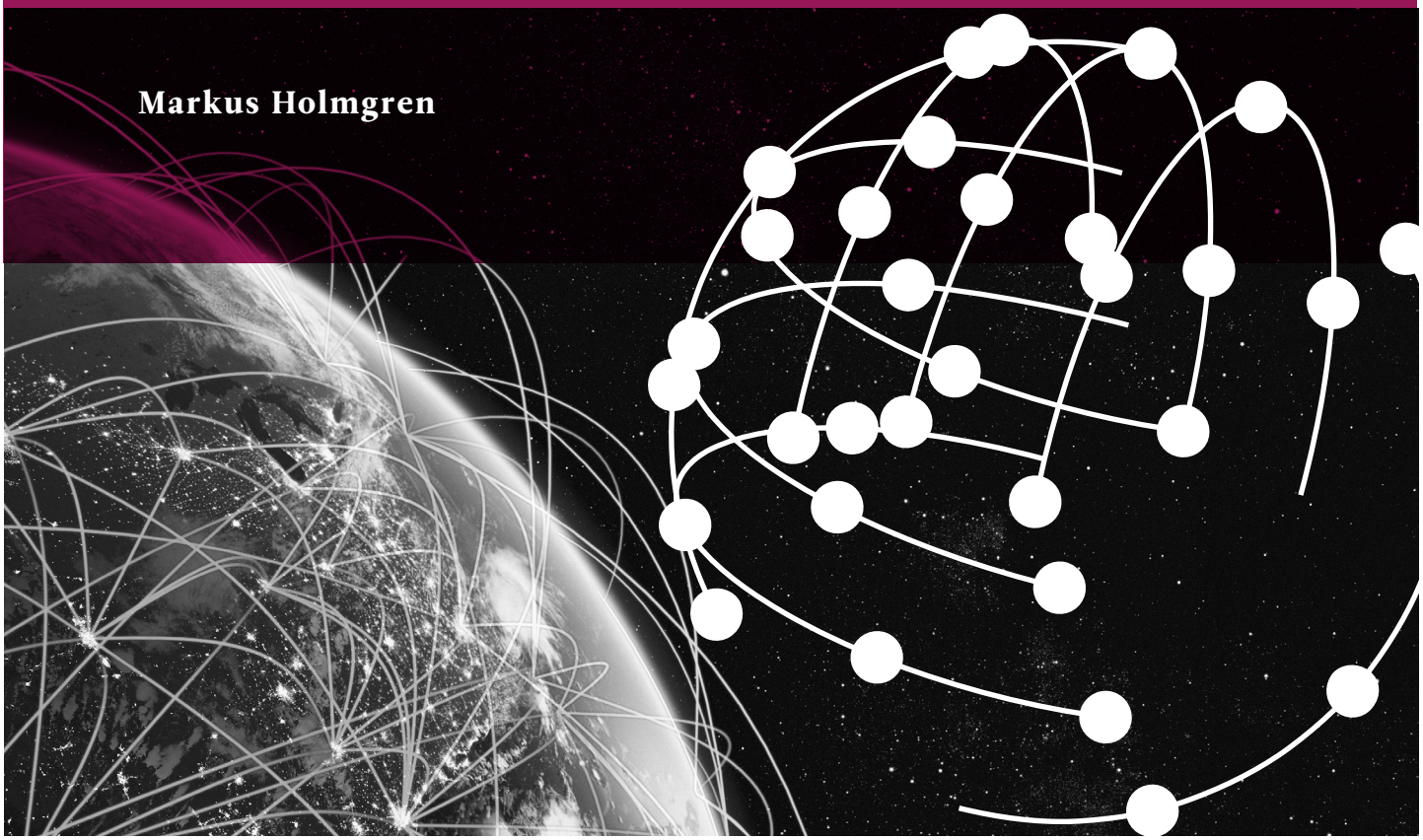
FIIA
BRIEFING PAPER
GEOECONOMICS SERIES

NOVEMBER 2022
/352

DIGITAL RESILIENCE BEYOND DATA LOCALISATION

NATIONAL APPROACHES TO GLOBAL CHALLENGES

Markus Holmgren



FIIA
FINNISH
INSTITUTE
OF INTERNATIONAL
AFFAIRS

DIGITAL RESILIENCE BEYOND DATA LOCALISATION

NATIONAL APPROACHES TO GLOBAL CHALLENGES

- Data localisation refers to the technologies and policies aimed at ensuring localised data hosting and localised data routing instead of utilising offshore server and processing centres.
- Data localisation is often suggested as a solution to global challenges stemming from the increasing dependence of societies on data and digital technologies, as well as the fear of an external actor leveraging this dependence for power political purposes. Data localisation does not, however, reduce key technological dependencies.
- The goal of digital resilience should be to ensure the security and continuity of data and infrastructure software, and to secure access to critical digital services irrespective of their location. Instead of data localisation measures, international cooperation should be deepened and digital traffic should have overseeing systems similar to those that have been in place for land, air, and maritime traffic for decades.
- EU member states would benefit greatly from the creation of a unified auditing and standardisation process within the European single market. At the same time, tighter ties with US digital service providers would improve digital resilience.

MARKUS HOLMGREN
Research Fellow
Global security
Finnish Institute of International Affairs

ISBN 978- 951-769-746-0
ISSN 1795-8059
Language editing: Lynn Nikkanen
Graphics: Otso Teperi
Cover photo: Ikon images / Lehtikuva

This FIIA Briefing Paper has been prepared as part of FIIA's co-operation with the National Emergency Supply Agency (NESA).

FIIA FINNISH INSTITUTE OF INTERNATIONAL AFFAIRS
Arkadiankatu 23 b
POB 425 / 00101 Helsinki
Telephone +358 (0)9 432 7000
Fax +358 (0)9 432 7799
www.fiia.fi

DIGITAL RESILIENCE BEYOND DATA LOCALISATION

NATIONAL APPROACHES TO GLOBAL CHALLENGES

INTRODUCTION

During the past decade, data localisation has become a buzzword that is offered as an easy solution to the many challenges created by the increasing yet uneven accessibility of data. In the foreseeable future, societies will be increasingly dependent on data in its many forms, which has led to fears of an external actor leveraging this dependence for power political purposes. However, data localisation is applicable to very few challenges, which is why it is crucial to carefully consider which problems can be solved with localisation and which are better addressed by other means.

Data localisation refers to attempts to keep data within a specified jurisdiction. More precisely, it refers to the technological, administrative, regulatory, and policy processes that aim at localised data hosting and routing. In a technological sense, data refers to the characters, quantities, and symbols on which computer operations are performed. The formulation of data to be localised varies from basic personalised (identifiable) data (e.g., registration and search history data) to photos, videos and written texts that could be connected to a user.

Data localisation does not technically include software but does in practice often require sizeable investments in it. The same is true of digital infrastructure, supply chain management and international regulation critical for data management, which goes to show how complicated the process of data localisation is. It is also expensive and difficult to achieve, especially without antagonising service providers and their host countries. For these reasons, data localisation is seldom a practicable approach to improving digital resilience.

Digital resilience includes the preparatory actions for securing the continuation of vital digital functions and critical digital infrastructure of a state. Being resilient means having the physical, legislative, and intellectual capability to adapt rapidly and effectively in the face of adversity or disruption.[1]

This Briefing Paper discusses data localisation and its role in national attempts at improving digital resilience. The paper proceeds with a brief look at various national approaches to data localisation. It then continues by briefly analysing four challenges to which data localisation is sometimes offered as a solution and presents alternative approaches that would be better suited to them. Finally, the paper provides policy recommendations for EU member states on how to improve their digital resilience. The key message of the paper is that data localisation is inefficient at building digital resilience. Instead, states should make sure that whoever handles data does so responsibly irrespective of whether the data is produced or handled in or out of jurisdiction.

DATA LOCALISATION AROUND THE WORLD

National responses to the perceived challenges created by the increasing yet uneven accessibility of data differ around the world. This paper discusses how different states and actors have approached data localisation. Figure 1 provides examples of the kinds of restrictions that are in place in Australia, Canada, China, the European Union, India, Russia, the United States and Vietnam. Each approach comes with different challenges, but they are all, at least in part, backed by a narrative arguing that they improve digital resilience and the ensuing digital sovereignty.

China and Russia have decreed that data concerning their citizens, legal persons and public institutions has to be stored on servers that are physically located in-country. The Chinese and Russian approaches are variations of so-called unconditional data localisation (Figure 2). Its main challenge is that it requires large internal markets so that 1) foreign corporations abide by the rules instead of abandoning the market, 2) there is domestic capability to pick up the market slack in case foreign providers bolt, and 3) the state has resources to track and enforce these policies.[2] For

1 See Fjäder, Christian (2014) 'The nation-state, national security and resilience in the age of globalisation', *Resilience*, 2:2, 114-129. See also Walker, Brian (2020) 'Resilience: what it is and is not', *Ecology and Society* 25(2):11.

2 See Pernot-Leplay, Emmanuel (2020) 'China's Approach on Data Privacy Law: A Third Way between the U.S. and the EU?' *Penn State Journal of Law & International Affairs* V.8(1). See also InCountry (2022) *Data Protection Laws in China – Ways to Stay Compliant with Cloud Data*; Hernández, Simón and Akhil Raina (2020) 'Legal Problems with Data Localization Requirements: The Case of the Russian Federation', *Global Trade and Customs Journal*, Issue V15(9), pp. 445-459; InCountry (2021) *Russian Data Protection Laws: Essential Guide on Compliance Requirements in Russia.*

Examples of data localisation measures of selected countries

Jurisdiction	Examples of restrictions
Australia	Unconditional restriction concerning personal health data. Restrictions on transfers to a list of countries.
Canada	Barriers to internet services for jurisdictions failing to meet set standards.
China	Unconditional in all sectors. All data concerning Chinese people, organisations and infrastructure. Web filtering and blocking. Encryption restrictions. Source code disclosure.
European Union	Conditional transfer restrictions concerning personifiable data. Cross-border contract rules.
India	Local storage requirement. Encryption restrictions.
Russia	Unconditional restriction concerning data related or connectable to Russian citizens.
United States	Unconditional restriction concerning critical data related to national security interests.
Vietnam	Local storage requirement. Web filtering and blocking.

Figure 1. Examples of data localisation measures of selected countries.
Source: Author's complication, based on national and EU legislation, regulations, court rulings, and selected international agreements.

these reasons, the approach suits China (whose digital markets are gigantic) better than Russia (whose digital markets are not), while posing economic challenges to both (through diminished access to information, capital, and supplies). In addition, following such draconian regulations to the letter is practically impossible if international data transfers are to be allowed at all. As such, their data localisation measures should be seen at least partially as tools for selective law enforcement to encourage government friendly behaviour.

India and Vietnam also require digital service providers to store data locally but have less strict criteria for this. In the Indian and Vietnamese approaches, also variations of unconditional data localisation, the main challenge is that complying with the legislation causes duplication of data.[3] Duplication secures local access to data but creates additional vulnerabilities from a cybersecurity point of view. Corporations have fewer incentives to protect duplicated data in facilities developed solely for compliance reasons, while a greater surface area also means a greater attack surface.

In the European Union, member states have grown wary of harmful market practices and of the way that states and corporations gather, store and analyse foreign data. To address these concerns, the EU requires data service providers to keep track of the data they gather on EU residents and to maintain the ability to remove it on request.[4] As such, it is not so much about data localisation as it is about assigning responsibility for data-storing practices and infrastructure software. A good example of this is that digital platforms are now required to disclose which cookies they are using and to ask for the user's permission. Yet this ruling is also an example of the kinds of problems that may arise from the EU's approach: making a legally binding agreement with a single click sets a dangerous precedent.

Another inherent challenge of the European approach is that following all the rules is expensive. In order to understand what kind of operational and technical updates are required for compliance, companies, organisations, and individuals often have to hire a specialised solicitor, and sometimes following all the rules is simply impossible (e.g., in the case of companies operating both in China and in the EU). Despite the allotted abatements, the requirements occasionally prove burdensome for small and medium-sized companies, especially when followed responsibly. As a result, the European single market relies on its attractiveness as a leverage to prevent harmful service prioritisations. The European approach could be categorised as de minimis, but has strong elements from each category in Figure 2.

Estonia stores most of its critical data in servers outside the country's borders. The Estonian approach diverges from the EU-led one and is in many respects the opposite of data localisation. Most governmental functions have been digitised, while servers and processing capabilities have been dispersed between various international data centres and service providers. At the core of the Estonian approach is a decentralised data-sharing network called X-Road, which enables

3 See Bailey, Rishab and Smriti Pasheera (2018) *Data localisation in India: Questioning the means and ends*. National Institute of Public Finance and Policy. New Delhi. See also Manh Hung Tran (2021) *Data localization requirements in Vietnam*. Baker McKenzie. Chicago.

4 See European Union (2016) *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC*; European Commission (2022) *NIS Directive. European Commission.* https://digital-strategy.ec.europa.eu/en/policies/nis-directive.

Approaches to data localisation

Unconditional data localisation	Ban on international data transfer for all data to all jurisdictions
Sectoral data localisation	Ban on data transfer for some data to all jurisdictions
De minimis data localisation	Ban on data transfers to jurisdictions failing to meet set minimal standards
Controlled localisation	Limited regulation with clauses

Figure 2. Categorising approaches to data localisation.
Source: Author's compilation, based on national and EU legislation, regulations, court rulings, and selected international agreements.

secured access to the management of data and tracks accessing history.[5] As a dispersed architecture with a centralised management system, X-Road partially resolves many, but not all, vulnerability concerns, but does not, for example, help with securing access to global data streams, and nor is it the most efficient way to deal with secrecy challenges.

Each of these approaches can be seen as trying to deal with challenges arising from the growing sense of importance placed on data and digital technologies, and the fear of an external actor leveraging this dependence for power political purposes. These concerns and fears are reflected in spurts of increased spending on cybersecurity, digital innovation, and digital resilience following revelations about the misuse of digital power.[6]

The US approach differs from others for the seemingly simple reason that US institutions and corporations have had a massive first-mover advantage in projecting power through digital architecture. The US openly criticises regulatory involvement in digital markets. Instead, the US prefers unofficially guided private self-regulation, while also threatening to cut the market access of non-compliant corporations. It also provides funding for domestic server construction and increasing data-handling capabilities.[7] While the aim in part is to prevent (primarily Chinese) industrial espionage, the US approach also aims to maximise the pool of available data. Thus, the US approach does not so much aim at keeping domestic data in as at making data visit domestic servers and through that maximising strategic leverage.

DATA LOCALISATION AS A SUPPOSED SOLUTION TO FOUR GLOBAL CHALLENGES

It is possible to identify at least four challenges arising from unequal access to data, and to which data localisation is often offered as a solution. They relate to: 1) national law enforcement, 2) cybersecurity and digital privacy, 3) supply chain security, and 4) the development of the digital sector. However, data localisation seldom provides a solution to these.

Data localisation as a national law enforcement solution

Policymakers sometimes wish that data localisation would increase national law enforcement capability. Countries may seek to prevent others from seeing how they use private data, and to ensure that data stored on a foreign shore does not become inaccessible for authorities, for example when relevant to a criminal investigation if organisations outside their control fail or decide to stop servicing them.

Localising data within a jurisdiction may secure access to a diminished pool of data, but it will not protect the jurisdiction from foreign corporations deciding to stop servicing the jurisdiction or critical local operators. Nor will it promote efficient handling of data

5 See Hübner, Risto (2021) *The Privacy, Data Protection and Cybersecurity Law Review: Estonia. The Law Reviews.* Law Business Research. London.

6 Segal, Adam (2016) The Hacked World Order: *How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age.* New York: Public Affairs.

7 See Birnak, Michael D. and Niva Elkin-Koren (2003) 'The Invisible Handshake: The Reemergence of the State in the Digital Environment'. *Tel Aviv University Law Faculty Papers.* Working Paper 54. See also Farrell, Henry (2005) *Regulating Information Flows: States, Private Actors and E-Commerce.* Esp. pp. 15–31.

without separate requirements, which could be applied anyway in the absence of data localisation measures.

What data localisation does do is increase public and private surveillance capabilities,[8] especially if data is used in a way that most other actors and/or international law find unacceptable. For example, if a governing regime engages in repressing political opposition, pressuring court officials, embezzling public funds, or engaging in human rights violations, the ability to hide information and utilise data in isolation will make data localisation appealing for the regime, even if those same measures will harm local digital markets, businesses, and resilience. By contrast, democratic regimes will be more likely to alleviate digital law enforcement concerns by crafting cooperation agreements, regulating international data traffic, and ensuring that actors assigned responsibility over data follow agreements and regulations, and deliver on their commitments even when situations change.

Partial limitations are also often more efficient than sweeping bans. Australia and Canada, for example, limit the transfer of individual data to countries with inadequate data protection and privacy standards.[9] In these cases, data is effectively localised within a cooperative sphere of influence / market regime rather than within a jurisdiction, which is not technically speaking data localisation. The approach allows for the creation of larger markets than any single country could muster and encourages countries to adopt responsible rather than repressive data-handling regimes.

Such rules-based cooperation should be encouraged. Many law enforcement situations, such as criminal investigations related to organised crime, money laundering, tax evasion, and terrorism, benefit significantly from international cooperation. In addition, intelligence-sharing between allies, cooperative rescue services, and international research and analysis programmes are increasingly common because they are effective.

8 Chander, Anupamand Uyên Lê (2015) Data Nationalism. *Emory Law Journal* V64: 3, p. 680.

9 Office of the Privacy Commissioner of Canada (2020) Appendix 3: Cross-border Data Flows and Transfers for Processing – Jurisdictional Analysis. https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2021/tbdf_app3/.

Data localisation as a cybersecurity and digital privacy solution

A common concern is that critical data would fall into the wrong (foreign) hands or get deleted either as a result of a malicious act or unintended disasters. While this threat is real, data localisation is rarely a fitting solution.[10]

From a digital resilience perspective, unintended disasters and malicious acts entail systematic differences. When it comes to unintended disasters like natural disasters or human error, the concern is that critical foreign digital service providers can make service prioritisations and cut countries or organisations out of their service network. While forcing a company to build up local capacities might, when successful, make them more hesitant to stop serving the locality, the same result can be achieved with service agreements and international regulation.

Risks arising from malicious acts can be divided into small-scale and large-scale threats. Small-scale threats, like unorganised cyber criminals, rarely involve spies, bribes, or contaminating components in earlier phases of the supply chain. In other words, their operations typically require systems that are connected to the internet. Thus, localising data in an intranet can increase cybersecurity even if the network security is not vigorously updated, as it would have to be against large-scale threats like large criminal organisations and intelligence services.

Maintaining a secure system is difficult and expensive even if it is air-gapped (not connected to the internet) because every update will need to be tailor-made and constantly tested. It is thus only viable for the most important functions. More systems, devices, and programs mean more opportunities for incursion. Smaller is often better in such cases. This also applies to closed systems, meaning those that keep their source code secret and do not utilise systems whose code has been published somewhere. When done well, closed systems are much more expensive to develop than those consisting of ready-made building blocks (of code), but also more secure.

Data localisation does not, however, refer to building such air-gapped systems unless they encompass the whole jurisdiction. Such a system would be technologically easy to create, but bad for the country. For example, North Korea for the most part operates within a closed digital system called Kwangmyong,

10 See e.g. Frazer, Erica (2016) Data localisation and the Balkanisation of the Internet. *A Journal of Law, Technology, & Society* V13(3).

and access to the global internet is limited to a few individuals. While the regime's control over which data remains inside the country is unparalleled, and they have an advanced cyberespionage cohort, North Korea's digital economy is miniscule, its cybersecurity weak, and its privacy protection non-existent.

A single country cannot produce all the services that it requires to succeed. At the same time, the physical location itself has only limited security implications. In addition, preventing citizens from using foreign services does nothing to protect their liberties from threats coming from inside the system. A more sustainable solution is to approach cybersecurity and privacy challenges case by case, and favour air-gapped and closed systems when and where needed.

Data localisation as a supply chain security solution

Data localisation is sometimes offered as a solution to supply chain security challenges like offshore bottlenecks or lack of control over suppliers. Data localisation as a supply chain security measure refers to the processes required for reshoring critical sections of supply chains for critical digital products. An extreme form of this is called digital autarky.

For practically all digital products, reshoring the whole supply chain is difficult or nearly impossible. Not only do natural resource deposits disrespect national borders, but the supply chains are often thousands of steps long and many of the sub-products (such as industrial chemicals, specialised valves, measurement tools, and software designs) are 1) only produced by one or two companies, 2) treated as corporate secrets, or 3) protected by patents. Thus, reshoring them would require purchasing patents and whole chains of companies, and reshoring them too.

From a supplier's perspective, diversifying supply chains and keeping track of alternative options is key. Those alternative suppliers are often located overseas, and data concerning them is also located on offshore servers. Therefore, limiting the international flow of data limits the supplier's capability to diversify and thus build resilience, especially if unconditional data localisation becomes a commonplace practice. A more sustainable approach relies on and enforces the creation of free and open international markets and agreements.

Data localisation as a digital sector development solution

One concern to which data localisation is sometimes offered as a solution is the perceived lack of domestic digital innovations and competitive corporations.

The hope is that digital service providers (Microsoft, Google, App Store, Dropbox, etc.) would set up local data handling capabilities, and thus bring expertise and jobs to the country. Unfortunately, this is unlikely since data server farms require few employees. To make matters worse, localising data inside a jurisdiction comes with the inbuilt downside of limiting people's and businesses access to information, thus limiting their purchase and investment options outside the said jurisdiction. The challenges are compounded if the approach pushes for the use of outdated solutions that degrade efficiency, which would make new innovations likely to be based on outdated solutions as well.

Data localisation becomes particularly problematic if it develops into a globally utilised approach. People and companies are already using different internet services depending on region and language, and if data localisation becomes more common, it will lead to further balkanisation of the internet. Due to increasing security and illicit market practice concerns, fragmentation is likely to deepen the digital divide between US and Chinese hubs of refined data and data utilisation capability.[11]

While the division into separate digital service bubbles will likely slow down global growth, it will be even worse for individual countries to be left out altogether. Innovation should be encouraged, and new producers supported in the digital sector as well, but suppressing alternatives is rarely an efficient approach. Fair and open markets are naturally resilient, but difficult to create and maintain. The bigger the market, the bigger the scaling benefits, but only insofar as participating countries commit to common rules that keep the market open and free from harmful monopolistic practices and illicit competition.

CONCLUSIONS: POLICY RECOMMENDATIONS FOR EU MEMBER STATES

As a widespread solution, data localisation risks further balkanisation of the internet, thus limiting pooling benefits and replacing a system defined by competition with a system defined by confrontation. However, in the face of harmful and illicit data management practices, expertly created international minimum standards offer an alternative to data localisation.

The European Union has taken a firm lead in developing functional regulation for international data flows and markets. The aim is to create a level playing field in the form of free and open markets. Balancing between security and innovation promotion while leaving room for profit margins is a complicated but important task that will not succeed without commitment.

Individually, EU member states are too small to provide their own critical digital services or to generate the required expertise for adequate digital resilience. Larger reliable markets are more resilient because scale allows diversity. For this reason, EU member states should deepen their commitment to the European single market with increasing monetary and expertise commitments. The most important step would be to ensure that the European single market extends to data-intensive tech sectors also in practice. A common European auditing process is a requirement for the European market to become an attractive alternative to the US market in the high-tech sector. Similarly, technical standards should be unified within the European single market.

EU member states should support the European approach of assigning responsibility over data also within their own jurisdictions. To this end, they should create an overseeing authority for digital traffic security similar to the one they have in place for land, air, and maritime traffic.

At the same time, it is not realistic to expect European markets to be able to provide all the required services. Instead of data localisation measures, more viable options include promoting closer relations with US digital service providers, as well as crafting international legislation that prevents harmful service prioritisations and facilitates trust-building between countries and businesses.

While operators should be held responsible for the security of their digital solutions, it is important to keep in mind that the costs cannot merely be placed on the private sector's shoulders for the simple reason that failing businesses are not resilient. On the contrary, keeping systems secure is difficult and expensive as it requires constant upkeep.

It is also important to recognise that while digital resilience must ultimately rely on fair and open markets, some critical data should be handled only in closed systems and some digital and supporting services have to remain in national hands.

National approaches to digital resilience arise from different situations and the need to respond to individual challenges. While lessons can be learnt, solutions cannot be copied, as circumstances differ. Countries and institutions must adjust to their environment and find their own best approaches to digital resilience. In this, expertise is key./