, I.** 2015. *Concept of Estonian Government Cloud and Data Embassies*, in; Kő A., Francesconi E. (eds) Electronic Government and the Information Systems Perspective. EGOVIS 2015. Lecture Notes in Computer Science, vol 9265. Springer, Cham.

[8] **MEAC**. 2008. *Cyber Security Strategy 2009-2013*, Ministry of Economic Affairs & Communications, Tallinn.

But these worries and concerns are not solely confined to the 'digital'. Another reason for building data embassies, it might be suggested, is down to a prevalent and ongoing geopolitical anxiety over the potential occupation of Estonian territory. Such concerns are not quixotic either. Estonia spent a large percentage of the 20th Century under repeated occupations from the Soviet Union (1940-1941 and 1944-1991) and Nazi Germany (1941-1944), so understandably the threat of future occupation now finds itself deeply ingrained within the Estonian psyche. The geographical proximity to the recent annexation of Crimea in 2014, or further conflicts in Ukraine and Georgia, have arguably exacerbated such fears, whilst some commentators have speculated on whether Estonia (or others in the Baltics) 'might be next'[9]. With the question of *digital continuity* now firmly at the forefront of the national conversation in Estonia, the DEI might not only be seen as a necessity in a digital age, but as a stringent additional defence mechanism against an intimidating and potentially aggressive neighbour.

Trend setters?

Will the concept of data embassies ever catch on? When speaking to one official within the Estonian government, it was made clear that Estonia should by no means be an exceptional case. Data embassies, they said, should become an "integral part of any government's cyber security strategy in the future". 2017 has so far shown us that governments are now facing a multitude of threats to both critical infrastructure and vital services, whilst concerns over the way in which data is collected, stored and used continue to grow. It seems unlikely that the Data Embassy Initiative will become the panacea governments are looking for overnight. In a best-case scenario, data embassies could be extremely beneficial in providing greater reassurances over the integrity and reliability of data and government services; but in a worst-case scenario, a network of data embassies could ensure a government could continue to function, even if forced into exile. Whilst governments have operated from in-exile before now (Poland and Norway did so from London in World War II), none have benefitted from the use of the cloud. Many states - especially those without universal recognition or status - could be drawn to the notion of an extraterritorial state and infrastructure.

Granted, Estonia's circumstances are somewhat unique, but they offer us a fascinating example of a government looking to push the boundaries in terms of data and national security in the 21st Century. Estonia's lack of political legacy and 'start-up' mentality mean that they are often open to such radical initiatives, comparative to the UK or other western governments for example. Many governments have taken to experimenting with cloud computing in recent years, with the benefits of reduced costs, increased efficiency and increased scalability of digital services an obvious advantage to any state's future digital strategy. We are yet to see a government attempt such a bold strategy as 'backing up' the nation-state, but will it be long before we see a complex international network of data embassies forming around the world?

---

[9] **Stuttaford, A.** 2015. *After Ukraine, are the Baltics in Putin's sights?*, Prospect Magazine, Issue 233; and, **Trimbach, D. and O'Lear, S.** 2015. *Russians in Estonia: Is Narva the next Crimea?*, Eurasian Geography and Economics, 56(5), 493-504.