OXFORD INTERNET INSTITUTE
UNIVERSITY OF OXFORD
REPUBLIC OF ESTONIA
MINISTRY OF ECONOMIC AFFAIRS AND COMMUNICATIONS
rit Estonian IT Centre
Nortal

GOVERNMENT RESILIENCE IN THE DIGITAL AGE

Tallinn 2024

AUTHORS

Andres Raieste

Senior Vice President, Public Sector (Global), Nortal

Andri Rebane

Director of Information Security Department, Estonian IT Centre

Madis Tapupere

Chief Technology Officer, Ministry of Economic Affairs and Communications

Dr. Keegan McBride

Lecturer in AI, Government, and Policy, Oxford Internet Institute

Adjunct Senior Fellow in National Security and Technology, Center for a New American Security

This report may be cited as Raieste, A., Rebane, A., Tapupere, M., McBride, K. (2024) Government Resilience in the Digital Age

Reviews and contributions:
Martin Sepp, Ergo Tars, Toomas Vaks

This collaborative report is an outcome of a workgroup composed of experts from the public sector, private sector, and academia.

The Oxford Internet Institute is a multidisciplinary research and teaching department of the University of Oxford, dedicated to the social science of the internet.

The Estonian IT Centre (RIT) provides the Republic of Estonia’s public sector with secure IT infrastructure and central services.

Nortal is a global strategic innovation and technology company and a valued partner for governments, healthcare institutions, leading businesses, and Fortune 500 companies.

TABLE OF CONTENTS

EXECUTIVE SUMMARY 4

INTRODUCTION 7

CHALLENGES TO THE CONTINUITY OF THE STATE 11

POLICIES FOR BUILDING RESILIENT DIGITAL STATES 14

Adopt a digital-first approach to critical public services and registries 17

Transition to remote-first and remote-enabled public sector jobs 20

Secure digital public infrastructure and services 22

Ensure widespread affordable access and redundancy to connectivity 24

Build redundancy to digital public infrastructure 26

Manage the third-party risk while preserving technological innovation 29

Create institutional capacity for developing government resilience 32

THE FUTURE OF RESILIENT DIGITAL STATES 34

BIBLIOGRAPHY 36

EXECUTIVE SUMMARY

Today's world is a digital one. States that want to remain relevant must digitalize, or they will be left behind. This is not a new phenomenon but has been unfolding for more than three decades. Following the global proliferation of the internet in the 1990s, there has been international interest in harnessing the power of technology to transform the way states operate. In the years to come, many states worldwide invested heavily in new initiatives focused on digitalizing their critical data assets or bringing traditionally paper-based services into new digital formats. States that made a more substantial commitment to digitalization are benefitting from it today, often seeing an increase in the overall effectiveness of their public sector. These states will have an advantage over their geopolitical rivals in the emerging digital world order. For states that did not digitalize or view it as a priority early on, recent crises have forced policymakers to realize the necessity of digital technologies for running a state in the 21st century.

States are currently navigating a time defined by multiple crises, a polycrisis. COVID-19 brought the physical world to a standstill for much of 2020. As a result, many governments could not operate or deliver many of their services. Climate change is also becoming increasingly disruptive for governments as natural disasters grow in number and severity. Some states may experience worsening wildfires; others may see an increase in the scale of flooding; some countries like Tuvalu may even face the loss of their physical territory. Conflict is on the rise, as demonstrated by the ongoing war in Ukraine and a growth in tension between the U.S. and China over Taiwan. Democratic states are also facing an increase in internal crises; for example, new challenges are emerging due to democratic backsliding, declining voter turnout, and dissatisfaction with democracy more broadly.

States are being forced to manage numerous ongoing crises at any given time, both domestically and internationally, in addition to their other critical responsibilities. Usually, states must do this with a public sector facing a shrinking budget, workforce, and ever-growing demands for efficiency and effectiveness. The only way to navigate these challenges successfully is by embracing the potential of digital technologies. This is what the world has seen. Digital states were better able to manage the COVID-19 pandemic than those that were not. Digital technologies also play a key role in monitoring, managing, or curtailing the impact of natural disasters. In conflict, states that can better leverage digital technologies, especially those that enable connectivity and data-driven decision-making, will have the advantage.

Thus, the world is witnessing the rise of new digital states where digital technologies and data are core to the functioning of the state itself. However, as a result, these states introduce new dependences on technology.

This is not something that should be feared, but it is something that should be respected. It is of the utmost importance that when states embark on their path toward digitalization, they prioritize the long-term resilience of the digital infrastructure that they are building.

This report was written to help guide policymakers interested in building and developing better, stronger, and more robust digital states. To do this, the report provides an overview of key progress made in creating government resilience in the digital age, and through this also the history of the current digital world order. Following this, the report adopts a scenario-based approach to illustrate the sorts of crises that states must prepare their digital infrastructure for. Drawing on the insights of this scenario, the report introduces seven key policy recommendations intended to help build and strengthen the resilience of a state's digital infrastructure.

> → **First, states must adopt a digital-first approach to public services and registries related to the continuity of the state.**
>
> → **Second, states must start enabling the transition to public sector jobs that can operate in a remote-first or remote-enabled manner.**
>
> → **Third, states must prioritize the security of their digital infrastructure and services.**
>
> → **Fourth, states must ensure resilience in connectivity by viewing internet access as critical infrastructure.**
>
> → **Fifth, states must improve their resilience by reducing opportunities for physical damage to disrupt their digital operations.**
>
> → **Sixth, states must invest in the ability to manage third-party risk without limiting opportunities for technological innovation.**
>
> → **Seventh, governments must adopt a whole-of-government approach to developing digital resilience.**

States that adopt the above recommendations when building their digital infrastructure, accompanied by the necessary organizational and policy changes, will be rewarded with a resilient digital state. If built properly, a sufficiently resilient digital state could run its core and critical digital services even if there was a temporary or more long-term loss of its physical territory due to a crisis. This is something that is now only possible due to technology. It also represents the need to shift how we think about states in this new digital world where digital is no longer tied to the physical boundaries of a nation.

The future of democracy is digital. During the pandemic nearly 30% of governments in Europe postponed elections between 2020–2022 [10], which arguably damaged their democratic process. Digital state processes have become a necessity to better protect our states during crises.

INTRODUCTION

In the aftermath of the Second World War, the global community developed the foundations for a new geopolitical order aligned with liberal values. The number of democratically aligned states began to grow during the same period; democracy represented hope and a vision of a better future. Following the defeat and dissolution of the Soviet Union in the 1990s, optimism continued to grow. For the first time in history, most of the world's population lived in states defined by liberal and democratic values [1].

During this period of democratization, another foundation of today's world came to the forefront – the internet. The internet and its global spread transformed the way the world communicated and bolstered support for the values of liberty, democracy, and freedom. In a 1994 speech, Vice President Al Gore hoped that "Central and Eastern Europe can use technology and the free market to build democracy – not thwart it. [2]" Several months later, he echoed these sentiments and his belief in the positive potential of the internet to "derive robust and sustainable economic progress, strong democracies, [and] better solutions to global and local environmental challenges. [3]" It was clear that technology, especially the internet, could transform the world's thoughts about states and governments.

Though many states started experimenting with technology to reimagine their governments, not all were fully committed or successful. Some states also saw technology as posing a potential threat to the state. It was argued that if the computerization of society could "alter the entire nervous system of social organization," then these developments would "change the stakes of sovereignty" [4] as private sector companies came to challenge the state's control over communications. In contrast, Estonia, which restored its independence in 1991, stands out as one of the few countries that fully embraced technology early on. Estonia's first information development plan, "The Estonian Road to an Information Society", was released in 1994 and argued that technology would play a vital role in the future of states, improving their efficiency and helping to strengthen and secure their culture, sovereignty, and security. Importantly, this strategy also saw the private sector not as a barrier or a challenge to the state but a key component in helping the government achieve its digitalization goal.

Now, more than three decades later, it is possible to look back and reflect on these early beliefs about the liberal geopolitical order, democracy, states, governments, technology, and the relationship between them. What emerges is an image of a new digital world. In this new world, however, democratic states are being challenged by democratic backsliding [5], declining voter turnout [6], and increasing dissatisfaction amongst voters [7] are beginning to weaken. While fighting to maintain their democratic systems of government and pushing back the growing global influence of authoritarianism [8], democratic states also face unprecedented external challenges to their stability and safety. In 2020, the COVID-19 pandemic caught many off guard and exposed numerous weaknesses in government operations. However, the pandemic also showed that states that could leverage data and technology more effectively performed better [9]. During the pandemic nearly 30% of governments in Europe postponed elections between 2020–2022 [10], which arguably damaged their democratic process. Even fewer states were able to seamlessly transition to remote schooling, damaging the education and learning of children. Climate change, too, is making itself increasingly known, with natural disasters becoming increasingly common and growing in severity and intensity. For some states, this means bearing the brunt of powerful floods, hurricanes, or fires for others, they are facing a future where their entire physical territory will disappear within their lifetime [11].

If before it was possible to ignore the benefits and positive potential of digitalization for states, today, this is no longer the case. States that do not digitalize will be left behind, increasingly vulnerable in a world defined by technology. Technology must be viewed as an essential and integral component of the state to overcome and address the world's growing complexity today. Many states now realise this and are investing large amounts of resources into digitalization. The European Union alone has budgeted more than €100 billion to help support the development of a digital and resilient Europe [12]. Digitalization will improve how effective and efficient states run, but it also brings new challenges and threats.

Many states cannot independently develop, build, or sustain the digital infrastructure and technologies they require and have engaged heavily with private sector technology companies [13]. This growing reliance on the private sector has led policymakers and academics to argue that there is an ongoing "coup," [14] where technology companies have begun to overtake and consume the state. These fears are even stronger when the companies relied upon are based within foreign states. There has been growing interest in policies supporting "digital sovereignty" and "data sovereignty" [15] to counteract these fears. Though such concerns are understandable, by tying digital infrastructure to the physical territory of a specific country new vulnerabilities are created. Similarly, by trying to reduce the power or strength of the largest technology industry the ability of the state to defend itself in the cyber domain is also weakened.

Yet, peace no longer exists in the digital world, and digital infrastructure is a clear target. The private sector plays a critical role in helping to defend states against robust, consistent, and comprehensive cyber threats from hostile nations daily [16]. These threats are real. In 2007, Estonia was targeted by a large cyber-attack significantly disrupted the country's normal operations. In the current war in Ukraine, Russia utilised both digital and physical means to disrupt Ukraine's ability to operate digitally targeting

key data centres with both malware and cruise missiles [17]. With military tensions continuing to rise between Taiwan and China, many have argued that China's first steps are likely to target Taiwan's critical digital infrastructure [18].

> **As threats to the physical territory of liberal and democratically aligned states continue to grow from conflict and other factors, it is important to think through how to build more robust and resilient digital states.**

Building and investing in a better, stronger, and more resilient digital future will not only help ensure the longevity of democratic states themselves, but also provide them with new opportunities to sell their vision of a new digital geopolitical order.

This report represents a first step in this process, challenging the existing conceptualisation of what it means to be a state in today's digital age. To aid this conceptual exercise, the report identifies several scenarios states may encounter in the decades ahead and explores how digital technologies could be used to overcome them. Following this exploration, the report identifies and offers several key policies and building blocks for constructing more robust and resilient digital states.

CHALLENGES TO THE CONTINUITY OF THE STATE

Crises and natural disasters have always been a part of our world. Whether they are the result of political, economic, social, or environmental factors, crises often share common characteristics that result in widespread disruption to societies and individuals. Historically, crises have often played a pivotal role in influencing the fate of a state. History is full of examples that demonstrate how states, when unable to overcome the challenges posed by a crisis, decline in power and influence or in some cases even cease to exist [19].

While the root causes of many crises remain similar today as they were centuries ago, for example when confronting a large natural disaster, war, or a pandemic, the world of today is more interconnected than ever before. As a result, the difficulty of addressing a crisis has rapidly increased in complexity and its potential impact is larger in scale. Due to the digital and integrated nature of the world, states are dependent on global supply chains, resources, and technology [20]. Recent examples of this include the COVID-19 pandemic which caused global supply chain disruption that continues to this day [21], the WannaCry ransomware attack, and the War in Ukraine.

Importantly, as today's world is digital, it is no longer possible to separate the physical and the virtual worlds. In each of the above examples significant impact was felt in both realms at the same time.

> **Today, the destruction of the virtual environment or critical datasets can cause more harm than the destruction of a building or physical infrastructure.**

During times of conflict, which is also becoming increasingly digital, denying your adversary's access to cyberspace and digital services could bring the functioning of the state to a halt.

While increasing levels of digitalization and technological innovation create new vulnerabilities for states, they also provide the means to make societies more resilient than ever before. Through technological development and strategic, comprehensive, digitalization of society it is possible for states to increase their resilience by reducing their dependence on the physical realm.

In the next chapter the report examines in more detail what policies can be implemented to make government more resilient in the digital age.

WHAT IS THE THREAT?
EXAMPLE UNMITIGATED CRISIS SCENARIO

THE START OF THE CRISIS:

Natural disasters, climate change, or military conflicts have resulted in significant disruptions to the standard operations of national services, causing them to be limited or, in certain instances, entirely non-operational.

The immediate aftermath of these disasters reveals a grim scenario where critical infrastructure has sustained extensive physical degradation. Numerous domestic data centres have been destroyed, leaving a significant portion of the national digital backbone inoperable. The reliability of electricity has become erratic, and the continuity of fuel supply is compromised. Furthermore, the local telecommunications infrastructure has been critically damaged, impeding effective communication.

In parallel, cyberattacks or the destruction of digital infrastructure may also occur, rendering some services permanently or temporarily unavailable. The interdependencies between registries and services can lead to cascading effects, causing an increasing number of services across different sectors to become unavailable. In such cases, alternative operating procedures shall be activated.

As a result, the continuous operation of digital services has been severely restricted, making it almost impossible to maintain the modern way of living. The dependencies among registries, various information systems, and underlying national services, such as electronic identification, have become starkly apparent as some systems fail due to the issues.

The nature of the crisis, the extent of the affected physical territory, and the low level of preparedness have collectively contributed to the realization of these risks. In response, some registries (paper or digital) may have been relocated to safer zones, while others remain offline – temporarily or permanently. In the worst case, critical data assets and their backups could be destroyed permanently or irreversibly corrupted, leading to a devastating data loss. The state and the services that rely on these registries are facing significant challenges; a few can function, but others have ceased to operate due to the lack of essential data.

This gradual deterioration of public services is having a broader impact on public sentiment and opinion. Access to information is severely constrained, leading to widespread fear and uncertainty among the population. The state now faces the daunting task of ensuring the short-term continuance of governance and providing support to displaced individuals who have managed to seek safety elsewhere.

CONTINUATION OF THE CRISIS:

Due to the ongoing crisis, a significant portion of the physical territory of the state has become uninhabitable. The government is grappling with the challenge of survival, while contemplating the possibility of conducting some operations in exile.

In this context, the resilience of the state's democratic institutions amidst climate change or prolonged conflicts, as well as the long-term preservation of the nation and its cultural heritage, has emerged as a strategic objective. Compelled to function with a diminished number of services, it is imperative that the state can continue to update information about citizens, ownership, cultural heritage, etc., to ensure the continuity of nationhood and facilitate the restoration of the nation following the prolonged crisis.

Moreover, citizens still require access to governmental services while in exile. Certain information from national registries will be transferred to foreign registries to facilitate the use of essential services, such as medical and educational data. It is essential that educational resources, such as schoolbooks, and virtual schooling be made available to sustain the language and culture in both the short and long term.

Failure to provide such services would eventually lead citizens to lose their connection to their homeland. This gradual erosion of national identity will cause the nation to lose its political and cultural distinctiveness. Consequently, individuals will no longer feel a sense of belonging, ultimately leading to a point where the state's continuity is compromised and rendered unsustainable under external pressures.

POLICIES FOR BUILDING RESILIENT DIGITAL STATES

In the two previous chapters, the report outlined how digital technologies and a growth in the number and severity of crises increasingly define the world of today. To remain relevant, states must digitalize; this is no longer optional. As the internal functions of the state become increasingly digital, it is essential to ensure their long-term resilience and reliability. This is especially important as states worldwide continue to face multiple, interconnected, and complex crises, from war to pandemics to climate change. Each of these may have a significant impact on the functioning of the state, for example, by disrupting internet connectivity, closing physical offices of public servants, or even causing destruction of data assets critical to the state.

As states undergo the transformation into new digital states, it is of the utmost importance to think strategically about how to build robust and resilient digital infrastructure that, even if unlikely in the short-term, have a high probability of occurring in the long-term. Drawing on the potential challenges and side effects that may follow a crisis, such as the one described above, this section outlines seven recommendations to increase the digital resilience of the state.

> **These recommendations, if adopted, will help to ensure that a digital state can function even when facing the worst of crises.**

In the worst-case scenario, they would help enable a state to run digitally even if it no longer maintained control over its physical territory.

01

ADOPT A DIGITAL-FIRST APPROACH TO CRITICAL PUBLIC SERVICES AND REGISTRIES

Digital rather than paper registries and services are more reliable and efficient, especially in crisis situations. Unfortunately, many governments have not digitalized their critical services related to the continuity of the state and the nation. To increase the state's reliability and resilience the digitalization of such services must be prioritized.

02

TRANSITION TO REMOTE-FIRST AND REMOTE-ENABLED PUBLIC SECTOR JOBS

Civil servants that assure the continuity of digital public infrastructure and services are affected by crises just as much as the rest of the population. Enabling public sector jobs to operate completely remotely is necessary for increasing national resilience.

03

SECURE THE STATE'S DIGITAL INFRASTRUCTURE AND SERVICES

Successfully denying access to, or tampering with, critical digital data, services, and registries is essential to ensuring the legitimacy of a digital state. Establishing mandatory security standards and requirements for public services and infrastructure from both internal and external threats provides the means to increase the long-term cyber resilience of the state.

04

ENSURE WIDESPREAD AFFORDABLE ACCESS AND REDUNDANCY TO CONNECTIVITY

In today's digital age, access to the internet is becoming as crucial as access to other infrastructure and amenities. The state must explore all technology options available for ensuring resilience.

05 BUILD REDUNDANCY- POTENTIALLY BEYOND TERRITORIAL BORDERS- TO DIGITAL PUBLIC INFRASTRUCTURE AND SERVICES

States must guarantee that digital public services and infrastructure are safeguarded against physical destruction resulting from the operation of these digital services within a limited physical space. This may involve positioning at least part of the infrastructure beyond their own territorial borders. In doing so, governments must also resolve issues on mutual trust to be capable of providing a safe harbour for digital governments on foreign territory.

06 MANAGE THIRD-PARTY RISK WHILE PRESERVING TECHNOLOGICAL INNOVATION

Almost all digital public services and infrastructure contain technological “black boxes” not properly auditable, transparent, and may even challenge the digital sovereignty of the state. As the world continues to digitalize this trend will continue. Procedures should be established to mitigate this risk to a reasonable level that does not severely inhibit innovation, avoiding over-regulation.

07 CREATE INSTITUTIONAL CAPACITY FOR DEVELOPING GOVERNMENT RESILIENCE

Government resilience involves decentralized responsibility for each government function, but to avoid cascading failures, a coordinated top-down approach is also needed. The appointment of a centralized body is recommended to oversee and ensure the execution of policies aimed at increasing resilience and continuity across all government levels.

01 ADOPT A DIGITAL-FIRST APPROACH TO CRITICAL PUBLIC SERVICES AND REGISTRIES

A key component for any digital state will be the development and maintenance of digital registries. These registries are responsible for maintaining up-to-date information on all aspects of the state, from registering births to managing real estate ownership. For such a system to work effectively, states rely on the public's trust in government institutions as well as a system of justice that fairly protects a citizen's rights.

In the digital age, ownership is mostly defined by data in digital registries and various systems distributed across public and private sector. The ownership of all significant things – parenthood, property, education, inheritance, even medical history, shares, wealth – is inherently digital. In such a system, digital data and information would take precedent over physical alternatives – this is the most efficient and resilient way to govern today.

Today, most modern governments have some form of digital registries and online services, but the transformation is usually partial at best. For example, some states may allow for people to apply online for a driving license, but they likely must collect the document physically at a government building. This is a problem that can be solved with technology; the limitations to broader digitalization are almost always related directly to legacy procedures, legal frameworks, or a lack of trust.

It is for this reason why digital states must not stop only at investing in technology but must rethink their internal processes and operations by adopting a digital-first approach to the public sector. The digital registries, services, information, and assets critical to the continuity of the state must be made accessible from anywhere (i.e., digital) and provide end-to-end outcomes.

> **Getting this right will require states to understand which registries, services, and assets should be viewed as "critical" for the long-term resilience of the digital state.**

Four especially relevant categories are presented below, which can be further categorized by their relevance to continuity of the state and their relevance to ensuring the flow of critical public services.

1. **State governance.** Services within this category include elections and voting, registry of laws and regulations, state decisions, strategic communications and state announcements. During a long-term crisis, such as a war, are likely to have a significant impact on this category.

2. **Registries of ownership, obligations and justice.** This category includes the most important registries: the population registry, business registry, property registers (cadastre, vehicles etc.), taxes, criminal records and other legal facts.

3. **Citizen services.** This category includes services such as getting new passport and identity documents, obtaining internationally recognized licenses and certificates (e.g. of education), receiving social benefits, and paying taxes. It also includes services related to the preservation of the national identity, such as access to the national archive, public broadcasting archive, national literature, and educational materials and assets to continue schooling.

4. **International integrations with neighbours.** This category is related to services that enable cross-border information exchange. These services are especially useful if a crisis is accompanied by the mass movement of people into new territory, for example by providing them with a form of digital identity that can be easily exported.

For services managed or owned by third parties (e.g., private sector entities), a mechanism could be introduced to incentivize digital development. For instance, when procuring educational books for children, digital versions should also be required. Unlike physical books, which can be damaged or become inaccessible, digital copies can be widely distributed and remain accessible, proving especially valuable in times of crisis.

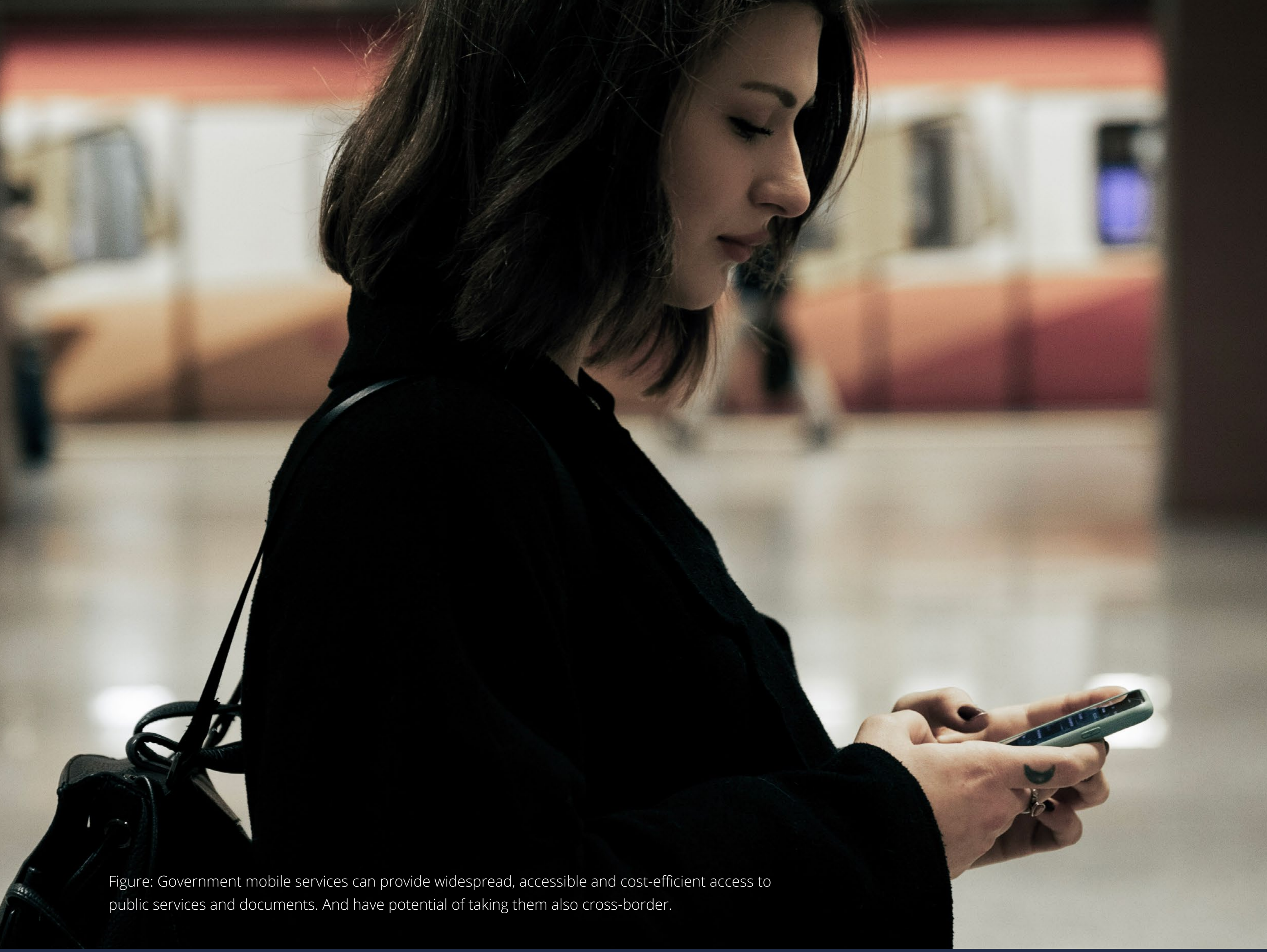

Figure: Government mobile services can provide widespread, accessible and cost-efficient access to public services and documents. And have potential of taking them also cross-border.

KEY RECOMMENDATIONS:

→ Identify which services and registries are critical for the long-term continuity of both the state and the nation in various state of emergency scenarios.

→ Implement a policy that requires the digital transformation of public services deemed vital for the state’s long-term continuity.

→ Adopt a policy that prioritizes the development of digital-first services and assets, ensuring compliance with established security standards and requirements.

02 TRANSITION TO REMOTE-FIRST AND REMOTE-ENABLED PUBLIC SECTOR JOBS

Adopting a digital-first approach to public service delivery will help to free up human resources as services become more efficient, automatic, or proactive but there will still be a need for public servants to ensure that systems remain operational and secure. For public servants working with critical services, during a time of crisis it is even more important that they can do their job. However, it is also likely that they too will be impacted during a crisis or state of emergency and their ability to operate from a physical office may not be possible.

The solution is to enable public sector workers connected to the operation of critical services the ability to work fully remotely. There are three primary considerations to consider when adopting a remote-first approach to the public sector workforce:

1. The transition of work to secure digital channels.
2. Ensure the internal systems, software and infrastructure are universally available and accessible remotely.
3. The establishment of new, remote-friendly digital internal decision-making, leadership, processes, and audit trails.

These changes are hard to do but are also a key component of ensuring the long-term resilience of the digital state.

Usually, digitalizing a service or its infrastructure is the easiest part of the solution. Instead,

> **the hardest aspect is transforming the organization itself, its decision-making processes, and its culture.**

Often organizations rely on paper or some key assets that can only be accessed locally, limiting opportunities for change and remote operations.

To overcome this challenge, it is possible to develop a model that differentiates between “remote-first” and “remote-enabled” jobs in the public sector. Remote-first jobs are those where it would be mandatory to be capable of working long-term remotely, with all organizational processes and systems supporting this. Remote-enabled jobs are those that could be required to work remotely under specific constraints, such as having flexibility toward the equipment needs and physical workplace.

It is not enough to have remote workforce policies or strategies in place, but these changes must be followed. By enabling remote operations of the digital state de-facto, it will help to build resilience in the event of a disruptive crisis. This readiness can be further increased by running crisis exercises. These exercises involve creating a controlled environment for simulating the conditions of a crisis, testing whether the developed remote working operations operate as anticipated.

KEY RECOMMENDATIONS:

- Identify public authorities and positions related to critical services for the continuity of the state and develop a categorization for jobs that should be remote-first or remote-enabled.
- Identify infrastructure and systems not accessible from a remote-first perspective.
- Establish a long-term IT and organizational strategy to shift to remote-first and remote-enabled jobs.
- Create an independent unit responsible for assessing organizational barriers to the remote-first transition and running annual or quarterly exercises that test an organization’s ability to operate under remote working conditions.

03 SECURE DIGITAL PUBLIC INFRASTRUCTURE AND SERVICES

In the digital age, the notion of conflict has changed. Cyberattacks are a daily occurrence and an unavoidable part of the world's new digital reality. As states continue to digitalize, it is essential that cyber security and the protection of digital infrastructure is made a priority. Estonia has been on both sides of this new reality. In 2007, Estonia suffered one of the first national scale cyberattacks in the world. As a result, Estonia implemented new laws and regulations, developed standards, and devoted large amounts of resources into improving their cyber defense capabilities. In the years that have passed, Estonia has managed to successfully defend against numerous massive cyberattacks without significant disruption to its digital society. In most cases, Estonian residents do not even know such events have taken place.

However, this threat will always be present. As much of a state's critical infrastructure has become digital – even physical infrastructure, such as power plants or hospitals – cyber defense must be a national priority. Over the past decades, it has become increasingly clear that while it is possible to build walls around systems, and strongly defend them, if an attacker is significantly resourced and motivated, they will find a way to infiltrate their target's systems.

> **As there is no peace in cyberspace, these digital systems must always be built from the perspective of wartime resilience.**

Investments in cybersecurity cannot be made post-factum they must be implemented from inception.

Ultimately, the long-term best practice is to develop a set of principles for the digital state that (when complied with) significantly increase the cost and time for an attack to be successful. Additionally, as threats are constantly evolving, the countermeasures must too. Digital states must assess and leverage modern solutions and tools to actively monitor, analyze, and respond to cyber incidents, including the use of cloud-based threat intelligence, machine learning, and artificial intelligence for pattern recognition. Gathered threat intelligence must be shared real-time through collaborative platforms across the state and internationally by like-minded nations to enhance its ability to respond and coordinate effectively.

In addition to external threats, countries must also secure the digital state from internal threats. Data integrity must be made a priority so that not even the people guarding or maintaining data for the state are able to change it without a trace being left. The Estonian government started using technologies such as blockchain to assure critical registries cannot be tampered with [22].

Getting this ecosystem right, with cybersecurity at the forefront, will require a digital state to build up its national and institutional cyber capabilities. By creating a community of collaboration between regulators, service providers, research organizations, universities, and companies it is possible to help develop this expertise.

KEY RECOMMENDATIONS:

- → Mandate nationwide adherence to cybersecurity standards and industry best practices while considering nation-wide risk scenarios and enforcing minimum security measures accordingly.
- → Assign a security and criticality classification to information systems and map the cross-dependencies of those systems. Prioritize the continuity of the systems with highest impact.
- → Consolidate the monitoring and analysis of cyber incidents to a centralized body for government wide situational awarenesses and rapid mitigation and response of the incidents.
- → Ensure that there is a sustainable and continuous budget for investment in cybersecurity to reduce the risk in the fast-paced threat environment. Our recommendation is to spend at least 10% of IT-budget to cybersecurity.
- → Enhance national and institutional capabilities in the domain of cybersecurity. Strengthen collaboration with research institutions and reliable partners to continually refine and update protective standards, thereby effectively addressing emerging and future threats.
- → Appoint an organization that is responsible for cybersecurity within the country with executive power for all abovementioned points.

04 ENSURE WIDESPREAD AFFORDABLE ACCESS AND REDUNDANCY TO CONNECTIVITY

Any loss of connectivity during a crisis implies that people are effectively cut off from the state and its services. In today's digital age, access to the internet is as crucial for people as access to basic infrastructure and amenities.

Several countries – such as Finland and Estonia – have implemented policies that declare connectivity as a basic infrastructure need (or even as a human right) and having declared it a national priority to provide every citizen with broadband access. These countries also show good correlation between connectivity and general level of digitalization.

Connectivity must, therefore, be both widespread and resilient, resistant to tampering and adversarial interference. States must aim to improve access and coverage to the internet across their territory and, where possible, create free public access points such as in schools, libraries, and other key locations.

> **Free market and competition should be assured to lower the cost of connectivity and increase the number of options.**

Countries can create incentives, subsidies, tax exceptions, license-free breaks, etc., for new telecommunications companies entering the local market to increase competition.

With widespread and affordable broadband, states can even consider providing a limited free 4G/5G option that can only be utilized to access select services (news, public services, etc.), with the rationale of shifting costs from helpdesks and front offices to digital services.

Building redundancy in connectivity is critical to assure resilience in crisis situations. During times of conflict, the infrastructure of the internet itself may be called into question, and undersea cables are vulnerable to sabotage and destruction. States must consider this and invest, where possible, into new and emerging communication technologies. For example, this may include adopting satellite communication programs that help overcome disruptions to traditional internet connectivity methods.

To further increase resilience during crises, interoperability should be forced to network providers through regulation. Cross-border interoperability further enhances resilience. The state would assure the required agreements between the telecommunication providers. This approach has been best exemplified by Ukraine. Shortly days after the Russian invasion began in Ukraine in 2022, the country's three main cellular operators activated a free roaming service between their respective networks [23]. If a user's mobile network signal becomes unavailable, they are advised to try one of the other two providers.

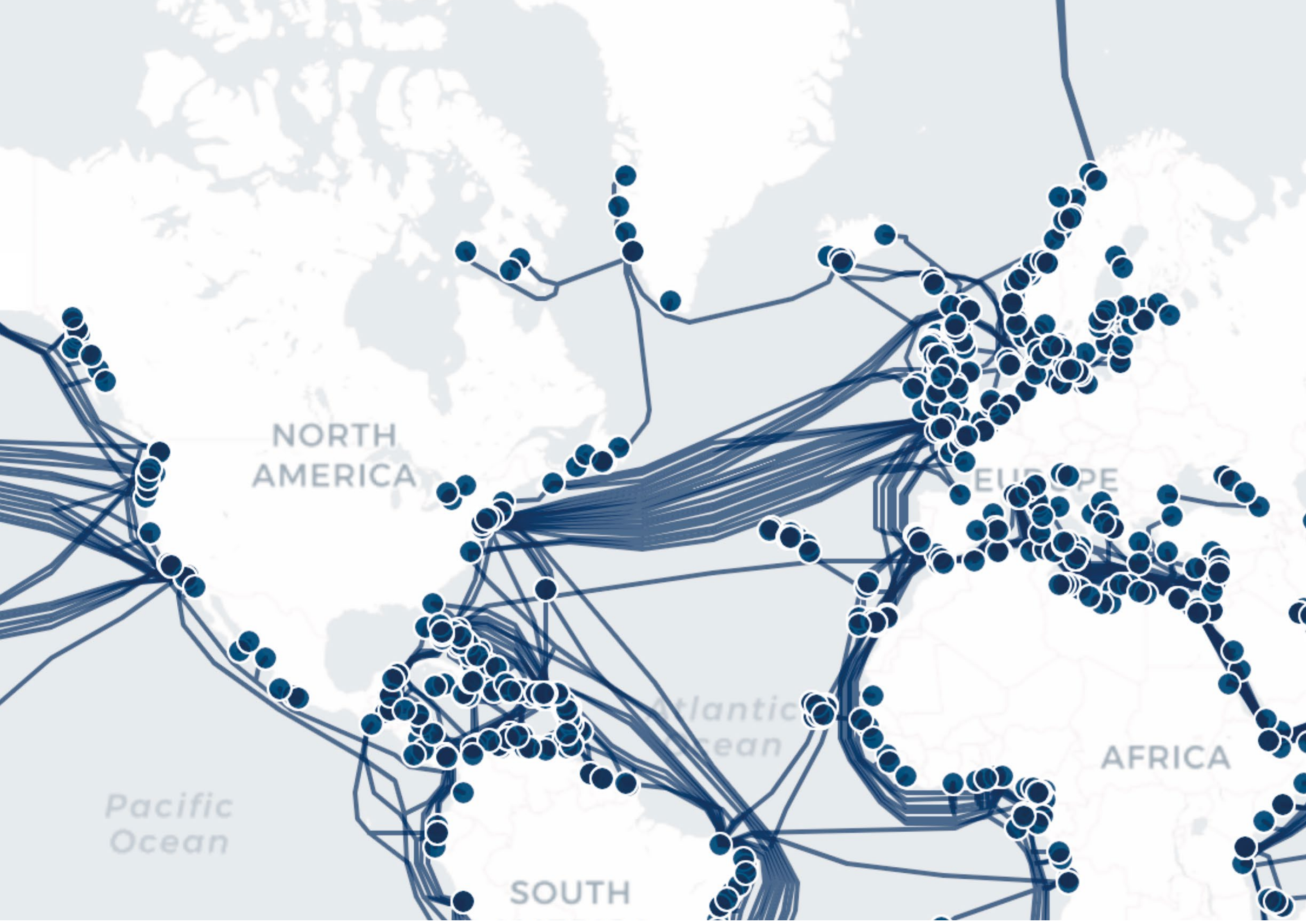

Figure: undersea cables connect the digital world together, but are also vulnerable to sabotage. States must develop resilience in connectivity through multiple technology options.

KEY RECOMMENDATIONS:

Establish a government function (e.g. National Connectivity Board) with direct mandate for:

→ Assure that affordable connectivity options exist for everybody. Consider having connectivity as a form of “human right”.

→ Conduct risk analysis on existing national connectivity options and introduce strategic diversification of connectivity types.

→ Exercise national digital infrastructure continuity in reduced connectivity scenarios. Implement rigorous testing protocols to ensure that critical systems remain operational during network disruptions.

→ Lower the cost of connectivity either through subsidies and incentives for new telecommunication providers or through direct benefits to end-users.

→ Create interoperability between telecommunication providers.

05 BUILD REDUNDANCY TO DIGITAL PUBLIC INFRASTRUCTURE

The extent to which modern societies rely on digital registries and public digital infrastructure is enormous. Most government databases are digital and, in the case of nations such as Estonia, so are almost all public services. Destruction or hostile control of just a few key critical registries or infrastructure facilities hosting them could send a government into turmoil.

A key weakness of digital states is that, fundamentally, their digital data and assets are based on territory in the physical world. If the location of these data are known then this location can be damaged or destroyed and if backups are not available this could deny a state the ability to provide critical services. Imagining a severe scenario, the resulting crisis could even damage the perceived legitimacy of the state itself. Additionally, in the case that key digital registries fall into the hands of an adversary, they could severely disrupt the state's data assets by deleting individuals or companies from registers, changing property rights, or altering the state's finances.

For this reason, several governments have sought to establish a Plan B to prepare for a potentially catastrophic scenario where public data necessary for the state's continuity and legitimacy can neither be tampered with nor destroyed in any circumstance.

One well-known solution for this is the Estonian Data Embassy [24], where key government registries and digital assets are backed up and stored on the territory of another sovereign country. In the case of a catastrophe, the data stored in the Data Embassy can be utilized to restore the legitimate state of governance and assure that tampering has not occurred. When initially conceptualized, this strategy was logical. There were fewer systems, the dependencies were manageable, and the amount of data was significantly lower. More importantly, however, the perception of threat was short-term. It was assumed that a crisis would last a short time – days, weeks, or months perhaps, but not years. It is now clear that this thinking was optimistic.

Today, digital systems are highly interconnected and complex, and any long-term solution would need to be capable of not only backing up data and systems to a sovereign territory but also operating them from there (or at least from other locations in the country).

> **Instead of a state-wide archiving solution, it is even more important to develop a Digital Embassy.**

This solution would allow for the duplication of a sovereign cloud onto foreign territory and, if necessary, allow for a foreign digital state to operate its digital services from it.

The war in Ukraine has highlighted the practical need for such a solution. When Kyiv was partially encircled in 2022, it became evident that Ukraine would face a dire situation if it lost access to is key digital registries. Following the Estonian Data Embassy model, efforts were made to break out of the capital and move entire data centres into friendly countries for safekeeping and backup operations [25]. Soon, large cloud providers also followed, and by today it can be said that Ukraine's digital continuity is assured by NATO countries and companies operating in NATO territories.

This transition toward building a resilient and dynamic cloud environment will not be an easy task. States should start by prioritizing the transition to local or international clouds for critical public services and infrastructure first. This change will require broad legislative and regulatory support, from removing obstacles in the existing legislation to creating capabilities, particularly in terms of international cooperation.

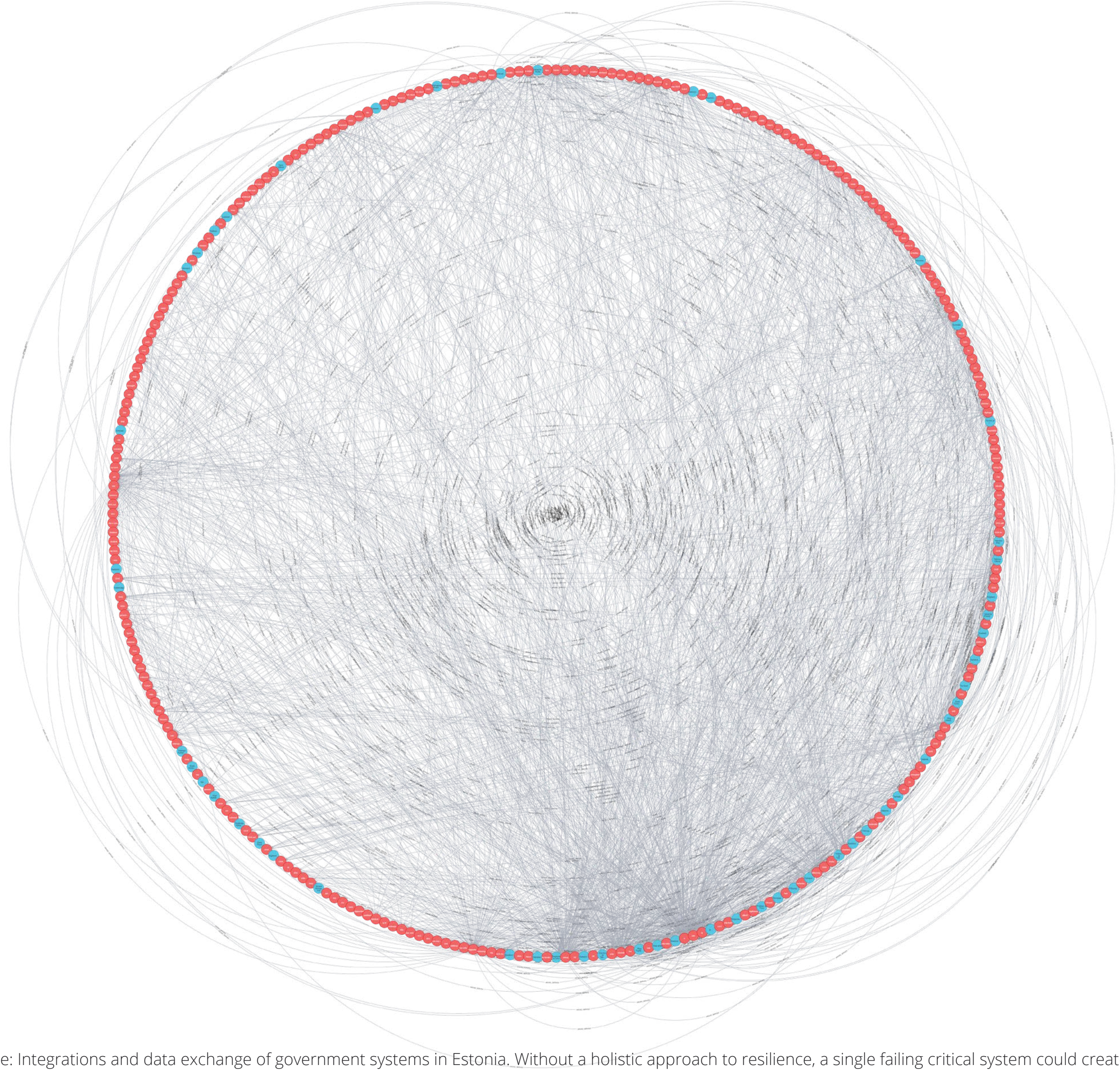

Figure: Integrations and data exchange of government systems in Estonia. Without a holistic approach to resilience, a single failing critical system could create a propagating cascading failure.

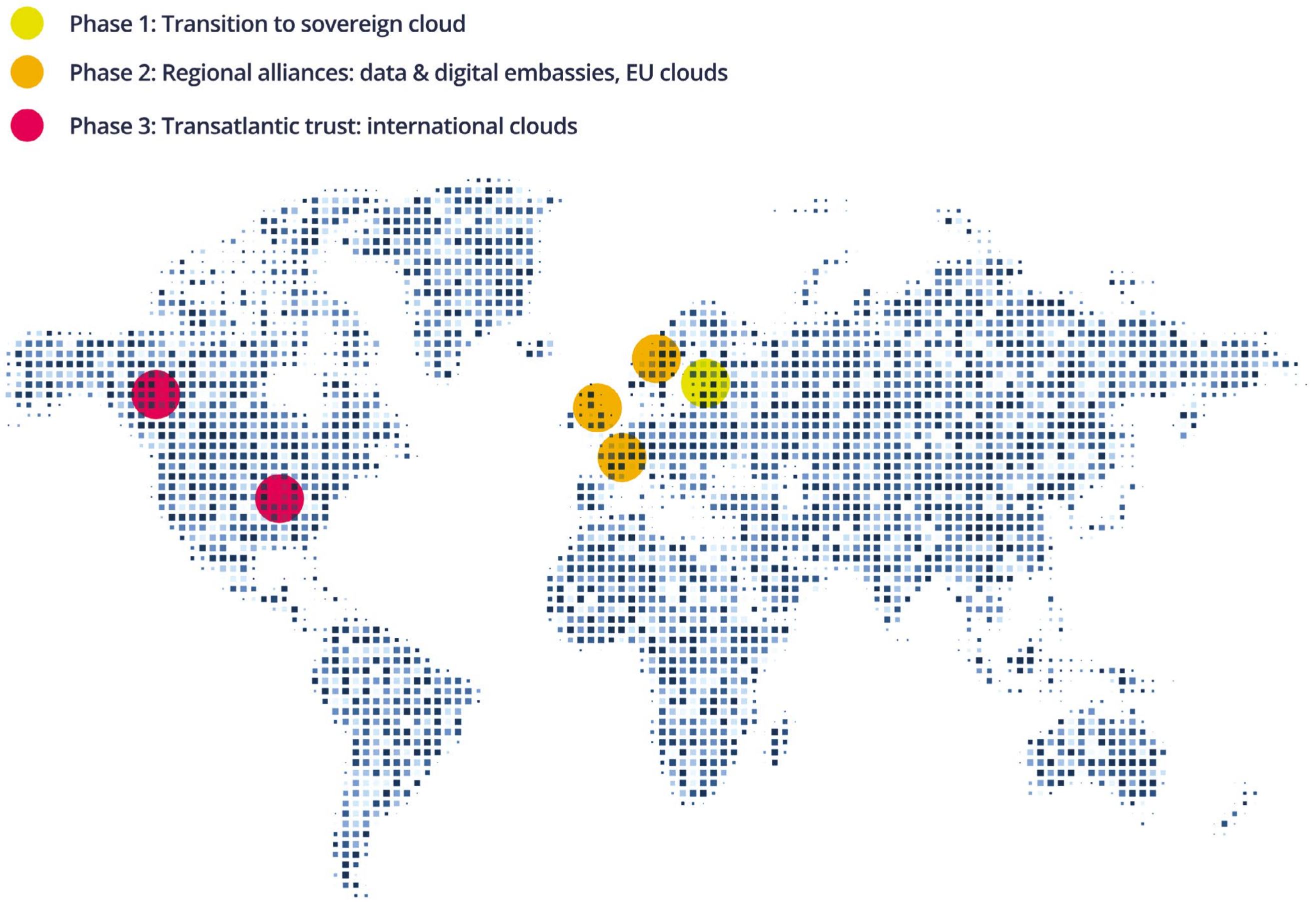
● Phase 1: Transition to sovereign cloud
● Phase 2: Regional alliances: data & digital embassies, EU clouds
● Phase 3: Transatlantic trust: international clouds

Figure: Phased transition to wider international alliances based on mutual trust and agreements. The locations on the map are for illustrative purposes only.

KEY RECOMMENDATIONS:

- Establish national information system standards that mandates critical public services and infrastructure to become cloud-compatible over a specific time span. The standard shall establish mandatory requirements for all government system procurements and internal developments.
- Assess the existing critical public services and infrastructure to identify gaps blocking the transition.
- Work with multinational partners and regulators on assuring control and trust over cloud services.
- Establish a national body (such as National Cloud Governance Centre) which would act as a single point of resource for cloud infrastructure, managing the market research, risk management, procurement, adoption, interoperability and minimum-security requirements for the entire government and providing incentives for all authorities for the transition.

06 MANAGE THE THIRD-PARTY RISK WHILE PRESERVING TECHNOLOGICAL INNOVATION

As the digital world is both globalizing and consolidating, third-party risk management is becoming a strategically critical capability. As much of the world's technology stack relies on third-party components, a compromise to any part of the supply or dependency chain can cause significant damage. Only by assuring the safety and compliance of the entire chain in its depth, could the results be deemed safe. One recent example of a successful supply chain attack was the compromise of SolarWinds, significantly impacting the national security of the United States [26].

Managing third-party risk is hard, and it will get harder. It will require states to be able to make strategic choices about the software and hardware they procure and also develop the capability to have a constant awareness of the current state of the digital global supply chain. While the security and compliance of a limited number of hardware and software products can be assessed to be safe, assuring compliance for all public digital services and infrastructure development and its dependencies in full risk depth is likely too much for any regulator.

Depending on a state and its position toward the global community, they might address these challenges differently. For example, a weighted-risk approach could be chosen where a risk-tolerant strategy could be followed, dependent on the criticality of the subject service. This approach would ensure that critical systems would receive proportionately higher compliance requirements, whereas non-critical systems could either be audited at a lower level or require only voluntary compliance.

However, not all risks can be fully mitigated. Most states are dependent on foreign technologies that have little or no alternatives. The Global Positioning System (GPS) is one example of a cornerstone technology for many modern services with limited competition and low adoption of these alternatives. While larger states may be able to develop their own operating systems, they will almost always rely on third-party components, and even then, it would almost certainly not be a cost-effective use of resources. Instead, regulators are now working to develop long-term SLAs that force compliance with domestic requirements.

In the broader sense, the key challenge to third-party risk management lies in finding the balance between openness and fostering innovation with regulation and ensuring risk mitigation.

To counter the risk of limiting innovation, a risk-tolerant fallback strategy should be utilized. For example, AI tools are mostly cloud-based and incorporating them into a digital state’s operations could potentially create a “black box” dependency. However, following a risk-tolerant approach, instead of banning the external dependency from the service, it could instead be introduced as a switchable feature, which could be turned off at any point. This might downgrade the service experience for the end-user, but it would ultimately not cause the service to fail entirely in case of interruptions with dependencies.

KEY RECOMMENDATIONS:

- → Establish a nationwide risk management policy to manage third-party risks. This policy shall establish rules on which systems can or cannot use what kind of proprietary technologies and if a more comprehensive system must be capable of operating in an emergency mode also independently of said technologies. These rules shall be minimal enough to be practical, implementable, and easily auditable.
- → Enforce the policy and rules for third-party risk management of most common technology and security standards through a central authority. This central authority shall build the capability to monitor and react to changes in the supply chain and find optimal cost-to-risk ratio alternatives.
- → Establish an audit authority for critical public services and infrastructure to comply with the established policy.
- → Exercise the resilience to third-party risks while testing and auditing relevant aspects in the policy.
- → Work with multinational regulators to manage third-party risk globally and share the knowledge with partners in like-minded nations.

07 CREATE INSTITUTIONAL CAPACITY FOR DEVELOPING GOVERNMENT RESILIENCE

Government resilience and plans for the continuity of the state are broad concepts, involving in some ways most if not all functions of the government. Considering scalability, each government function or service should be responsible for their own resilience, creating a de-centralized approach to resilience. This encompasses both specific plans and changes, but also broader increase in the maturity across several disciplines required for the operation of digital services. A recommended approach is to appoint a dedicated advisor in government organizations to develop resilience plans and coordinate with other government bodies and private sector partners.

However, to mitigate the risks of cascading failures, and managing the practical reality of coordinating with large number government authorities, an additional top-down approach is recommended. To see a whole-of-government policy through execution, typically requires creation of a vertical that has necessary executive power and long-term commitment.

For that end,

> **we recommend governments establishment of a vertical body that is responsible for overseeing, coordinating and achieving outcomes that directly relate to increasing government resilience and continuity of the state.**

That unit should be well-placed in the government power structure to be effective in execution, for example under the State Secretary Office or a similar centralized function.

The unit would be responsible for:

1. Owning end-to-end crisis plans across all government.
2. Analysing cross-dependencies for cascade failures and eliminating them.
3. Running government resilience exercises and auditing government organizations for their resilience.
4. Building crisis management competence.
5. Executing crisis management coordination during a crisis with vertical power structure.
6. Policy analysis and coordinating necessary regulative changes.

EXAMPLE OF A GOVERNMENT RESILIENCE EXERCISE.

- In an example scenario of a State Announcements Service, all employees are forced to work remotely. The building is sealed off and powered down, simulating a severe crisis scenario. At the same time, an artificial peak of service load is created, simulating people who are now accessing the service due to the nature of the crisis. To make matters both worse and realistic, the service is also under an extreme cyberattack, further denying access. In an ideal but also achievable outcome, there are minimal to no service interruptions for the citizen.

THE FUTURE OF RESILIENT DIGITAL STATES

The future resilient digital state utilizes the digital domain to ensure its continuity. It is fully digitalized and demonstrates geographical location independence for its core digital services. How a specific state achieves this goal will depend on their respective context but will certainly involve positioning at least part of their core digital infrastructure outside of their territorial border. It also places significant demands on the state's capabilities, as ensuring digital operations requires a level of maturity and coordination likely higher than currently exists.

The above recommendations are offered from the perspective of developing increasingly resilient digital states. However, these recommendations should not only be viewed from a lens of helping states overcome crises. Instead, they can also be understood as an acknowledgement of the future trajectory that the world is facing. Emerging digital technologies are reshaping our world and the way that we exist within it, states are not immune from this change. Failing to digitalize, states will not be able to effectively manage the growing number and complexity of crises they will face in the years ahead. As digital and emerging technologies like AI continue to reshape our world, states must also show their willingness to adapt.

Key to this adaptation will be a state's ability to integrate digital technology into their understanding of the state itself. There is also substantial opportunity for the international community to update the way in which they think about emergent digital states. What might it look like if a state loses sovereignty over its territory due to conflict, or if its territory disappears due to a natural disaster or another crisis? What would it mean if a state was able to maintain its public services, national identity, and democratic system of government via virtual means? These digital states represent a potential future where governance, culture, and community are not necessarily defined only by the territory where an individual is born but by their participation and contribution in the digital realm as well.

This is not an abstract thought experiment, but a call to action to the international community to take this issue seriously. These are issues that the world will have to confront in the near term as some states are already on track to watch their physical territory disappear due to rising sea levels. This is just one example, but there are many more and they are likely to continue to occur in the years ahead.

BIBLIOGRAPHY

1. D. DeSilver, “More countries are now democratic than at any point since World War Two,” World Economic Forum, 11 12 2017. [Online]. Available: https://www.weforum.org/agenda/2017/12/more-countries-are-now-democratic-than-at-any-point-since-world-war-two/. [Accessed 23 10 2024].

2. A. Gore, “The National Information Infrastructure,” 11 01 1994. [Online]. Available: https://www.speeches-usa.com/Transcripts/al_gore-internet.html. [Accessed 10 2024].

3. A. Gore, “VP Remarks -- International Telecommunications Union,” 21 03 1994. [Online]. Available: https://clintonwhitehouse1.archives.gov/White_House/EOP/OVP/html/telunion.html. [Accessed 10 2024].

4. S. Nora and A. Minc, The computerization of society: a report to the President of France, Cambridge, Massachusetts: MIT Press, 1980.

5. The Economist Intelligence Unit, “Global democratic backsliding seems real, even if it is hard to measure,” The Economist, 12 09 2023. [Online]. Available: https://www.economist.com/interactive/graphic-detail/2023/09/12/democratic-backsliding-seems-real-even-if-it-is-hard-to-measure.

6. F. Kostelka and A. Blais, “The Generational and Institutional Sources of the Global Decline in Voter Turnout,” vol. 73, no. 4, 2021.

7. F. Lewsey, “Global dissatisfaction with democracy at a record high,” University of Cambridge, 2020. [Online]. Available: https://www.cam.ac.uk/stories/dissatisfactiondemocracy.

8. A. Polyaakova and C. Meserole, “Exporting digital authoritarianism: The Russian and Chinese models,” Brookings, 2019.

9. M. Mazzucato and R. Kattel, “COVID-19 and public-sector capacity,” vol. 36, no. 1, 2020.

10. T. S. James, A. Clark and E. Asplund, “Elections during Emergencies and Crises,” International Institute for Democracy and Electoral Assistance (International IDEA), 2023.

11. S. Stolzoff, “This Pacific island country is disappearing. What happens next?,” National Geographic, 08 07 2024. [Online]. Available: https://www.nationalgeographic.com/environment/article/tuvalu-islands-sea-level-rise-climate-change.

12. D. Herszenhorn and L. Bayer, “EU leaders agree on €1.82T budget and coronavirus recovery package,” POLITICO, 21 07 2020. [Online]. Available: https://www.politico.eu/article/eu-leaders-reach-deal-on-coronavirus-recovery-fund/.

13. K. McBride, “Regulation is Not Enough: A Blueprint for Winning the AI Race,” Just Security, 29 06 2023.

[Online]. Available: https://www.justsecurity.org/87005/regulation-is-not-enough-a-blueprint-for-winning-the-ai-race/.

14. M. Schaake, The Tech Coup: How to Save Democracy from Silicon Valley, Princeton: Princeton University Press, 2024.

15. M. Scott and K. Komaitis, “Reenvisioning Europe’s digital sovereignty,” POLITICO, 23 09 2024. [Online]. Available: https://www.politico.eu/article/europe-ursula-von-der-leyen-tech-brussels-digital/ .

16. T. Burt, “Escalating Cyber Threats Demand Stronger Global Defense and Cooperation,” Microsoft On the Issues, 15 10 2024. [Online]. Available: https://blogs.microsoft.com/on-the-issues/2024/10/15/escalating-cyber-threats-demand-stronger-global-defense-and-cooperation/.

17. B. Smith, “Defending Ukraine: Early Lessons from the Cyber War,” Microsoft, 22 06 2022. [Online]. Available: https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/. [Accessed 23 10 2024].

18. J. A. Lewis, “Cyberattack on Civilian Critical Infrastructures in a Taiwan Scenario,” CSIS, 11 08 2023. [Online]. Available: https://www.csis.org/analysis/cyberattack-civilian-critical-infrastructures-taiwan-scenario.

19. K. Butzer, “Collapse, environment, and society,” Proceedings of the national Academy of Sciences, vol. 109, no. 10, 2012.

20. B. Hammi, S. Zeadally and J. Nebhen, “Security threats, countermeasures, and challenges of digital supply chains,” ACM Computing Surveys, vol. 55, no. 14s, 2023.

21. R. Panwar, J. Pinkse and V. De Marchi, “The future of global supply chains in a post-COVID-19 world.,” California Management Review, vol. 64, no. 2, 2022.

22. S. Semenzin, D. Rozas and S. Hassan, “Blockchain-based application at a governmental level: disruption or illusion? The case of Estonia,” vol. 41, no. 3, 2022.

23. European Commission, “Joint Statement by EU and Ukrainian operators to help refugees from Ukraine stay connected,” 05 04 2022. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/joint-statement-eu-and-ukrainian-operators-help-refugees-ukraine-stay-connected.

24. T. Kotka and I. Liiv, “Concept of Estonian Government Cloud and Data Embassies,” Valencia, Spain, 2015.

25. C. Stupp, “Ukraine Has Begun Moving Sensitive Data Outside Its Borders,” Wall Street Journal, 06 14 2022. [Online]. Available: https://www.wsj.com/articles/ukraine-has-begun-moving-sensitive-data-outside-its-borders-11655199002.

26. D. Temple-Raston, “A ‘Worst Nightmare’ Cyberattack: The Untold Story Of The SolarWinds Hack,” NPR, 16 04 2021. [Online]. Available: https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack.