Chapter 2

KEY FUTURE UNCERTAINTIES IN DIGITAL TRANSFORMATION AND POTENTIAL IMPLICATIONS FOR LATVIA

Introduction

Digital transformation is driving rapid change on an unprecedented global scale, generating heightened uncertainty. In this context, individuals, organisations and governments planning for upcoming decades can no longer rely on assumptions that the future will resemble the present to any great extent. Rather, they must explore and prepare for a range of alternative scenarios embodying potential changes and the new opportunities and challenges they might bring. Such an approach can help ensure that the strategies and policy frameworks designed today are resilient and adaptive in the face of digital transformation and the direction, pace and scale of changes it could bring.

This chapter begins by exploring three alternative scenarios for the future of digital transformation, based on broad differences in power structures and relationships between societal actors. The first scenario considers a world where active citizens take digitalisation into their own hands and form a comprehensive "third pillar" of empowered online communities that provide a counterweight to states and markets. The second scenario describes a world in which governments set up digital platforms that become the backbone of their economies, promoting exchange between countries using the same system but creating barriers with those who do not. The third scenario presents a future in which multinational digital corporations become so efficient and comprehensive in serving their users that many of the roles traditionally held by the state, such as education and welfare, are offered by non-state entities.

Individually, and as a set, these scenarios provide an opportunity to rethink untested assumptions about future trajectories and the policies built on them. What roles might communities and peer-to-peer initiatives play in Latvia's digital future? What kind of digital government does Latvia want to be? In which strategic partnerships and collective initiatives might Latvia participate to secure its place in the world? Scenarios in themselves do not provide answers to these questions, but rather provide a framework within which such questions can be asked.

The chapter concludes by identifying some key perspectives for action that emerge from the scenario analysis. These actions fall into four main categories: 1) evaluating and strengthening Latvia's strategic partnerships for digital transformation; 2) identifying smart approaches to education and skills for adaptive and critical Latvians; 3) finding pathways to an inclusive digital Latvia, by and for the people; and 4) building capacity to benefit from the access and use of personal data while safeguarding digital security and privacy.

Why scenarios? Decision making in a context of uncertainty

The pace and scale of digital transformation is creating a high level of uncertainty regarding the shape of the future in the coming years. As a range of linked digital technologies continue to emerge and combine, enabling radical new actions and behaviours, these in turn produce cascading and uncertain implications for all aspects of society, the economy, environment and governance. Unlike more predictable global megatrends, such as population aging, which may take place gradually over decades, technological change can lead to sudden and divergent impacts that are difficult to anticipate.

It is impossible to predict or fully control which new business models may emerge, which new forms of collective action may be enabled, which digitally powered forms of state involvement may prove most effective, how the structure and functioning of the economy may evolve, and how the changing nature of value and power in a more digital world may reshape the global order. With each of these uncertainties come potential changes that could bring tremendous opportunities to improve human well-being and address complex global challenges, but could also generate significant disruption and create new potential threats.

Designing effective strategies and policies in a fast-moving and unpredictable domain such as digital transformation demands a strategic foresight approach (Box 2.1). This entails looking beyond current trends and expectations about the future and considering a number of different scenarios. Foresight scenarios are a set of alternative descriptions of how the future might look, constructed for the purpose of taking action in the present. They are not forecasts or an attempt to predict what the future will look like. Neither are they a set of recommendations or vision of any particular desired future. Put simply, scenarios do not say what *will or should* happen; only what *might* happen, leaving the question what can be learned from them open to discussion.

The foresight scenarios presented in this chapter are intended to help Latvian decision makers better anticipate disruptive changes, develop innovative new strategies and policies, and test existing plans and practices against a range of plausible alternatives. Additional benefits from using scenarios in policy making include the ability to reveal and test implicit assumptions about the future in current policy, to connect policy domains previously separated into silos, to turn disagreement among experts into an asset and to discuss matters that might otherwise be too sensitive to raise.

The scenarios were produced using the outputs of an initial one-day foresight workshop that brought together a wide range of Latvian stakeholders working in the fields of policy, technology academia and others. The scenario exercise also incorporated findings from a series of interviews with Latvian policy makers and experts, a foresight survey, an OECD internal scenarios exercise, and inputs from the OECD Directorate for Science, Technology and Innovation. Two additional foresight workshops were then held to refine the policy implications brought forward at the end of this chapter and to identify crucial issues for Latvia's digital future.

Box 2.1. What is strategic foresight?

Strategic foresight is a discipline that looks beyond current assumptions and, instead, takes into account a range of plausible future developments with a view to identifying implications for policy making. It employs a range of methodologies, such as scanning the horizon for emerging changes, analysing megatrends and developing multiple scenarios.

Strategic foresight can assist governments in designing **more resilient and adaptive strategies** through the following approaches:

- **Better anticipation** identifies changes that could emerge in the future and new opportunities and challenges for policy making.
- **Future-proofing** uses a range of plausible future scenarios to stress-test existing strategies.
- **Policy innovatio**n develops new innovative ideas and policies that are robust across a range of futures.

How to use this chapter

This chapter is intended as a starting point for further analysis and deliberation on the future of digital transformation and potential implications for Latvia. Its findings, while largely consistent with the rest of this report, can also be viewed as complementary, and can serve as an additional lens to evaluate how best to implement the recommendations contained in other chapters, in particular where these might be affected by unexpected future developments.

Above all, it is hoped that this chapter will serve as an inspiration and building block for ongoing strategic foresight dialogue in Latvia. This entails modifying the scenarios and developing new ones as circumstances evolve, as well as exploring the deeper intersections of digital transformation with other key sources of disruption, such as COVID-19 (Box 2.2). Such sustained and participatory strategic foresight efforts by Latvia's decision makers and the broader policy community will be indispensable to the ongoing work of developing resilient and adaptive strategies for Latvia's success in the digital era.

Box 2.2. Implications of the COVID-19 pandemic

The sudden emergence of the COVID-19 global pandemic provides a clear reminder of the importance of preparing for the unexpected. Although the likelihood of such a pandemic had long been accepted, its precise timing and nature have been unpredictable. The pandemic is now generating further cascading waves of disruption and uncertainty affecting all areas of policy. In this context of heightened turbulence, strategic foresight approaches, such as the one demonstrated in this chapter, can help governments avoid the risk of making policy decisions based on overly hasty or narrow assumptions about the future.

Some interactions between COVID-19 and digital transformation already seem clear, including a sudden acceleration of online work, learning, commerce, entertainment and politics. The uncertainties, however, are even greater. For example, will there be a lasting growth in virtual work, and how might this affect earnings and migration patterns both within and between countries? Will COVID-19 hasten deglobalisation and the creation of separate digital regions, or create momentum for renewed global collaboration? Will the economic crisis increase the dominance of large technology firms or create new niches for innovative competitors? Will citizens welcome or reject new forms of digital surveillance aimed at advancing public health? Could concerns over increasing sovereign debt lead to a growth of cryptocurrencies? What kinds of digitally enabled political movements might emerge as a result of the social fractures accentuated by the crisis?

While this chapter was drafted before the emergence of the COVID-19 pandemic, the three scenarios described can serve as a valuable foundation for thinking through many of the further uncertainties and possible developments related to the interactions between COVID-19 and digital transformation, and the potential implications for Latvia's digital strategy.

Directions for a desirable digital Latvia

The ultimate purpose of the strategic foresight analysis in this chapter is to help Latvia identify pathways towards a desirable digital future, while consciously navigating a context of uncertainty. In order to create a basis for this discussion, the workshops included an exchange on overarching priorities and aspirations for the country's digital future. These should not be considered a formal consolidated government vision, or the official position of any individual or organisation. Rather, they capture some insights into future directions that were perceived favourably by Latvian stakeholders and policy makers alike. During the intervention, these directions served as a first step towards identifying strategic options for the government to consider. They represent a starting point for discussion, setting a basis for a fruitful debate on Latvia's ambitions and priorities going forward.

Stakeholders and policy makers both voiced their desire for an inclusive digital Latvia for and by the people. This would imply putting the well-being of Latvians at the centre of any decision, programme or policy objective, and giving Latvian citizens a chance to connect, contribute and be digitally active. Latvians have expressed a desire for a digital future where they can participate in their own language and in line with their individual capabilities and limitations. This aspiration carries the need to create digital opportunities for all and ensure that Latvians have the necessary skills and tools to make use of them to their best advantage. Stakeholders wish to be involved and be given the chance to contribute to Latvia's digital transformation. One way to allow the voices of citizens to be heard would be public consultations on digital topics.

Closely linked to this aspiration is the desire for a successful digital Latvia to be based on a smart approach to education and skills. This includes an adaptive and responsive education sector that fosters digital learning for all Latvians, both in the form of generic ICT skills (digital literacy and data literacy) as well as complementary skills such as information processing and problem-solving capacities. A digitally skilled nation is one where citizens in urban and rural areas alike can benefit from digital opportunities and know how to safeguard themselves in digital environments. It is one in which learning systems at all levels have the capacity to adapt and evolve with their environment, responding to market needs and technological development. It also works to fully harness the rapidly improving opportunities for life-long learning outside the formal education system, made possible by technological advances, for example learning by doing at work and in daily life. Smart education would allow for existing knowledge and expertise to spread and for new partnerships to form and flourish. In Latvia, digital skills should not be considered in isolation, but rather be closely connected to people's personal and professional ambitions, and seen as a means to enhance the human capital of all citizens.

Another aspiration for Latvia's future is to create a sense of connectedness by strengthening the country's internal co-operation and networks. Stakeholders and policy makers alike voiced the wish for greater collaboration between public, private, civil society, academic and individual actors, in order to better connect existing capabilities. Moving from shorter-term, project-based agreements towards more long-term partnerships in various fields could allow for even more stable relationships to develop. These partnerships might exceed the purpose of knowledge exchange, creating a productive environment where innovation can flourish. Strategic connections between the myriad successful projects in the digital field would strengthen Latvia's position as a small and flexible country. This approach could also offer opportunities to serve as a test bed for new public-private partnership concepts.

A further desired aspect of Latvia's digital success is the ongoing capacity to safeguard digital security and safety. This means enabling Latvians to use technologies in a safe and protected manner, while allowing them to share data openly. Rapidly evolving conditions require constant strengthening of digital security and ethics safeguards, built systematically into decision-making processes. The desired result would be the successful integration of digital systems with both individual and institutional security a priority.

Three scenarios: Imagining Latvia in various future contexts

The three scenarios below provide alternative descriptions of future environments that Latvia could face in the coming years. These scenarios are intentionally extreme, fictional simplifications intended as a tool for identifying potential new opportunities and challenges. None of these scenarios will come about as described and the truth is likely to be a messy combination of all three as well as other factors. The state of the Latvian society and economy in each of the scenarios can only be imagined – and will depends on a range of interconnected (re)actions and developments, as well as various policy choices over the course of many years. Nonetheless, it is possible to envisage certain characteristics of each of the "future Latvias", pointing towards challenges the country may face as well as opportunities it can seize.

#Me2.0

People have harnessed digital technologies to create new regional and global communities to better advance their interests.

These movements have challenged the dominance of governments and firms, forming a third pillar of the global system: the civil sector.

Communities use technologies effectively to tackle local and global challenges.

Polarisation between groups and questions of accountability remain challenging.

Platform governments

Governments operate highly efficient and effective online platforms that facilitate economic exchange and most other activities.

Most governments belong to political blocs with platforms that interact with each other but not with other blocs.

Infrastructure is of paramount concern in the national development and security strategies of countries.

Large amounts of data in government control come with great responsibility, and the need for checks and balances.

Corporate connectors

A small number of global technology companies function as one-stop shops for every aspect of life.

Through their economic power and analysis of popular will, technology corporations have gained legitimacy to take up space in global governance.

Many fields previously under the charge of governments are now in the hands of corporations.

Trust in corporations is high and the main allegiance of most people is to a firm, not a government.

#Me2.0

Summary

It is 2035, and people around the world have harnessed digital technologies to create new social movements and community structures to advance their needs. In so doing they have challenged the dominance of territorial governments and private sector firms, creating a revitalised third pillar within the global economy, society and governance system: the civil sector. People use their online identities in increasingly active ways to further their economic opportunities, civic participation and personal development, both in digital and physical space. Technologically enabled peer-to-peer-like organisation structures, grass-roots initiatives and self-organised global, regional and local communities have empowered citizens like never before.

#Me2.0

- People have harnessed digital technologies to create new regional and global communities to better advance their interests.
- These movements have challenged the dominance of governments and firms, creating a powerful third pillar of the global system: the civil sector.
- Communities use technologies effectively to tackle local and global challenges.
- Polarisation between groups and questions of accountability remain challenging.

Together with more readily available technologies, value shifts have driven people to mobilise around common goals on both an ad-hoc and ongoing basis. As environmental degradation and resulting inequalities increased, trust in global institutions to develop tangible solutions and protect common resources fell significantly. Citizens began to take the initiative to come together and look for new ways to build low-impact lifestyles, foster better health outcomes and recreate a sense of community. Small-scale experiments and pilot initiatives on a local level, and collaboration through connected digital communities on a global level, allowed them to forge a new way path. These new communities no longer fit with previously established definitions and boundaries of civil society organisations, with many adopting new formats and approaches. Some blend online and offline activities and have evolved from existing structures to support particular interests; others emerge ad hoc based on a spontaneous expression of a grievance, trending hashtag or current event. Communities at the global, regional and local levels connect, co-ordinate and compete in a complex cross-cutting pattern of interactions.

Rather than displace governments and business entirely, however, these new movements and organisations serve as a complement and counterbalance, providing the necessary political pressure and practical examples to force governments and firms to perform better in meeting citizen and consumer needs. Nevertheless, new challenges have arisen with the growing power of these societal movements and organisations, including diverging outcomes and polarised views among members of different communities, and inconsistent standards of transparency, accountability and democratic decision making.

Signals: Self-organised communities, digital commons and open source intelligence

Strategic foresight uses signals of change observed in the present to point to plausible new trends or discontinuities that could emerge and grow, and result in a future scenario which differs from current expectations. The following signs of change are already visible and, if they continue to grow, could give rise to the scenario in the previous section.

The Internet has brought about a range of self-organised communities and online mass collaboration projects. Examples include wikis (most famously Wikipedia), open licensing organisations, open source software repositories and communities, and peer-to-peer support networks. The architecture of the Internet itself was developed partly through a community approach by a group of computer scientists, engineers and technicians.

Online community organisation led to powerful action taken offline, most famously during the Arab spring or the 2009 Iran “Twitter revolutions”, but also in the context of the “Fridays for Future” movement, which pushed for greater action to tackle the environmental crisis, or the “#MeToo” campaign, which called for action against sexual harassment. Often these networks serve to fill a gap in management or legislation, which is not adequately addressed by governments or corporations. For example, mutual-aid accountability is an effective response to online harassment on platforms such as Twitter, and mutual-aid mentorship technology can help track spam responders, for example on Wikipedia (Matias, 2015).

The Internet has allowed people to protect and manage common resources in new powerful, community-driven ways (Hesse, 2008; Walljasper, 2011). For example, the citizens of Sarantaporo, a small village in Greece, founded an initiative to deploy local broadband infrastructure as a commons in the absence of dedicated efforts by telecommunication networks or the government (Mölleryd, 2015). Other people have formed their own commons to mix music and videos, as have scientists who use open access, community-managed journals to publish their research as an alternative to commercial publishers. Among many others, digital commons are also devoted to sharing university course curricula and to gathering together neuroscientific research found across the web (e.g. Open Course Ware by the Massachusetts Institute of Technology).

Similarly, people are taking steps to exercise control over artificial intelligence (AI), machine learning methods and the ways in which data are processed and used. Open source intelligence (OSINT), which allows actionable and predictive intelligence to be obtained from public, unclassified sources, is also gaining traction. Open source AI technologies and AI kits, based on open source platforms, are making machine learning projects accessible for everyone. In addition, individuals increasingly want to understand the algorithms behind the appliances they use. For example, AutoPilot, an autonomous car development platform, is working on a software that could allow its users to see the visual elements the AI is tracking when driving (Nvidia, 2020).

How this world came about

In 2019, the Internet held unprecedented opportunities for community-based collaboration and empowerment. Increasing availability of assets such as open source software, broad information sources and large-scale databases have given individuals the means to be creative, experimental and effective in powerful ways. With digital literacy and related skills improving on a global scale, coding and software development have shifted from an expert field to the mainstream, with most digital appliances becoming accessible for everyone. More and more individuals have discovered how technologies such as AI, 3D printing and distributed ledgers could allow them to make real-life improvements in their own communities.

A spate of data leaks and publicity surrounding large-scale, data-driven manipulation, as well as environmental and ethical scandals in the corporate technology sector, led to a growing sense of disempowerment among individuals online. As a response, civil society groups began to advocate for more transparent data management policies, users started to boycott certain providers, and community-driven alternative services and platforms started to emerge, challenging the dominance of corporate ones. As a means to regain trust, both governments and corporations sought community advice, and consulted with civil society to design more legitimate and safe digital products and services.

Meanwhile, deep uncertainty and volatility linked to climate crises and inequality resulted in social unrest, disrupting “business-as-usual” local and national political systems. Few systemic changes were implemented on time, and in most parts of the world, pollution, waste and emissions kept increasing while climate disasters hit vulnerable communities particularly hard. Citizens looked for ways to fill the solidarity gap left by corporations and government, and built up trust in local initiatives, communities and constituencies. As a result, the civic sector expanded significantly, equipped with digital technologies that enabled these groups to adopt their own governance rules, develop effective decision-making mechanisms, and create value locally and sustainably. Examples include the creation of AI and blockchain-enabled experiments, for example, to grow crops, introduce safe lending systems and build sustainable, community-based housing models.

What this world looks like

Under the **#Me2.0 scenario**, Latvia's civil sector functions as a central new pillar addressing national and local issues that were formerly within the government's purview. Society harnessed the untapped potential of Latvia's digital infrastructure and created local and cross-border groups of like-minded individuals to address issues in a direct, tailor-made manner. This might include co-ordinated actions for environmental protection, and the gathering and sharing of information both online and in person through widespread automation and use of open source AI (e.g. for transport and logistics). As a consequence, Latvians generally have high confidence in the potential of their individual actions to effect change, as well as the potential of concerted efforts. In communities with high digital literacy, online education opportunities are widely used, enabling citizens to specialise in a broad range of professional fields and to access international job markets.

However, due to a sharp generational and rural-urban digital divide which excluded some communities from digital emancipation processes, society might have become increasingly polarised. This could include a growing division between citizens living in the same geographic areas whose membership of digital communities and cross-cutting social movement increasingly shapes their identity and their lives. Those who turned away from the digital sphere due to a lack of skills, or increased difficulty with distinguishing between fake news and legitimate information, were left behind and find participating in public discourse difficult. Populations living in less vocal or well-organised local or online communities have a lower capacity to lobby for government services and economic activities, and find themselves increasingly vulnerable to digitally organised criminal activity.

Insights about Latvia's digital strategy

The #Me2.0 scenario highlights the potential importance of emerging new actors in the civil sector and the associated implications for Latvia. It underscores the potential benefits of tapping into specific, tailored knowledge of communities and social movements of various forms – online and offline, local and internationally connected, formally organised and ad hoc. Such communities may function as a powerful means to generate feedback about the varying needs of Latvians for digital learning or public services based on their differing regions, age groups or ethnic background. Minority-oriented social movements could also take on an important role in fostering social cohesion within Latvian society by generating data and insights to improve inclusion and diversity policies.

The scenario points to opportunities that could arise from promoting digital community building in an inclusive and ethical way, in order to empower citizens and mobilise ideas, talent and energy towards achieving societal goals. Conversely, the growing importance of digital communities might also heighten the risks posed by increasing divisions and disputes over values between members of different groups. Online division and polarisation could create closed communication circles with each promoting its own relative truth. Furthermore, risks associated with enhanced opportunities for organised criminal activity quickly become apparent. Digital communities based in Latvia may be well connected to foreign partners, undermining established national security and ethical standards. Overall, the scenario poses the question of which new collaborative structures and frameworks would best allow the country to connect new actors with established ones to create economic and social innovation, while simultaneously keeping citizens and communities safe.

Based on the #Me2.0 scenario, policy makers in the digital field could explore a range of strategic questions:

1. What role should communities, local initiatives, peer-to-peer approaches and **decentralised technology development** play?
2. What new **resources and support could be made available to civil society organisations** to help them connect digitally on a global scale?
3. How can **digital community building be promoted**, for example through local initiatives that are co-ordinated and promoted online, such as participatory municipal budgets?
4. How could **emerging technological values disputes be identified** and foster honest and factual debate?

Platform governments

Summary

The year is 2035 and platform governments have played a decisive role in shaping the digital transformation in two main ways. First, most governments now provide and leverage a main platform for digital activity in the economy and society. Second, many governments have become integrated into digital megaregions, openly sharing data internally while maintaining digital borders with the outside.

Platform governments

- Governments operate highly efficient and effective online platforms that facilitate economic exchange and most other activities.
- Most governments belong to political blocs with platforms that interact with each other but not with other blocs.
- Infrastructure is of paramount concern in national development and security strategies.
- Large amounts of data under government control carry great responsibility, and necessitate checks and balances.

In this world, government platforms channel digital activity by citizens, corporations and societal organisations, a process which allows for the collection and analysis of large amounts of data by the state. These detailed insights allow governments to provide highly efficient service delivery and develop policies in a highly targeted manner. Platform users have a crypto-verified digital identity that ensures trust as well as a seamless transition between the analogue and digital world.

Most platform governments are members of a bloc or alliance, operating as part of a common digital megaregion. Each region interconnects societies closely on the inside and separates them from the outside through a digital border. Data flows freely between all members of each region, and governments are able to use aggregated data analysis to make informed policies. What used to be the World Wide Web has diverged into multiple national and supranational systems on the one hand, and ungoverned digital spaces outside any institutional control on the other. Data, trade and investment flows between regions are highly limited and undergo thorough scrutiny.

Signals: Digital public services, citizen ranking, unique identity systems, foreign investment screening and provider regulation

Strategic foresight uses signals of change observed in the present to point to plausible new trends or discontinuities that could emerge and grow, and result in a future scenario which differs from current expectations. The following signs of change are already visible and, if they continue to grow, could give rise to the scenario in the previous section.

A range of signals in the present show how governments are taking a more digitally driven approach to interacting with citizens – expanding digital service delivery, providing citizens with unique digital identities and using big data for rating purposes. Furthermore, a number of governments have taken steps to ensure control over various layers of their digital space through measures such as foreign investment screening, data localisation and provider bans.

A wide range of countries have established various forms of digital service delivery. The Estonian government was an early adopter in this regard, creating e-Estonia, a countrywide digital initiative using electronic solutions to facilitate citizen interactions with the state. Numerous online services such as digital identification, digital signatures and online medical prescription have been made available to citizens, initiatives similar to which exist in New Zealand, Singapore and the United Kingdom. The backbone of e-Estonia is an underlying data exchange platform called X-Road that links all information systems of the government to make data easily accessible. The system was designed to scale as new e-services and new platforms come online and other governments join the network. Governments also seem to have the lead in the field of digital currency; for example, the European Union is debating the introduction of its own cryptocurrency (Guarascio, 2019).

Government identification systems are evolving in many parts of the world, often as an essential component of digital government. India has set up the world's largest biometric system, Aadhaar, with more than 1.2 billion registered citizens. The Unique Identification Authority of India (UIDAI)[1] issues a 12-digit number to residents which allows for greater transparency of identities and the roll-out of government welfare schemes and programmes. Aadhaar is a key component of Digital India and was designed as a strategic policy tool to improve social inclusion and public sector delivery as well as budget management. Other national electronic identity programmes have been launched in Algeria, Cameroon, Italy, Jordan, Senegal and Thailand.

Governments use digital means and big data to create personal profiles and rate or predict behaviour. The People's Republic of China (hereafter "China") is pioneering a nationwide "social credit" system, which uses big data to assign a score to natural persons and legal entities, drawing on a wide variety of sources. The system centralises data under a single identity, assigns a score, and adjusts interactions and governmental services accordingly. It is envisioned as a powerful tool for the enforcement of laws, regulations or other party-state targets (Shi-Kupfer and Ohlberg, 2019). Other countries are working with similar rating mechanisms in specific areas. For instance, Canada's new Express Entry system for the selection of labour migrants allocates points for a broad variety of socio-demographic characteristics to predict successful labour market integration. In the United States, social media information is required for visa applicants, in order to create risk profiles.

Many countries have increased scrutiny over foreign investment, a move that may allow them to protect their own digital markets. In 2017, China introduced the Cyber Security Law, which defines key categories such as "critical infrastructure" and "personal data" in a broad way, presumably as a means to exert control over foreign investment. The Cyberspace Administration of China is authorised to pursue a cyber security review of all products and services used in critical infrastructures – including the exposure of source codes (KPGM, 2017). Some governments such as Germany have adopted a more explicit approach in recognising digital issues in national security, while others such as the United States are thoroughly scrutinising foreign investment in digital businesses.

Other ways in which governments exert influence over the digital space include data localisation rules, restrictions on cross-border data flows and Internet provider bans. Legislation of cross-border data flows can take various forms. Some require *ex post* accountability for the data exporter if the personal data sent abroad are misused, others make data transfer subject to various types of safeguards and some are subject to case-by-case authorisation (Casalini and López González, 2019). Data localisation requirements stipulate that firms must store certain digital data in host countries and thus set up storage infrastructure. Both requirements are becoming more common and tend to target particular types of data, in particular those with a personal or sensitive component. Examples of provider bans include the introduction of the Russian Sovereign Internet Law to replace the Domain Name System, and bans of certain Internet services by governments as a means to support the establishment of local providers (BBC News, 2019).

How this world came about

Between 2019 and 2035, a few governments employed a more active approach to digital transformation, introducing digital platforms to improve their way of working. At first, citizens and corporations used the platform for a limited number of services, such as managing health records, filing taxes and registering a product or business. As satisfaction grew with the convenience of this approach, services expanded gradually into fields such as financial accounting, smart contracts and skill development. No major hack or other breach that would have impeded trust occurred during this phase. Instead, trust in the system and among its users was high and the use of unique digital identities improved online accountability and traceability. As the number of interactions through the platform increased, its usefulness grew and its name began to be synonymous with the Internet.

Thanks to the increasing amount of data collected and the interlinking of databases, governments gained unprecedented insights into the behaviour, needs and preferences of their citizens and companies. Policy making became more targeted and data-driven, serving the needs of individuals and organisations in fast, customised and adaptable ways. For example, the medical records of a child born in a hospital would automatically be analysed by artificial intelligence, and used to allocate government financial support and identify schooling options years ahead of time. Despite existing privacy concerns, the majority of the population voiced high levels of satisfaction with the new system. Political support rose for the implementing platforms, with better social and economic outcomes reported than for their less digitally driven neighbours.

Acceding to pressure from pioneering governments and public demand, other governments followed this example and started building their own platforms, or commissioning existing ones to adopt new approaches. Within a few years, a highly governmentally driven approach to digital transformation became the dominant model with platforms consolidating further to benefit from economies of scale. Only a few countries opted out of this trend by taking a more passive approach, or alternatively using government power primarily as an instrument to slow down the digital transformation and its impacts.

Countries connected to each other within digital megaregions eventually restricted data flows from and to other regions in order to protect local providers and exert better control over data management. Security concerns gave rise to restrictions on foreign investment in the digital space and eventually ensured that rival regions did not possess a financial or political stake in the platform. This allowed for effective protection of citizens' personal privacy and industry intelligence vis-à-vis external threats, and necessitated strong digital borders consisting of firewalls and cyber protection.

However, these measures were partially offset by the additional opportunities this approach created for local digital companies. Some smaller countries created an alliance permitting mutual free data flows based on common privacy standards and a shared data frontier with the rest of the world. A few global institutions emerged to enable trusted data flows between different countries or blocs, respecting their various conditions.

What this world looks like

Under the **Platform Governments scenario** Latvia becomes a digital platform government, within a bloc of like-minded states. Building on its high system integration capacity Latvia develops a sophisticated data collection and management system and fosters the continuous adoption of services by the government platform. This enables citizens, businesses and civil society actors to access high-quality services more easily, with a concomitant rise in overall trust in government. As with all governments, however, institutional mechanisms and incentive structures do not always allow Latvia to make the most of new data insights, and as a result some opportunities are missed resulting in sub-optimal outcomes.

Latvia co-ordinates closely with other countries in the same digital bloc, which may be limited to Baltic or Nordic countries, span Europe or include like-minded partner countries geographically dispersed around the world. While intra-state and intra-bloc data circulation is generally welcomed as a means to improve quality of services, data leaks to agents outside Latvia's digital region are feared. Indeed, as a result of a prior lack of investment in a comprehensive cyber security framework, Latvia has faced various large-scale hacks and cyber-attacks. Consequently, there is heightened sensitivity around international trade (especially between blocs), which is increasingly associated with national security concerns. Other platform governments under the control of authoritarian leadership have made use of their administrative capacity to exert excessive data-driven influence over their citizens' lives. This has led to heightened awareness in Latvia, where initial steps are taken to mitigate the susceptibility of the system to any kind of abuse.

Insights about Latvia's digital strategy

The Platform Governments scenario highlights challenges and opportunities related to the development of an integrated digital information management system for government, with necessary safeguards both within the Latvian government and internationally. It raises the question of the role the Latvian government wants to play in the digital economy and society, and the choice of digital partners with which it should tighten connections. The scenario highlights the long-term implications of digital partnerships with other countries and the need for common value sets and democratic beliefs.

Conversely, a weak government information management system could elevate the risk of Latvia falling behind countries willing to take bolder measures. Investing in a more capable and integrated approach could allow Latvia to tailor and adapt policies according to its population's needs, better achieve economic innovation and citizen well-being, and strengthen the ties of Latvians with their country. For example, such a system could provide the Latvian government with detailed real-time knowledge about the capabilities, health, well-being, attitudes and behaviour of Latvian citizens and firms, allowing the government to create new and adaptive employment opportunities, foster and monitor skills uptake and react to the concerns of Latvians more strategically.

The scenario also underscores a number of significant risks linked to abuse of an integrated system. If a government with extremist tendencies or groups with criminal intent were to access the keys to a highly detailed and effective information management system, they could potentially abuse it in numerous ways. This could include targeting political opponents, advancing private economic interests or manipulating the beliefs and behaviour of citizens through targeted political advertising. As the scenario demonstrates, whichever government entity were to carry out extensive data gathering and analysis of citizens, would effectively control a substantial digital intelligence capability. Overall, Latvia must consider carefully the choice of data-driven capabilities it wants to build up, and evaluate how it can establish a leadership approach and the necessary systemic checks and balances, to ensure data insights are used for beneficial decision making for all.

Based on the Platform Governments scenario, policy makers in the digital field may wish to explore a range of strategic questions:

1. What checks and balances are built into current digital policies, and would they be sufficient to ensure trust, security and accountability if the state digital infrastructure were to grow considerably in scale?
2. Does a **country's geopolitical place in the world** present new challenges from a digital perspective and what decisions could be taken today to avert potential dilemmas?
3. Can **greater state involvement in the digital economy and freer markets** be reconciled, in order to deliver greater well-being for citizens?
4. What **kind of digital government** does our country want?

Corporate connectors

Summary

In this world of 2035, a small number of global technology companies function as one-stop shops for every aspect of life, from socialising to health monitoring, learning and consuming. Through their economic power and constant analysis of popular will, they have taken a more active role in global governance. Many public sector activities in fields such as infrastructure deployment, school curricula and security provision have been outsourced to these private companies.

Corporate connectors

- A small number of global technology companies function as one-stop shops for every aspect of life, from socialising to health monitoring, education and security.
- Trust in corporations is high and the main allegiance of most people is to a firm, not a government.
- Through their economic power and constant analysis of popular will, technology corporations have gained legitimacy to take a more active role in global governance.
- Many fields previously under the charge of governments, such as public infrastructure provision, school curricula or monetary policy, are now in the hands of corporations.

Individuals, referred to as citizen-consumers, have developed strong connections with large digital corporations, and the main allegiance of most people is to a firm, not a government. Government tax revenues have dwindled, and the number of public officials has more than halved over time. The general response has been to integrate private sector actors further in a range of policy fora. Lobbyists of technology companies stand openly as candidates in local and federal elections, and the United Nations General Assembly now includes delegations of major corporations.

Signals: Superstar firms, market concentration and fields of public interest

Strategic foresight uses signals of change observed in the present to point to plausible new trends or discontinuities that could emerge and grow, and result in a future scenario which differs from current expectations. The following signs of change are already visible and, if they continue to grow, could give rise to the scenario in the previous section.

Many firms today are significantly larger than the most productive firms decades ago, with a significant increase in industry concentration recorded in Europe and North America (Bajgar et al., 2019). Some globally operating "superstar" firms have a larger revenue than entire states and vast user bases, lending their actions and decisions a new global scale and significance. These winner-takes-most dynamics have increased the economic and political power of a handful of firms, particularly in the high-tech sector.

Network externalities and the scale of consumer and industry data has led to concentration among several markets. Corporations operating digital platforms collect granular user data on an aggregate level that allows them to build predictive models capable of determining consumer preferences and anticipating behaviour (OECD, 2018). Customer-centred business intelligence has not only evolved as a new mechanism for corporations to gain economic power, but has also given corporations insights into human preferences on an unprecedented scale.

Some of these powerful firms have begun to play a role in determining the priorities of policy institutions, for example in the field of migration. The technology sector relies strongly on migration to fulfil their skill needs. For instance, in Silicon Valley close to 60% of workers in STEM jobs with a bachelor's degree or higher are foreign born. Among software engineers, the share rises to 70% (Kerr et al., 2016). The ability to easily bring in foreign workers is an important factor for firms when selecting hub locations, with Canadian and American cities competing in the recent Amazon HQ2 tender process on the basis of ease of bringing foreign workers.

Furthermore, technology firms exert increasing influence over issues of public interest, for example in the education, health and housing sectors. Today, many schools and universities rely on cloud services proposed by Google or Microsoft. The former has developed a specific product, Google Classroom, which enables students and professors to exchange among virtually, as if in an actual classroom. In terms of health care, Alphabet, the parent company of Google, has invested significantly in the use of technology to better understand health, and also employs data generation, detection and positive lifestyle modifications to tackle disease, for example through the acquisition of Fitbit (CB Insights, 2019). Regarding smart city planning, large-scale corporate projects are on the rise. However, the remodelling of the Toronto waterfront into a "smart city" by a US company, with features like snow-melting roadways, an underground delivery system and a range of data-collecting sensors, has raised privacy concerns (Deschamps, 2019).

How this world came about

During the initial phase of consolidation, leading up to 2019, a race between technology corporations for market share among citizen-consumers and suppliers ensured a fair degree of competition. This kept prices low or even free for citizen-consumers and fees low for suppliers. However, as membership solidified and no new competitors emerged, all platforms began simultaneously to raise their prices and fees. There was no proof of collusion and unfounded allegations were quickly removed from social media sites. Some suspected that what might resemble co-ordinated action by platforms may simply be a product of rational optimisation advised by their respective business intelligence AIs. Productivity growth, while extremely high initially, started to slow, in part as a result of new innovators being acquired and subsumed by the platforms rather than being able to grow to scale.

The increasing influence of corporate connectors was accompanied by new responsibilities, but also with increasing capacity to make decisions on issues of public interest. For example, the challenges of social media echo chambers, censorship and free speech, and fake news were largely addressed by the platforms, with governments lacking the knowledge and means to remain involved. This trend led to the emergence of several online deliberation spaces which started to influence digital decision making. This new form of democracy, characterised by constant nuanced online engagement, enabled corporations to understand the evolving preferences of citizens better than ever before. However, the inability of platforms to get every decision right ensured that national democracy continued to represent local interests. Governments appointed tech ambassadors to lobby and represent the interests of their residents vis-à-vis corporations.

Digital corporations continued to pay very little corporation tax. Due to a lack of financial means, governments started outsourcing many of their functions to the corporate sector. Many quality-control regulations, for example on taxis and hotels, were replaced by rating systems based on sensors and checks imposed by the platforms that connect them with customers. Over the years, corporate connectors became involved in an increasing number of policy fields ranging from infrastructure to education, health and security. Due to the high quality of the services they provided, most citizen-consumers continued to be loyal and trusted them with data-driven insights into their daily decisions. Nonetheless, movements critical of increasing corporate influence persisted, but struggled to gain traction and reach a large audience as their messages frequently disappeared from social media channels.

By 2030, the idea of citizenship had taken on many new and different meanings. In addition to statehood, individuals developed increasingly close connections with large digital firms or online platforms that provide an extensive range of services and support in exchange for loyalty, personal data and fees for premium features. Eventually, this new form of digital citizenship became transnational, just like the firms that offer it.

What this world looks like

Under the **Corporate Connectors scenario**, Latvia's economy has become closely intertwined with large global corporations, driving a number of national, regional and local companies out of business. Many Latvian SMEs prospered initially by integrating into a corporate ecosystem in order to access new global markets, but now find their profits squeezed as the intermediary takes a larger share. While convenience for citizen-consumers rose due to a streamlined interface and internally co-ordinated services, this has required and resulted in substantive amounts of sensitive personal data being collected and controlled by corporations. These firms have leveraged their technological supremacy to offer much stronger cyber security for such data, rigorously safeguarding them from potential hacks or leaks. However, access to this information by governments or others for public benefit is highly limited. As a result, Latvia's government is subject to significant corporate influence, relegating it to a bystander position, and policy oversight has become much harder.

Global corporations have seized the opportunity resulting from government services increasingly lacking in precision and quality to replace them with their own, more tailored and convenient offers. As a result, many services previously provided by government such as infrastructure, health care or education are now at least partly in the hands of corporations. Due to the often high levels of citizen-consumer satisfaction, trust in corporations is high overall, but the needs of vulnerable and economically disadvantaged groups are often neglected. Latvia consequently faces a high level of inequality that the weakened government struggles to tackle effectively.

Insights about Latvia's digital strategy

The Corporate Connectors scenario highlights challenges and opportunities related to a growing presence of large global technology firms based outside the country, their deepening influence over Latvian citizens, businesses, public policy and society, and their further involvement in fields of public interest in Latvia. Potential risk associated with this scenario could heighten if Latvia were to become dependent on one or a small number of technology providers. Not only could such arrangements lock Latvians into certain technologies, it could also weaken Latvia's negotiating position when adapting systems at a later stage. In addition, close ties with a particular provider could affect the Latvian government's leverage concerning regulation and enforcement issues, both nationally and in a multilateral context.

More broadly speaking, the scenario underlines the need to identify policy levers nationally and multilaterally to ensure the potential influence of corporations over Latvia's economy and society is kept in check. This could require reinforced strategic international partnerships in fields such as competition and data policy, but also demand a systematic screening effort in national policy making. For example, it is possible to envisage a situation where all Latvian schools that use applications from a particular technology provider creating incentives to adopt the same ecosystem in other personal and professional contexts or even for administrative matters. Ultimately, this could create a path dependency making changes to Latvia's broader technology procurement strategy increasingly costly. Decisions in strategic fields such as education and data management could end up in the hands of a private corporation where profit-driven incentives may matter more than serving the needs of all citizens equally.

Conversely, Latvia may enjoy various benefits from collaborating with globally leading technology providers. Such agreements could allow the country to achieve faster roll-out of new technologies and services, simplify procurement systems within an established partnership and benefit from economies of scale when working with the same provider in various contexts. The scenario raises the question of which measures best ensure that democratically chosen objectives are respected and advanced within any private-public partnership. Overall, it amplifies the need to limit the influence that private actors can acquire over fields of public interest and determine the types of regulation that best ensure the protection of Latvian citizens and their diverse needs and interests.

Based on the Corporate Connectors scenario, policy makers in the digital field may wish to explore a range of strategic questions:

1. What **strategic partnerships and collective initiatives** would enable Latvia to exert maximum leverage in favour of public well-being in a world where firms outweigh states?
2. How can **competition between digital services** be promoted in order to make it easier for consumers to switch providers?
3. Should Latvia encourage or participate in initiatives to **rate and rank firms by quality of cyber-security**, and require such information to be provided as a "digital product label" to inform consumer choices?
4. **What kind of access** does Latvia want to give private corporations in **which policy fields**?

Strategic perspectives for Latvia to consider

The foresight process draws on the higher-level implications of Latvia's potential actions in each of the scenarios: How well would any option perform under various future contexts and can any "no regrets" option be identified? Which current beliefs and expectations built into policy making may be challenged by future disruptions?

The outlined options offer a complementary input to the specific and technical recommendations outlined in the following chapters of this report. They are meant to enrich Latvia's digital strategy with long-term, strategic thinking offering an additional lens to aid the prioritisation and selection of actions. Each of the actions identified may provide an opportunity to move closer to one of the desired future directions identified above (see section "Directions for a desirable digital Latvia"), while simultaneously strengthening Latvia's capacity to deal with potential future changes. Each of the following paragraphs will describe high-level implications for Latvia and list exemplary strategic options the government could consider in this context.

Latvia is a country with numerous strengths that can allow it to thrive in a digital future, but also faces certain challenges:

- Latvia's internal connections provide the ability to collaborate effectively across various policy and industry fields. Collaborations between policy makers and the research and academic field have potential for further development, particularly given the high quality of Latvian education.

- Latvia has various structures in place that allow for direct feedback loops between the government and the public. These channels have the capacity to generate valuable inputs for policy makers, but also pose challenges related to transforming these insights into evidence-based policy making and strengthening data-driven decision making.
- Latvians are keen to take up digital technologies and share high ambitions for their government overall, generally trusting in its ability to deliver on a digital strategy. At the same time, there may be room to share more responsibilities with other stakeholders within the country, for example by creating new enabling factors for the private sector or taking better advantage of those already present.
- Stakeholders have identified a risk that hasty regulation in the digital field may hamper innovation opportunities.
- Latvia has great potential to be an agile, adaptive and fast-moving country as a result of its well-connected, relatively small population. However, the country has limited opportunities to lead on international issues such as regulation of global corporations and must be able to respond strategically to changes outside its direct control.

Strengthen Latvia's internal and external partnerships for digital transformation

The scenario discussion in the previous section provided various concrete future contexts in which success depends on a whole-of-society approach to digital transformation in Latvia. This would require strengthening co-operation and effective collaboration across government, business and civil society organisations to advance key digital priorities. Such partnerships are necessary not only to leverage the data, insight and expertise held by different partners, but also to ensure an ongoing healthy diversity of power centres and checks and balances within Latvian society. In addition, the scenario discussion pointed to the strategic importance of networks and partnerships extending beyond Latvia's borders. Strengthening these partnerships will allow the government to leverage necessary regulation in fields where Latvia alone can only exert limited influence, such as data governance and competition policy. Partnerships can also help to keep the Latvian digital ecosystem (e.g. information management systems) connected and compatible with like-minded partners sharing a similar set of values.

Strategic data partnerships. The scenario discussion also emphasised the value of large-scale data analytics for making accurate, evidence-based decisions in various fields. All three scenarios highlight the political and economic influence that comes with access to insightful digital data (whether by communities, corporations or governments). For Latvia, this underscores the need to respect appropriate limits and safeguards in cases where various actors obtain access to sizeable data sets providing granular and insightful information on any given issue, according to the level of data sensitivity potential. This could include limiting the number of agencies with access to specific kinds of data. One particular perspective for action here is collaboration between academia and industry.

Accordingly, data partnerships are of crucial importance for stakeholders in the academic, business and development field. In order to reap the benefits of big data analytics, Latvian stakeholders must establish strategic systems that allow for compatible, value-based data collection, sharing and analysis. Options for action may include:

- co-operating with leading academic institutions abroad and other parties to collect a critical mass of data and improve data co-ordination
- ensuring compatibility between networks and data providers
- creating a platform for integrating and sharing government data with third parties such as civil society and corporations in a controlled and ethical way – taking into consideration, in particular, the value as well as the sensitivity of health data
- continuously strengthening a digital security and ethics checklist system for any government decision, for example in the field of public procurement
- formalising a strategy of collaboration between digital platforms of other countries in northern Europe
- establishing multi-stakeholder (involving academia, private sector, technological community, civil society, government) consultation procedures on the creation of regulations in order to avoid excessively rigid regulations.

Industry-university partnerships. There is potential for mutual benefit between higher education institutions and industry arising from developing and sharing digital knowledge and skills in innovative and impactful ways for Latvia's economy and society.

Ministry-university partnerships. Universities are a key potential partner in digital transformation, bringing a necessary complement of independence, objectivity, accountability, in-depth analysis and evidence to inform policy making, decision making and implementation on digital policy issues. Such partnerships can help establish necessary checks and balances to allow Latvia to plan for futures characterised by enhanced data-driven control by governmental or private sector actors, among others. The following actions could help develop and reinforce effective partnerships between universities and government:

- taking advantage of existing flexibility in policies such as procurement and other funding mechanisms to enable longer-term collaborations, so that partners in government, universities and institutes can invest in developing the necessary expertise and relationships – and identifying and addressing potential barriers
- encouraging universities to support policy making, for example through analysis of policy implementation
- facilitating staff rotation and exchange between universities, business and government, to help address gaps in expertise and longer-term perspectives in public service.

Language technologies. Recent successes with developing language tools, such as machine translation and the technologies that support them, could hold potential for Latvia to further specialise in a field with multiple future opportunities in the civic, public and private sectors.

Rail Baltica project partnerships. The Rail Baltica project is a major cross-border partnership offering digital opportunities for Latvia, among others. Given the project's innovative nature and technology-driven planning (e.g. regarding the cloud-based Common Data Environment), Rail Baltica offers opportunities to strengthen ties with neighbours on digital matters and further integrate Latvia's digital ecosystem. The project can also serve as a stress-test for Latvia's capacity to engage with various stakeholders, ensure digital safeguards and streamline public-private partnerships. Potential avenues for further development include:

- engaging with communities on opportunities offered by the opening of a new high-tech high-speed railway station
- reviewing in advance opportunities and risks related to opening up the technology and offering procurement contracts to private firms.

Project funding alliances. Government needs to lead and further co-ordinate and consolidate the funding efforts of firms, communities and academia in fields such as large-scale digital infrastructure (e.g. transportation or 5G projects) and ICT research and development. This would enable better alignment of expectations and the creation of synergies among different stakeholders and strengthen their position when negotiating with international partners. Actions to consider include:

- partnering with digital finance and Fintech experts to set up open source co-ordination systems aligning funding partners on the basis of shared objectives and key performance indicators, and providing access to civil society and community partners
- connecting funding alliances to international partners, for example at the EU level
- using alliances to foster knowledge exchange between private sector, civil society and academic actors.

Identify smart approaches to education and skills for adaptive, critical Latvians

A digitally empowered public can serve as an important source of digital innovation, entrepreneurship and productivity. A digitally capable citizenry can also help hold governments, corporations and other organisations to account for their digital policy choices, and enable society to navigate the many challenging trade-offs related to digital transformation, such as the automation of work and the collection and use of personal data. In addition, the strategic foresight process highlighted the point that in a digital, complex and fast-changing world, there is an increasing need not only for "digital skills" such as data visualisation or manipulating AI, but also skills like creativity, problem-solving, adaptability and critical thinking.

Applied learning programmes for students. To be prepared for a complex and fast-changing digital world, young Latvians must not only acquire theoretical ICT skills, but also learn in practical ways about the benefits and – just as importantly – any potential dangers that digital transformation can engender. From this perspective, practical collaborations between the formal education sector and firms, research institutions and communities based in Latvia could be beneficial, and could take various forms, for example:

- establishing long-term partnerships between Latvian schools and companies to offer practical learning opportunities and strengthen ties between Latvian talent and local employers
- offering case-study programmes, innovation labs or hackathons in schools in collaboration with Latvian private sector partners, thereby allowing students to tackle real challenges facing Latvian companies and apply their theoretical knowledge in a practical manner, thus preparing the next generation for potential future challenges of the digital transformation, fostering their innovation capacity and strengthening the links of Latvian companies with young talent to ensure local SMEs and established companies have access to suitable staff in a context of fierce international competition
- making use of these partnerships to ensure a faster feedback loop between practitioners and educators in order to adapt Latvians' skills and school curricula continually in accordance with future needs, and better leveraging existing capacity within firms through connections with academic or community partners.

Human capital investments. Human capital is a well-known driver of economic growth and innovation, and the information-driven digital economy has further accentuated this dynamic. In order to harness the potential of an economy heavily reliant on human resources, Latvia must ensure continued flows of investment into its biggest asset – its employees. To support continuous learning even after the end of formal education, Latvia could explores ways to incentivise firms to invest in their employees. These could include:

- rolling out (further) programmes for employer-sponsored continuous vocational training (i.e. provided or paid for at least in part by firms)
- introducing new incentives and funding (i.e. firm-level incentives) for specific company-led learning and training programmes in the ICT field
- systematically assessing the policy environment for Latvians working in the gig economy, including potentially an assessment of the adequacy of Latvian labour policies, insurance schemes and work contract formats for gig economy workers.

Digital learning hubs. The scenario discussion – especially the #Me2.0 scenario – highlighted the potential of community-driven digital innovation. Granting Latvians across the country better access to open source tools and learning opportunities to become digitally savvy would give them a greater stake in the country's digital development. In this context, the workshop pointed to the option to further develop Latvian digital learning hubs that connect with existing infrastructure such as regional libraries and education institutions – potentially building on the success of the DigiHubs network.[2] This would enable training opportunities to be offered across Latvia in urban and rural areas alike, and could serve as an accelerator for digital transformation. It would also enhance digital skills among all age groups and respond better to diverse needs across the country. E-learning platforms (including technical infrastructure and learning content) should be developed, in order to increase opportunities for distance learning and e-learning.

Identify pathways to an inclusive digital Latvia for and by the people

The scenarios highlight both sides of digital transformation – the opportunities technology creates for people to voice their opinion and become active, as well as the potential threats of technology to equality, inclusion and individual control over their data and lives. Deliberate efforts can help to maintain citizen trust and provide Latvians with new means to voice their needs and opinions and fulfil their own digital aspirations. These efforts can leverage economic and social innovation stemming from all regions, sectors and institutions of Latvia.

Social impact funding and crowdfunding. Potential opportunities to foster inclusive economic development can be envisaged in a few ways:

- providing open source tools to help funders track their progress towards achieving key social performance indicators
- helping citizens, communities and businesses track the progress of funded projects and contribute to achieving them
- developing new crowdfunding tools in collaboration with community leaders, for example through reward systems or gaming approaches.

Secondary data use legislation. Further attention may be need to be paid to the secondary use of data and anonymity, particularly in relation to the sale of medical data to third parties and countries. Potential measures include:

- defining private data as a good with quantifiable economic value that takes into account costs in terms of individuals' privacy and rights, thus helping to inform decisions regarding which services merit what volume of data.
- developing and adopting a transparent ethics framework to guide data legislation.

Corporate trust measures. Trust in corporations could be measured in a similar manner to trust in government, providing useful insights for Latvia's approach to public-private partnerships.

Participatory decision making. In future contexts where data-driven insights become increasingly powerful, decision-making structures must build in the necessary feedback loops and accountability measures to avoid misuse. One way to develop systematic checks and balances could be to foster a leadership approach that allows more room for all parts of an organisation to voice their opinion and question decisions. Research has shown that participatory decision making contributes to more robust decisions and strategies. This approach could be initiated through a training series on participatory decision making for managers from diverse sectors, by offering simulation games on collective decision making in schools, by testing new tools for public consultations (e.g. in collaboration with media partners) or by offering leadership coaching for entrepreneurs.

Strengthen the capacity to access and use personal data, while safeguarding digital security and safety

The scenarios suggest that Latvia's government might wish to review its system for accessing, integrating and analysing digital information in the future. In a more digital world, creating value for citizens will depend partly on the ability of organisations to access and draw insights from rapidly growing quantities of personal data. At the same time, a more integrated and effective government information system also creates profound risks, which must be mitigated with strong safeguards. The same information that is critical for improving services by monitoring and influencing outcomes also provides significant potential for misuse. Latvia, like most countries, is faced with the challenge of advancing two priorities simultaneously: strengthening the effectiveness of the government's digital information system, while at the same time increasing safeguards. A person-centric principle applies in this context: when a person is the source of data, that person has the right to determine when and where that data is used.

Task force on risks of integrated digital information system. An interdisciplinary task force could explore a broad range of current and potential future risks related to building a stronger and more integrated digital information system. This would include:

- considering situations related to both cybersecurity and the potential abuse of the system by users who gain access both illegally and legally
- developing mitigation solutions in collaboration with key stakeholders that would feed into integrated data safeguarding solutions.

Integrated data safeguarding solutions. The scenario discussion re-emphasised the importance of a consolidated, ongoing, adaptive approach to existing and future safeguarding measures. A nationally co-ordinated digital security strategy could include efforts at the technological, institutional, political and cultural level:

- Technological solutions could integrate mechanisms to separate data and store them in multiple locations, mechanisms to control and track access to information, mechanisms to extract only the minimum data required for a given need, and others.

- Institutional solutions could incorporate rigorous and transparent monitoring and auditing of all data use by both internal and external watchdog functions.
- Political solutions could include partnerships with other governments to mutually audit each other's national safeguards.
- Cultural solutions could involve a high degree of awareness among citizens of the risks and signs of abuse, such that the population will not tolerate moves to weaken or remove safeguards.

ICT provision expertise. Latvia could improve the overall quality and interoperability of services it provides by enhancing the skillset and knowledge of officials. This could include identifying new incentives to recruit ICT experts and practitioners, for example on the basis of staff rotations with Latvian companies.

Conclusion

This chapter explored three alternative scenarios for the future of digital transformation and some of the initial implications for Latvia's digital strategy. The chapter is intended as both a complement to the recommendations in the broader report and as a starting point for further analysis and deliberation in Latvia as part of the ongoing process of developing (and redeveloping) resilient, adaptive and successful strategies.

As both this chapter and the broader report demonstrate, Latvia possesses many of the attributes needed to thrive in the digital era. In a context of rapid change and high uncertainty, however, continued success means advancing beyond what was previously considered satisfactory and investing in new practices and capabilities. Core among the requirements for good governance in the 21st century is the capacity to engage systematically with future uncertainties by mainstreaming strategic foresight approaches in government policy making. The OECD encourages government officials and the broader policy community in Latvia to build upon their foresight experience in the Going Digital exercise, in order to continue their forward-looking work both within the digital policy sphere and beyond.

References

Bajgar, M., et al. (2019), "Industry concentration in Europe and North America", *OECD Productivity Working Papers*, No. 18, OECD Publishing, Paris, *https://doi.org/10.1787/2ff98246-en*.

BBC News (2019), "Russia internet: Law introducing new controls comes into force", *www.bbc.com/news/world-europe-50259597*.

Casalini, F. and J. López González (2019), "Trade and cross-border data flows", *OECD Trade Policy Papers*, No. 220, OECD Publishing, Paris, *https://doi.org/10.1787/b2023a47-en*.

CB Insights (2019), "How Google plans to use AI to reinvent the $3 trillion US healthcare industry", *www.cbinsights.com/research/report/google-strategy-healthcare*.

Deschamps, T. (2019), "Google sister company releases details for controversial Toronto project", The Guardian, *www.theguardian.com/world/2019/jun/24/google-toronto-smart-city-sidewalk-project-alphabet-redevelopment*.

Guarascio, F. (2019), "Alarmed by Libra, EU to look into issuing public digital currency: draft", Reuters, *www.reuters.com/article/us-eu-cryptocurrency-regulations/alarmed-by-libra-eu-to-look-into-issuing-public-digital-currency-draft-idUSKBN1XF1VC*.

Hesse, C. (2008), "Mapping the new commons", paper presented at "Governing Shared Resources: Connecting Local Experience to Global Challenges", the 12th Biennial Conference of the International Association for the Study of the Commons, University of Gloucestershire, Cheltenham, United Kingdom, 14-18 July, *http://dlc.dlib.indiana.edu/dlc/bitstream/handle/10535/304/Mapping_the_NewCommons.pdf*.

Kerr, S.P. et al. (2016), "Global talent flows", *Harvard Business School Working Papers*, No. 17-026, *www.hbs.edu/faculty/Publication%20Files/17-026_a60ac33d-3fd5-4814-a845-137a38066810.pdf*.

KPMG (2017), *Overview of China's Cybersecurity Law*, 2017 KPMG Advisory (China), *https://assets.kpmg/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf*.

Matias, J.N. (2015), "The tragedy of the digital commons", *The Atlantic*, *www.theatlantic.com/technology/archive/2015/06/the-tragedy-of-the-digital-commons/395129*.

Mölleryd, B. (2015), "Development of high-speed networks and the role of municipal networks", *OECD Science, Technology and Industry Policy Papers*, No. 26, OECD Publishing, Paris, *https://doi.org/10.1787/5jrqdl7rvns3-en*.

Nvidia (2020), "Driving innovation", *www.nvidia.com/en-us/self-driving-cars*.

OECD (2018), "Market concentration", issues paper, OECD, Paris, *https://one.oecd.org/document/DAF/COMP/WD(2018)46/en/pdf*.

Shi-Kupfer, K. and M. Ohlberg (2019), "China's digital rise", *MERICS Papers on China*, No. 7, *https://merics.org/en/report/chinas-digital-rise*.

Walljasper, J. (2011), "Elinor Ostrom's 8 principles for managing a commons", *On the Commons*, *www.onthecommons.org/magazine/elinor-ostroms-8-principles-managing-commmons*.

Notes

[1] Available at: *https://uidai.gov.in*.

[2] Available at: *https://latlit.eu*.

From:

Going Digital in Latvia

Access the complete publication at:

https://doi.org/10.1787/8eec1828-en

Please cite this chapter as:

OECD (2021), “Key future uncertainties in digital transformation and potential implications for Latvia”, in *Going Digital in Latvia*, OECD Publishing, Paris.

DOI: https://doi.org/10.1787/fa7178b3-en

This work is published under the responsibility of the Secretary-General of the OECD. The opinions expressed and arguments employed herein do not necessarily reflect the official views of OECD member countries.

This document, as well as any data and map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area. Extracts from publications may be subject to additional disclaimers, which are set out in the complete version of the publication, available at the link provided.