

# Digital Sovereignty

## State Action and Implications for Singapore

CAROL SOON  
Principal Research Fellow &  
Head, Society & Culture

ANN MAK RUI  
Research Assistant

CHEW HAN EI  
Senior Research Fellow

Institute of Policy Studies  
Lee Kuan Yew School of Public Policy  
National University of Singapore

June 2023



---

Centre for Trusted  
Internet and Community



This report is funded by the NUS Centre for Trusted Internet and Community  
[Research Grant CTIC-RP-20-04]

# Table of Contents

<b>Executive Summary</b>	<b>4</b>
<b>1 Introduction</b>	<b>6</b>
1.1 Methodology	7
1.2 Unpacking digital sovereignty	8
1.2.1 A short history of digital sovereignty	9
<b>2. Challenges that digital sovereignty poses to Singapore</b>	<b>10</b>
2.1 Risks of a fragmented Internet	10
2.2 Threats to Singapore's status as a business hub	11
2.3 Difficulties in safeguarding Singapore's cybersecurity	12
<b>3. How countries pursue digital sovereignty</b>	<b>13</b>
3.1 Digital sovereignty defined	13
3.1.1 The different levels where digital sovereignty plays out	15
3.2 Justifications for digital sovereignty	16
3.2.1 Prevent cyber-enabled foreign interference	16
3.2.2 Reduce foreign technological dependence	17
3.2.3 Boost autonomy and competitiveness of domestic industries	18
3.2.4 Regain data sovereignty	19
3.3 Digital sovereignty in practice	22
3.3.1 Enhancing cybersecurity	22
3.3.2 Data localisation requirements	24
3.3.3 Data protection and privacy legislation	26
<b>4. Singapore's performance on global indices and benchmarks related to digital sovereignty</b>	<b>29</b>
4.1 Guarding against cyber-enabled foreign interference	30
4.1.1 What Singapore has done to secure its infrastructure	30
4.1.2 Singapore's performance on cybersecurity indices	32
4.2 Growing the digital economy	36
4.2.1 What Singapore has done in terms of the digital economy	36
4.2.2 Singapore's performance on digital economy indices	38
4.3 Facilitating cross-border data flows	40
4.3.1 What Singapore has done to enhance cross-border data flows	40
4.3.2 Singapore's performance on cross-border data flows indices and benchmarks	44
4.4 Protecting citizens' data and privacy	45
4.4.1 What Singapore has done in terms of data privacy and protection	45
4.4.2 Singapore's performance on data protection and privacy indices	45

<b>5. Safeguarding Singapore's digital future</b>	<b>47</b>
5.1 At the individual level	48
5.1.1 Increasing vigilance and care among Singaporeans	48
5.2 At the organisational level	50
5.2.1 Introducing differentiated levels of digitalisation support for SMEs	50
5.2.2 Incentivising the private sector to prioritise data protection and privacy	51
5.2.3 Encouraging data sharing by the private sector	52
5.3 At the national level	56
5.3.1 Developing national-level metrics	56
5.3.2 Advancing gender equality in STEM fields	58
5.3.3 Implementing a data classification framework for cross-border data flows	60
5.4 At the regional level	62
5.4.1 Growing regional cybersecurity capacity	62
5.4.2 Greater coordination against cybercrime	64
5.3.3 Greater harmonisation on regional data privacy and protection laws	66
<b>6 Conclusion</b>	<b>67</b>
<b>7 References</b>	<b>68</b>

## Executive Summary

Singapore must navigate an increasingly fragmented digital landscape as digital sovereignty gains momentum worldwide. More and more states, guided by differing motivations and understandings of digital sovereignty, are pursuing unilateral policies and initiatives to regulate the Internet and the digital sphere more broadly. This can be seen in a diversity of countries ranging from Australia, Brazil, Germany, India, Italy, Senegal and Vietnam.

The current review explores what digital sovereignty means for Singapore. It begins by tracing the rise of digital sovereignty across the globe, and the challenges it poses for Singapore. The review then unpacks the key motivations behind the growing attempts of states to intervene in the digital sphere, and common strategies that states have undertaken to achieve these objectives.

The latter sections of the review focus on how Singapore can respond to the rise of digital sovereignty. To do so, we first examined the country's performance in the different domains of digital sovereignty. Based on the key gaps and challenges identified, the review concludes by recommending different measures Singapore can adopt to safeguard its digital future. Notably, this review is grounded in the belief that digital sovereignty presents both challenges and opportunities for Singapore, and highlights case studies and best practices the country can learn from to better harness the benefits of the cyberspace.

### Digital sovereignty

While ideas of digital sovereignty have gained traction across many parts of the world, it remains a complex concept lacking a unified definition. Digital sovereignty is often used interchangeably or alongside other related terms (e.g., technological sovereignty), and has been espoused by a range of actors to address issues of digital autonomy and empowerment. Nonetheless, as it has been used primarily in relation to the state, this review focuses specifically on digital sovereignty played out at the state level. This can be described as the growing trend where “nation states with different visions are seeking to increase their control over the Internet, primarily by using national tools rather than transnational cooperation and coordination” (Svantesson, 2019, p.28).

The pursuit of digital sovereignty by different states poses numerous challenges for Singapore. It has drastically escalated the likelihood of an impending “splinternet” — the situation where, rather than a singular, unified global Internet, governments isolate the Internet in national or regional networks with separate infrastructure that cannot interact with one another. However, as a regional hub that is highly connected with the rest of the world, such fragmentation would threaten Singapore's economy, connectivity and cybersecurity, amongst many other impacts. Hence, it is critical that Singapore actively monitors and responds to this development.

While states pursue digital sovereignty to achieve different objectives, the review identifies four dominant themes that motivate state action. Firstly, states often pursue digital sovereignty in order to prevent cyber-enabled foreign interference, which may undermine countries' stability and security. Some also seek to reduce their countries' dependence on foreign digital technologies and architecture, as this dependence is believed to perpetuate an inequitable distribution of economic benefits across firms and countries. Another common objective among states is to boost the autonomy and competitiveness of their domestic industries. Lastly, many also pursue digital sovereignty in order to regain their data sovereignty, whereby

data is seen as being overly concentrated in the hands of a few large firms and countries. While states have employed various strategies to achieve these objectives, three particularly common measures are cybersecurity strategies, data localisation requirements, and data protection and privacy legislation. Hence, based on the objectives and strategies examined, digital sovereignty can be seen playing out across four domains: cybersecurity, digital economy, cross-border data flows, and data protection and privacy.

Singapore has been recognised as one of the most wired and technologically advanced Information and Communications Technology (ICT) markets in the world (International Trade Administration, 2022). As part of its drive to become a Smart Nation, Singapore has introduced various policies and initiatives on the domestic and global front, leading to strong performances on indices that assess its digital economy, cross-border data flows, and data protection and privacy. For instance, the Salesforce's *Cross-Border Data Flows Index 2021* lauded Singapore's "stellar track record in creating the right policy and regulatory environment for the development of the digital economy", such as its clear and robust data protection regulation (e.g., the Personal Data Protection Act) and guidelines. However, room for improvement remains — particularly in the areas of cybersecurity, gender inclusivity in Science, Technology, Engineering and Mathematics (STEM) fields, data sharing, as well as data protection and privacy behaviours on the organisational and individual level.

### **Recommendations**

This review adopts an ecosystem approach to recommend the different measures that Singapore can undertake — on the individual, organisation, national and regional levels — to safeguard its sovereignty while maximising the benefits of the cyberspace.

On the individual level, policymakers should enhance the effectiveness national awareness campaigns to cultivate greater vigilance and care towards personal data among Singaporeans. Policymakers can also consider introducing differentiated levels of digitalisation support for small-medium enterprises (SMEs), incentivising a wider range of organisations to prioritise data protection and privacy, as well as developing initiatives that encourage private sector data sharing. On the national level, recommendations include developing national-level cybersecurity metrics, a national strategy for increasing gender equality in STEM fields, and implementing a data classification framework for cross-border data flows. Lastly, as a member of the Association of Southeast Asian Nations (ASEAN), Singapore should spearhead efforts to grow the region's cybersecurity capacity, strengthen regional coordination against cybercrime, and advocate for the greater harmonisation of data protection and privacy laws across ASEAN.

# 1 Introduction

The growth of the Internet, particularly during the 1990s, was originally perceived as a threat to the norms of state sovereignty (Couture & Toupin, 2019; Perritt, 1998). While the Internet began as a US government enterprise, created for research and defence objectives (Lewis, 2010), its use began growing among the public in the 1980s, particularly with the advent of the personal computer (Campbell-Kelly & Garcia-Swartz, 2013). By the early 1990s, global interoperability in data networking had begun to emerge (Mueller, 2002);<sup>1</sup> and the release of the World Wide Web further propelled adoption of the Internet across the globe (Glowniak, 1995; National Research Council, 1999).

Proponents of Internet freedom held that the Internet was qualitatively distinct from the physical world — a cyberspace that rendered state intervention both difficult and undesirable (Pohle & Thiel, 2020). As such, the Internet would develop its own rules which should be respected by states (Wu, 1997). Proponents even predicted that the development and integration of technologies would culminate in a “borderless society” (Green & Ruhleder, 1995), interconnecting individuals to such a degree that state boundaries would lose some of their relevance (Hermawanto & Anggraini, 2020). This was evident in John Perry Barlow’s famous declaration that “[governments] have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear.... Cyberspace does not lie within your borders” (Barlow, 1996).

Up until the late 1990s, most states paid little to no attention to the Internet (Palfrey, 2010). In fact, a highly permissive regulatory environment in the US and other Western countries was vital for the evolution of the Internet during its first two decades (Radu, 2019). Recognising its vast potential for stimulating innovation and economic growth, key policy decisions were made to allow market forces to operate (Oxman, 1999), and segregate the institutions of Internet governance from the direct oversight of the state (Deibert & Crete-Nishihata, 2012).

However, from the mid-1990s, many governments began taking steps to regulate the Internet. Most initially adopted a “functional approach” — attempting to use existing legislation, executive powers and resources most similar to that part of the Internet to regulate it for myriad reasons (Ang, 2008). For instance, if one aspect of the Internet functioned like a broadcasting station, then existing broadcasting rules would apply. However, Asian governments were observed to be more proactive compared to their peers (Wu, 1997), as they introduced Internet regulations soon after making it publicly accessible (Ang, 2008).<sup>2</sup>

As awareness of the kinds of content available online grew, pressure began mounting for governments to “do something” about harmful material (Ang, 2008). The Internet became

---

<sup>1</sup> By 1991 or so, data communication had begun to converge across the globe on Transport Control Protocol/ Internet Protocol (TCP/IP) and Internet-style domain names. TCP/IP enables any computer worldwide to exchange information with any other computer, regardless of the physical networks to which they are attached or the hardware they use.

<sup>2</sup> For instance, Singapore introduced the Class License Scheme in 1996, which automatically licensed all Internet Service Providers (ISPs) and Internet Content Providers (ICPs) (Chua, 2013). The scheme drew worldwide attention, as the first Internet-specific legislation aimed at regulating content. In South Korea, the National Security Law was applied to the Internet, where content that praised North Korea was blocked (Ang, 2008). However, the block was soon lifted following intense international criticism.

subject to US regulation for the first time in 1996, through the Communications Decency Act (CDA) which sought to protect children from exposure to indecent or obscene online material (Mercier, 1997). However, many of the CDA's provisions regulating decency were struck down by the courts as violations of the First Amendment (Ehrlich, 2002). That same year, attempts by the French government to pass legislation that would police the kinds of acceptable online content were also repudiated by its Constitutional Council (Ang, 2008). Hence, during the mid-1990s, initial albeit limited government efforts were made across different countries to regulate the Internet.

In addition to greater awareness of the threats and vulnerabilities arising from the Internet's development, there has gradually been the mounting realisation that the Internet is integral to economic activity and national security (Lewis, 2010). This, in turn, has contributed significantly to the rise of digital sovereignty across the globe. As the tussles and threats of a "splinternet" emerge, it is critical for Singapore to monitor and respond to these global developments. In this review, we first define and unpack the concept of digital sovereignty, and the different contexts and domains in which it is being contested. Next, we examine the key challenges that have emerged due to the rise of digital sovereignty around the globe and the implications for Singapore. By analysing global indices, international and domestic strategies, policies and programmes, we also identify the existing gaps as well as learning points that Singapore can adapt for its local context. Lastly, through an examination of the existing challenges and gaps, we propose a set of "anticipatory" and "responsive" steps that Singapore can undertake to safeguard its sovereignty and maximise the benefits of technology, while overcoming the pitfalls of an increasingly fragmented space.

## 1.1 Methodology

For this report, we conducted a literature review of about 350 sources, comprising academic research, consultancy reports, policy research, intergovernmental research, press releases and news publications. Key search terms that were used included "digital sovereignty", "technological sovereignty", "cyber sovereignty", "data sovereignty", "Internet sovereignty" and other related terms specific to each section. While their exact meaning and usage may vary from discipline to discipline (Hummel et al., 2021), the above search terms have often been used interchangeably, or in association with one another, in political, academic and media discussions (Adonis, 2019). Hence, a range of terms were included to comprehensively capture the literature regarding digital sovereignty. The review was conducted from September 2022 to May 2023. Current, Singapore-based and diverse sources were also included whenever possible.

As part of this landscape review, we also conducted in-depth interviews in March 2023 with domain experts from around the world on their thoughts on digital sovereignty. The four domain experts comprised two professors who are thought leaders in the field, a Managing Director of a leading industry association, as well as a digital rights activist.



**Susan Ariel  
AARONSON**  
Research Professor  
of International  
Affairs, George  
Washington  
University



**Ingrid VOLKMER**  
Professor of Digital  
Communication and  
Globalisation,  
University of  
Melbourne



**Jeff PAINE**  
Managing Director,  
Asia Internet  
Coalition



**Ploy  
CHANPRASERT**  
Founder,  
Digital Reach

## 1.2 Unpacking digital sovereignty

At the time of writing, there is no single, clearly defined definition of digital sovereignty (Baezner & Robin, 2018; Elms, 2021a). While digital sovereignty has also been espoused by a variety of actors like indigenous communities, tech activists, grassroots movements and individual citizens to examine digital autonomy and empowerment at those levels (Couture & Toupin, 2019), it has been primarily used in relation to the state (Adonis, 2019). In light of this, and given that earlier policy reviews in this series had addressed the individual level (e.g., [digital inclusion](#) and [citizen participation in governance](#)), this review focuses on digital sovereignty played out at the state level. As the term implies the merging of two subject areas — sovereignty and the digital sphere — we first examine the root concept of sovereignty.

Sovereignty is a notoriously nebulous concept, as its specific meaning has varied and been contested throughout history (Bartelson, 2006; Nagan & Hammer, 2004). The history of the concept has been one of “conceptual migration” (Falk, 2001), whereby the specific challenges of each historical period has influenced the objectives and functions granted to sovereignty at a particular space and time (Besson, n.d.). Nonetheless, despite the lack of a singular, unified definition, most interpretations of sovereignty have centred around two core features. Sovereignty is typically associated with: (i) supreme authority within a geographically bounded territory (Krasner, 1988) and (ii) independence from other sovereigns (Koskenniemi, 2009). Both aspects are interconnected, as undisputed control over a territory implies freedom from unwanted interference by an external authority (Philpott, 1995). The rise of the sovereign state is often traced back to the Treaty of Westphalia in 1648 (Hassan, 2006), which restructured the elaborate matrix of overlapping jurisdictions in Europe. Through the treaty, political authority became consolidated within a clearly demarcated territory, whereby external actors were excluded from domestic authority structures (Rudolph, 2005).

State sovereignty has become a foundational principle of international relations, guiding states in their internal and external rights and responsibilities (Ramos, 2013). Following the establishment of the United Nations (UN) in 1945, the principles of sovereignty have been



enshrined into the UN Charter. The foremost right of sovereign states is their absolute jurisdiction over its territory and the citizens residing in it.<sup>3</sup> They are also protected from external interference, as other states are prohibited from intervening in “matters which are within [its] domestic jurisdiction”, or from threatening its “territorial integrity” and “political independence”.<sup>4</sup>

### 1.2.1 A short history of digital sovereignty

As highlighted in the Introduction, the 21st century has been marked by an escalating tide of state attempts to regulate the Internet (Palfrey, 2010; Martinet, 2021), as ideas of digital sovereignty gain popularity (Glasze et al., 2022). Spurning the libertarian values that characterised the early days of the Internet (Martinet, 2021), states are increasingly asserting their control over the Internet and digital sphere more broadly (Pohle, 2020).

Initially, digital sovereignty claims were made primarily by authoritarian governments (Pohle, 2020; Glasze et al., 2022), often with reference to ideas of a Westphalian world order of territorially defined sovereign states, national self-determination, and non-interference from other states (Budnitsky & Jia, 2018; Creemers, 2020). The Chinese government in particular, has consistently asserted its sovereignty over the digital sphere, long before similar ideas gained traction in the West (Cong & Thumfart, 2022). Domestically, it undertook the controversial “Great Firewall of China” during the late 1990s, with the alleged intention of filtering and censoring false information from outside of China (Chandel et al., 2019). China also began advocating for the norms of digital sovereignty in the global arena, using international governance organisations as a platform to lobby for greater state influence in Internet governance processes (Sherman, 2022; Cai, 2018). Digital sovereignty has long been regarded in China as crucial to safeguard its national security and ideological security (Wang, 2020). Even as early as the mid-1990s, academic publications in China were already exploring the idea of digital sovereignty (Thumfart, 2022), whereby the Internet was regarded as a national concern due to threats of interference posed by a US-dominated Internet (Cong & Thumfart, 2022).

While authoritarian governments spearheaded the discourse on digital sovereignty, other governments also grew increasingly keen to regulate the Internet. This manifested in the rise of the Internet filtering on a national level across the globe, with a 2006 study by the OpenNet Initiative (ONI) of 40 countries finding evidence of technical filtering in 26 countries (Deibert et al., 2008). While the states that practised state-mandated filtering were predominantly clustered in East Asia, the Middle East and North Africa and Central Asia, extensive filtering was also documented in Northern Europe and the US. Over time, states have expanded their range of control mechanisms that restrict and influence access to information at different points of control (Deibert et al., 2011). Hence, the start of the 21st century witnessed a transition across the globe, from a more laissez-faire approach towards greater state intervention in the digital sphere.

Since the 2010s, ideas of digital sovereignty have spread to many political spheres across the world (Bosoer, 2022). The concept has been increasingly pursued in countries as diverse as

---

<sup>3</sup> Article 2(1) of the UN Charter states that “the Organization is based on the principle of the sovereign equality of all its members”.

<sup>4</sup> Quotations are taken from Articles 2(4) and 2(7) of the UN Charter.

Australia, Brazil, Germany, India, Italy, Senegal and Vietnam (Internet Society, 2022). Underlying the expanding discussion on digital sovereignty is the concern that the digital transformation is a threat to “the sovereign state” and in some case, “the sovereign subject” (Glasze et al., 2022). Hence, governments have begun pursuing digital sovereignty for a myriad of objectives and to address a multitude of issues relating to the Internet and technology. Section 3 will unpack some of these key issues.

## 2. Challenges that digital sovereignty poses to Singapore

The growing pursuit of digital sovereignty across the globe has significant implications for many states, particularly Singapore. Singapore must contend with an international climate where states, guided by differing interpretations of digital sovereignty, are increasingly undertaking unilateral policies and initiatives to regulate the digital sphere (Wood et al., 2020). This trend was observed in a report commissioned by the Internet and Jurisdiction Policy Network, which remarked that “nation states with different visions are seeking to increase their control over the Internet, primarily by using national tools rather than transnational cooperation and coordination” (Svantesson, 2019, p.28).

### 2.1 Risks of a fragmented Internet

As a small state lacking in strategic weight, Singapore is highly susceptible to, and has limited control over international trends (Public Service Division, n.d.). Singapore must navigate the mounting efforts by other states to expand control over the digital sphere, which has greatly escalated the possibility of an impending “splinternet”, or “balkanised Internet”. This refers to the situation where, rather than a singular, unified global Internet, governments isolate the Internet in national or regional networks with separate infrastructure that cannot interact with one another (Ball, 2022; Collins & AFP, 2019).

Due to the layered and distributed architecture of the Internet, fragmentation can take various forms (Perarnaud et al., 2022). It may take the form of technical fragmentation, which results from what may be deliberate or unintentional efforts to sever, limit or disrupt technical connectivity between one part of the Internet and the rest of the network (Perarnaud et al., 2022). One instance occurred in 2019, when Russia adopted a law to give the country a “sovereign Internet” by creating a national domain name system (DNS) that would safeguard the Russian-language section of the Internet should it be disconnected from the World Wide Web (“Putin Signs Internet Isolation Bill Into Law,” 2019). Internet fragmentation may also occur at the content level, whereby connectivity is preserved at the technical level, but users are limited in their practical access to online content (Perarnaud et al., 2022). This may be achieved by compelling technology companies to limit specific content. One example is the Cyberspace Administration of China’s ordering of the country’s top technology companies to conduct “immediate cleaning and rectification” of their platforms to remove “offensive” content (Reuters Staff, 2017).

The growing fragmentation and heterogeneity of cross-border data rules was reported by the Centre for Economic Policy Research (Evenett & Fritz, 2022). The centre’s report analysed

information from over 15,000 policy and regulatory developments and found that European and Group of 20 (G20) governments had taken 1,731 legal and regulatory steps since the start of 2022. These measures mainly targeted data governance, online content moderation, and competition law enforcement. Moreover, the pace of state intervention also appears to be accelerating. While the first quarter of 2020 saw 71 regulatory developments, there were 217 policy interventions announced or implemented in the first quarter of 2022. Concerningly, it was also revealed that one-third of global trade in digital economy goods faced market access barriers, highlighting the pervasiveness of trade barriers between national digital sectors.

Singapore has consistently ranked as one of the most globally connected countries in the world, in terms of flow of goods, capital, people, as well as data (Subhani, 2020; “Singapore the most connected country in the world,” 2016). Hence, Singapore’s economy relies heavily on the Internet and free flow of data across borders and may be seriously impacted by an increasingly heterogenous and fragmented digital landscape. It has even been estimated that Singapore’s economy could lose up to \$200 million daily should the country’s Internet shut down, an extreme but possible consequence of widespread Internet fragmentation (Chia, 2022). Additionally, worsening Internet fragmentation, whereby the global Internet splinters into separate intranets which lack interoperability, could impair Singaporeans’ ability to connect with others from around the world (Low, 2022). Access to content and information from different parts of the world could also be limited due to incompatible technologies.

## 2.2 Threats to Singapore’s status as a business hub

The growing pursuit of digital sovereignty across the globe also presents a major threat to Singapore’s status as a hub. Over the course of its history, Singapore has maintained its status as a hub for various activities, from being a successful free entrepôt during its colonisation under the British empire (Borschberg, 2016) to a regional hub for technology and innovation (Yeo, 2021). Singapore has ranked highly on indexes measuring innovation, such as the Bloomberg Innovation Index 2020 (Jamrisko, 2022)<sup>5</sup> and Global Innovation Index 2022 (World Intellectual Property Organisation [WIPO], 2023).<sup>6</sup> Moreover, approximately 80 of the world’s top 100 technology companies, such as Google, IBM and Microsoft, have a significant presence in Singapore — many of which have maintained their presence in the country for some time (Ng, 2021). Unsurprisingly, Singapore’s digital economy<sup>7</sup> has now become critical to the progress and welfare of the country and its citizens.

However, the pursuit of digital sovereignty by different states may jeopardise Singapore’s position as a regional hub for innovation and technology. Cross-border data access, usage, and exchange are all critical for economic growth, as nearly every sector — ranging from manufacturing, retail and services — relies on the flow of data between countries (Meltzer & Lovelock, 2018). In the case of Singapore, cross-border data flows and the overall digital

---

<sup>5</sup> Singapore was ranked 3rd on the Bloomberg Innovation Index.

<sup>6</sup> Singapore was ranked 7th on the Global Innovation Index 2022.

<sup>7</sup> While there are various ways to understand the digital economy, the G20 Digital Economy Task Force (DETF) defines it as encompassing “all economic activity reliant on, or significantly enhanced by the use of digital inputs, including digital technologies, digital infrastructure, digital services and data. It refers to all producers and consumers, including government, that are utilising these digital inputs in their economic activities” (Hatem et al., 2020).

economy have expanded significantly over the years (Ministry of Trade and Industry [MTI], 2017; Google et al., 2022).

Consequently, the growing pursuit of digital sovereignty, such as through data localisation requirements and privacy legislation, poses serious risks to Singapore's digital economy. This was expressed by Ravi Menon, the managing director of the Monetary Association of Singapore (MAS) who warned that "we need more data connectivity, and less data localisation.... If data cannot cross borders, the digital economy cannot cross borders and we will be poorer for it" (Reuters Staff, 2018). While there do not appear to be studies that have calculated the economic impacts of restrictive foreign data policies on Singapore specifically, numerous studies suggest that such measures are generally detrimental for the country itself and its trade partners. For instance, studies by Frontier Economics (2022), Information Technology and Innovation (Cory & Dascoli, 2021) and the European Centre for International Policy Economy (Bauer et al., 2015; Ferracane & van der Marel, 2018) have found that restrictions on cross-border data flows will likely reduce trade volume between states. Hence, Singapore's economy may suffer from lower levels of digital trade with states requiring data localisation.

Moreover, data localisation requirements will likely increase costs for Singapore companies that have expanded overseas, for instance, by requiring them to make costly investments in local data infrastructure or hire more staff (Brannon & Schwartz, 2018). Given the pervasiveness of the digital economy in Singapore, these higher costs may not only impact Singaporean technology companies per-se, but also any company that uses the Internet to collect the data of foreign citizens. Besides data localisation requirements, it has also been observed that there may be a trade-off between privacy regulations and data-driven innovation (Goldfarb & Tucker, 2012). This is because the collection of consumer data provides companies with a wide range of benefits, such as enhancing their search engine algorithms or effectiveness of their advertisements. Hence, strict data protection and privacy laws in foreign states may impede Singaporean companies' ability to engage in data-driven innovation. Moreover, with a growing number of states actively supporting the growth and digitalisation of their domestic companies, this will increase the competition faced by Singaporean technology companies. As there are more than 300 Singapore-based technology companies now operating overseas (Liu, 2022), greater competition in foreign markets may threaten the economic livelihood of these companies and their employees.

## 2.3 Difficulties in safeguarding Singapore's cybersecurity

Additionally, the rise of digital sovereignty around the world has implications for safeguarding Singapore's cybersecurity. Cybersecurity is of paramount importance to Singapore, given its heavy reliance on technology and interconnectedness with the rest of the world (Cyber Security Agency of Singapore [CSA], 2016a). Moreover, it has become even more critical due to the rising prevalence of cyber-attacks in the country. The Singapore Cyber Landscape by the CSA (2022a) revealed that Singaporean companies and citizens are facing increasing incidents of malicious cyber activities such as ransomware attacks, phishing and malicious command-and-control servers.

The rise of cross-border data restrictions reduces the potential for countries to collaborate to address cybersecurity threats. Given the inherently transnational nature of the Internet, cyber

threats are typically transnational — with the Internet offering a global pool of Internet users and technologies which can be targeted (Grabosky, 2004). As such, many of the cyber threats faced by Singapore often originate from overseas sources. For instance, the Singapore Police Force has observed that at least 90 per cent of scams in Singapore have overseas origins. This is because most scams are executed across national boundaries by crime syndicates, which are well-equipped and skilled at utilising technology to cover their tracks (Chua, 2022). As for ransomware, many of the ransomware cases reported by Singaporean companies to SingCERT in 2021 also originated from outside of Singapore (CSA, 2022b). Hence, cross-border collaboration is critical to effectively address cybersecurity threats (Barriuso, 2022). For instance, cooperation between law enforcement agencies across countries such as Romania, Taiwan and Belarus, was essential to arrest the suspected leader of a cybercrime ring that had targeted financial institutions in over 40 countries (Peters & Jordan, 2019). Such incidents demonstrate the immense value of transnational cooperation in enabling the investigation and prosecution of perpetrators of cyber threats.

However, data localisation requirements diminish information-sharing opportunities between Singapore and other states' law enforcement, intelligence and other security actors — depending on the range of data covered by the respective requirements (Swire & Kennedy-Mayo, 2022; Sheppard et al., 2021). Data localisation may also hinder Singapore's ability to conduct forensic investigations of cyber-attacks, as perpetrators frequently switch between countries to avoid detection (Swire & Kennedy-Mayo, 2022). Moreover, as cybersecurity increasingly utilises automated techniques like machine learning and artificial intelligence, data localisation may decrease the quantity and variety of data available for Singapore to train datasets for defensive purposes. As Singapore has not implemented any overarching data localisation requirements, it may also be subjected to non-reciprocal cooperation — states with data localisation requirements are prevented from sharing data and yet profit from the information shared by states without localisation like Singapore. Thus, the rise of states undertaking unilateral policies in pursuit of digital sovereignty further exacerbates the challenge of safeguarding Singapore's cybersecurity.

## 3. How countries pursue digital sovereignty

### 3.1 Digital sovereignty defined

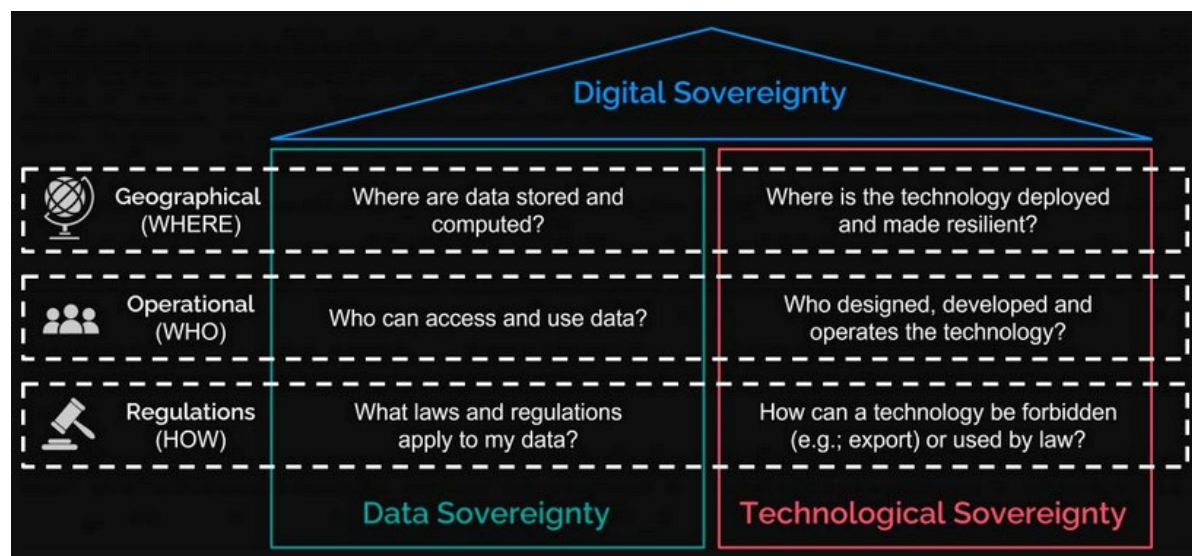
Despite its growing prominence in academic and public discourse, digital sovereignty is a complex concept lacking a unified definition. This ambiguity is partially due to its novelty in the academic literature, as most English publications on the concept were published only after 2010 (Couture & Toupin, 2019) — during the time that ideas of digital sovereignty began gaining momentum across the globe. To unpack this concept, this section identifies and analyses the overarching trends in countries' motivations and approaches to digital sovereignty across the world.

Digital sovereignty is often used in relation with several terms — in particular, technological sovereignty, cyber sovereignty, data sovereignty and Internet sovereignty. The use of varying terms may be the result of linguistic and cultural differences between the various actors of digital sovereignty, or their respective areas of focus (Couture & Toupin, 2019). Nonetheless,

although they are frequently used in place of another, the terms should not be understood as synonymous (Autolitano & Pawlowska, 2021).

Digital sovereignty is often framed as an umbrella term encompassing both data and technological sovereignty (Martinet, 2021). Data sovereignty tends to focus on data-related areas like data storage, processing and access (Moerel & Timmers, 2021), whereas technological sovereignty is typically centred on key technologies, digital infrastructure and innovation (Autolitano & Pawlowska, 2021). These two concepts may be subsumed under the overarching concept of digital sovereignty (e.g., Kaloudis, 2021; Bjola, 2021), which also covers a wider range of regulatory and policy elements in the digital sphere (Burwell & Propp, 2020). Figure 1 below presents an example of how these terms have been conceptualised in relation with one another.

Figure 1. Data sovereignty and technological sovereignty as pillars of digital sovereignty



Source: Zakhour & Gomes (n.d.)

While digital and cyber sovereignty should also not be equated as identical concepts, the exact relationship between the two remains unclear (Bosoer, 2022). It appears that the term “cyber sovereignty” is typically used in relation to authoritarian states, who prescribe a “Westphalian” approach towards the cyberspace (Lahmann, 2021). Likewise, Internet sovereignty has often been associated with China (McKune & Ahmed, 2018; Zeng et al., 2017) and Russia (Kolozaridi & Muravyov, 2021), to such an extent that it has been regarded as part of their national brand (Budnitsky & Jia, 2018).

What constitutes the digital sphere also differs across definitions. While some definitions identify the digital assets that are involved, they vary in their specificity. For instance, some definitions state the specific assets involved, such as “data, hardware and software” (Fleming, 2021). Conversely, others offer more vague descriptions of the digital sphere, such as “the Internet and broader digital ecosystem” (Musiani, 2022) or the “digital exhaust created by a person, business or government” (Mozur et al., 2022). This variation is unsurprising given that different agents understand and assert digital sovereignty in their own unique manner. Hence, the assets relevant to digital sovereignty also tend to differ from actor to actor.

### 3.1.1 The different levels where digital sovereignty plays out

As a multifaceted concept, digital sovereignty typically manifests at the levels of (i) state versus state, (ii) state versus industry, and (iii) state versus state via industry. At the state level, states pursue digital sovereignty to protect or further their national interests against the perceived threats posed by other states. They may do so for a variety of reasons, such as to strengthen their autonomy, security or economic competitiveness (Pohle & Thiel, 2020).

[Ingrid Volkmer on motives for digital sovereignty] “Governments are still adopting very national perspectives on digital sovereignty.... In France, it’s culture-specific, so they want to protect French culture in this globalised world. And in Australia, it’s also about businesses, and in other countries about something else. In Africa, it’s about the digital economy. So, each of these countries have their very different regulatory motives, their different understandings of what sovereignty is.”

[Jeff Paine on motives for digital sovereignty] “Different areas and regions have different goals.... If you take places like China, Turkey or Russia, they will actually point to what the European Union’s idea is, but obviously they have slightly different goals and objectives. You know, exerting control over citizens, really to be able to actually control the regime or the empire, so to speak.”

To achieve their objectives, states have adopted a diverse range of strategies regarding the digital sphere (Volkmer, 2021). This may include data localisation requirements (Wu, 2021), data protection laws (Elms, 2021a) or other miscellaneous legal obligations, such as granting governments the right to access proprietary data (Bauer et al., 2015).

The pursuit of digital sovereignty is also evident in the interactions between states and technology companies (Floridi, 2020). States increasingly perceive technology companies as having excessive power and resources, hence necessitating regulation. These concerns often centre around “big tech” — technology companies like Meta, Alphabet, Amazon and Microsoft, which have come to dominate their respective market segments across much of the globe (Stucke, 2018).

However, the tension between states and technology companies extends beyond the big tech companies. Online platforms, digital advertising companies, data brokers and companies from different sectors (e.g., insurance, consulting, or health analytics companies) also interact with all kinds of information about Internet users (Morey et al., 2015; Christl, 2017a). The collection, trade and utilisation of personal data by this diverse range of technology companies have been increasingly scrutinised (Christl, 2017b), with a growing number of states seeking to regulate these companies. This drive to regulate technology companies is also not limited to concerns over their harnessing and use of personal data. States can be seen intervening for a range of reasons, which will subsequently be unpacked in the following section.

However, states are not solely regulating technology companies when they impose restrictions and requirements. Instead, they may seek to curtail influence from another state via regulation of specific industries and companies. The strategic importance of technology companies has been especially evident in the current US-China Tech War, where the US has progressively

attempted to restrict Chinese firms' access to US technology (Swanson, 2022). Notably, the semiconductor industry has recently come under the spotlight, after the US government passed a sweeping set of controls on semiconductors and other high-tech exports to Chinese companies (Wang, 2022). In response, the Chinese government has developed plans to provide more than 1 trillion yuan to subsidise the purchase of domestic semiconductor equipment by Chinese firms (Zhu, 2022). The short-form video platform TikTok, owned by Chinese company ByteDance, has also become a major flashpoint for tensions between the West and China. Mounting concerns that user data may be accessed by the Chinese government has led to the app being banned on official government devices across the US, UK, Canada, New Zealand and the EU (Murphy et al., 2023). Hence, the relationship between states and technology companies is a complex yet highly important dimension of digital sovereignty.

## 3.2 Justifications for digital sovereignty

While states pursue digital sovereignty for a variety of reasons, we focused on four dominant themes in existing literature.

### 3.2.1 Prevent cyber-enabled foreign interference

One key concern driving states to pursue digital sovereignty is the threat of cyber-enabled foreign interference. Cyber-enabled foreign interference may be defined as “any activity that occurs in cyberspace that enables broader efforts by one state to influence or interfere in another state” (Milner, 2021). Numerous countries, ranging from Australia (Doherty, 2019), Canada (Canadian Centre for Cyber Security, 2021) and Singapore (Ministry of Foreign Affairs [MFA], 2022), have expressed concerns about the worsening risk of foreign interference enabled through digital technologies. This may occur through data breaches, espionage and hostile information campaigns, which threaten countries' stability and security. While the threat of foreign interference is not new (Lai, 2019), technological developments like the rise of social media platforms (Ringhand, 2021), deepfakes (Pawelec, 2022), and the digitalisation of government services and processes (Dowling, 2022), have escalated the threat by increasing the scale and ease of foreign interference operations.

Numerous studies attest to the growing threat of cyber-enabled foreign interference. An example is the rising employment of “cyber troops” by governments and political parties around the world to manipulate the opinion of domestic or foreign audiences (Bradshaw & Howard, 2017). One instance was revealed in 2019, when Meta announced its removal of 783 accounts, pages and groups that engaged in “coordinated inauthentic behaviour” across countries like Germany and Afghanistan — activities that were allegedly coordinated by Iran (Gleicher, 2019). But while accusations of cyber-enabled foreign interference tend to be directed at a few specific countries, the threat is likely more pervasive than it seems. For example, a report by Facebook (2021) revealed that between 2017 and mid-2021, it had taken down 150 covert influence operations originating from over 50 countries.

Cyber-enabled foreign interference is especially concerning when targeted towards elections and referendums. According to research by the Australian Strategic Policy Institute (ASPI), there has been a marked increase in cyber-enabled foreign interference in elections and referendums since 2017 (O'Connor et al., 2020). One particularly high-profile example



occurred during the 2016 US elections, where Russia reportedly conducted an extensive influence campaign that included the hacking Hillary Clinton's campaign and proliferation of propaganda on social media platforms (Abrams, 2019). Since then, allegations of political interference by foreign governments have continued to amass, such as in the 2017 French presidential elections (Daniels, 2017), the 2019 European Parliament elections (Scott & Cerulus, 2019), and the 2020 Taiwanese presidential elections (Chung & Hetherington, 2018).

Consequently, many governments are under mounting pressure to adopt measures to prevent cyber-enabled foreign interference. For instance, the Special Committee on Foreign Interference in all Democratic Processes in the EU, Including Disinformation (INGE), released a report urging the EU to develop a common strategy to combat foreign interference campaigns (European Parliament, 2022).

It should be noted that the threat of cyber-enabled foreign interference is also linked to concerns over foreign technological dependence. Specifically, states are increasingly wary that the use of foreign technologies may render them vulnerable to foreign surveillance and espionage. For example, countries such as New Zealand (Greenfield, 2018), Sweden (Mukherjee, 2022) and Australia (Choudhury, 2019) have banned Chinese suppliers like Huawei and ZTE from selling 5G equipment in their countries, due to fears that it could be used by the Chinese government for espionage (Maizland, 2020). Meanwhile, the Chinese government has long accused US technological products of containing backdoors, or built-in weaknesses, which allow the US to infiltrate sensitive networks and access foreign data (Rolland et al., 2020).

Such concerns were greatly amplified with the 2013 Edward Snowden revelations, where it was revealed that the US government had been conducting extensive Internet and phone surveillance on millions, including country leaders like Angela Merkel ("Edward Snowden: Leaks That Exposed US Spy Programme," 2014). Surveillance was carried out by tapping directly into the servers of nine prominent US companies, including Facebook, Microsoft and Google (Gellman & Poitras, 2013), fuelling intense distrust towards US technological companies (Shahani, 2014; Miller, 2014). The aftermath of the Snowden revelations saw intensified calls for digital sovereignty, with countries often citing the need to safeguard against foreign surveillance and interference (Donahoe & Canineu, 2014). For instance, the Brazilian government responded by mandating that storage, management and dissemination of Brazilian data be done through in-country data servers under the Marco Civil (Israel & Boadle, 2013).

### 3.2.2 Reduce foreign technological dependence

Another motivation behind states' pursuit of digital sovereignty is to reduce their dependence on foreign digital technologies and architecture. There has been a mounting perception that developing countries' foreign digital dependence leads to an inequitable distribution of economic benefits. This is because big tech companies have expanded their products worldwide, extracting data and profit from users across the globe and concentrating power and resources in either the US or China (Kwet, 2019a). Consequently, by being saturated with readily available services and technologies, developing countries are unable to grow domestic industries and develop products capable of competing with big tech (Kwet, 2019a). In light of this perspective, developing countries are increasingly seeking to assert greater autonomy in

the digital sphere. This was evident when countries such as Indonesia, India and South Africa, refused to sign the Osaka Declaration on Digital Economy, due to concerns that they would be denied “policy space” for their digital industrialisation under the proposed agreement (Kanth, 2019). Policies such as data localisation requirements (Hicks, 2019; see Section 3.3.2) and stronger data protection laws (Coleman, 2019; see Section 3.3.3) have also been considered as ways to reduce the dominance of foreign technology players.

Concerns over foreign technological dependence are typically directed towards the US and China, which now stand at the forefront of a wide range of technologies. One example is the cloud computing industry, where eight out of the 10 of the hyperscalers<sup>8</sup> with the largest market share are either American or Chinese companies (Synergy Research Group, 2020). However, the technological dominance of the US and China has been perceived as a threat to the national autonomy and interests of states across the world. Countries are increasingly wary that technological dependence may lead to a form of “digital neo-colonialism”, where, by controlling the digital ecosystem, the US and China will be able to influence the political, economic and cultural aspects of other states’ domestic life (Gravett, 2020; Kwet, 2019b).

[Susan Ariel Aaronson on distrust towards US and Chinese companies] “There is extreme distrust of the giant digital firms in the US and China. It’s this distrust — but at the same time, everybody uses these products and services.... And TikTok is a perfect example of [this].”

### 3.2.3 Boost autonomy and competitiveness of domestic industries

States are also increasingly pursuing digital sovereignty to bolster the autonomy and competitiveness of domestic industries. Such an aim may be linked to the previous objectives. For instance, the desire to strengthen domestic technology industries may be partially driven by concerns about foreign technological dependence. This was evident in the wake of the Snowden revelations, when the German government responded with measures aimed at regaining digital sovereignty. They adopted initiatives to develop trusted IT products and use national IT security technologies, rather than remaining reliant of foreign providers (Pohle, 2020; Steiger et al., 2017). But regardless of the potential influence of other factors, strengthening economic autonomy and competitiveness is a distinct goal that has been clearly prioritised by numerous states. This was evident with the EU, which has expressed concerns that it is lagging in the digital sphere and has become dependent on foreign technologies (Madiaga, 2020). Consequently, in its “2030 Digital Compass: The European Way for the Digital Decade”, the EU outlined its plans to achieve digital leadership by drastically increasing investments in critical technologies like cloud computing and AI, as well as digital infrastructure (European Commission, 2021).

[Jeff Paine on the EU’s economic motivations] “If you look at the EU policymakers, when they look at digital sovereignty, they really want to, one, seek to lessen dependence on foreign technology.... And really, what they want to do is be able to embrace innovation, but also give their local domestic players a chance at competing with international players.”

---

<sup>8</sup> Hyperscalers can be broadly defined as data centre operators that offer innovative, scalable cloud computing services (Pankajakshan, 2022).

To strengthen domestic industries, states have introduced measures aimed at promoting local innovation, and nurturing local technology and service providers so that they can better compete against foreign rivals (Pohle & Thiel, 2020; Internet Society, 2022). For instance, under its Collective Awareness Platform for Sustainability and Social Innovation (EC Program CAPS), the European Commission has invested around €60 million for ground-up, citizen-led ICT-enabled initiatives which address urgent social and sustainability issues (Passani et al., 2015; Bria, 2015). Meanwhile, Vietnam also introduced its “Make in Vietnam” initiative in 2019. The initiative sought to promote the establishment of 100,000 local technology firms and make Vietnam one of the top 30 countries in IT development (Nguyen, 2019). It was also inspired by similar campaigns in other countries, such as “Made in China 2025” (Kennedy, 2015).

The measures taken may also form part of states’ larger economic and industrial policy strategies, with the aim of digitising entire sectors of the domestic economy. Hence, they may not only target the newer IT-related sectors, but also other industries and sectors such as telecommunications and logistics (Pohle & Thiel, 2020). One example is “Thailand 4.0”, Thailand’s national development plan of utilising technology to enhance the competitiveness of local businesses and the country’s economy (“Thailand’s Digital Transformation Boosts Data Industry,” 2021). A key prong of “Thailand 4.0” involves driving the adoption and innovation of digital, automatic, and robotics technologies across small and medium-sized enterprises (SMEs), manufacturing companies and the service sector.

### 3.2.4 Regain data sovereignty

Another key motivation driving states is the desire to regain their data sovereignty. Data has become a highly contested asset in the discourse surrounding digital sovereignty. It encompasses a vast spectrum of information in various formats — ranging from structured, numeric data in traditional databases, to unstructured text documents, videos and financial transactions (Aaronson, 2021). Notably, data has become critical to every sector of society (Aaronson, 2022), with the *Economist* (“The World’s Most Valuable Resource Is No Longer Oil, but Data,” 2017) dubbing it “the oil of the digital era.”

There are primarily three groups of players that are relevant in discussions on data (Gao, 2022). Firstly, the individual creates the raw data and utilises the processed data. Meanwhile, the firm processes the raw inputs provided by consumers and typically manages such data. Lastly, the state oversees and regulates the use of data by these other groups. However, the recent years have seen more and more governments considering or implementing national rules to govern different types of data — particularly public, personal and proprietary data (Aaronson, 2021). Data is increasingly regarded by governments as a commercial asset that must be cultivated and controlled to serve their national interests (Aaronson, 2023).

[Susan Ariel Aaronson on data sovereignty] “Data sovereignty is about hoarding data. And countries that practice data sovereignty, even if they’re India, with 1.2 billion people, or China, are undermining the potential of data. Data’s been around for forever, and it will be around for forever, and you want to make it as accessible as possible.”

However, data is an inherently multidimensional asset that is difficult to pinpoint. It can take the form of a good, service, or both; its trade does not require any physical interaction; and its speed and frequency makes it difficult to locate on the borderless network (Aaronson, 2018). Moreover, legislating different types of data can be challenging from a practical perspective due to the overlapping nature of data categories. For one, personal and non-personal data may not always be easily segregated. Personal data may also be a component of business or company data, as in the case of employee records (Mishra, 2019). Hence, the complex, multidimensional nature of data must be carefully considered by states as they seek to pursue their data-related objectives.

[Susan Ariel Aaronson on the multidimensionality of data] “Data is multidimensional, right? It’s a proprietary good. It can be personal data, and it can be a public good simultaneously.... You can’t destroy it. It can constantly be reused.”

[Ingrid Volkmer on the complexity of data] “[Policymakers] don’t look at this data fluidity. That’s another gap. Because they often treat data, if you look through policy frameworks, you’ll see they talk about content. If the content needs to be made available, and the consumption of the content.... But in today’s world, I wonder what content really means.... Data is always replaced. It’s on the move. It’s always dynamic. There is no fixed content that you can regulate.”

Individuals’ personal data is collected and used by a wide range of technology companies, not limited to big tech companies, which collect data through an array of collection methods and sources, for instance, through user activity on their websites, surveys, or users’ Internet-connected devices’ IP addresses (Freedman, 2023). The definition of personal data in EU’s General Data Protection Regulation (GDPR) is “any information that relates to an identified or identifiable living individual” (Information Commissioner’s Office [ICO], n.d.-a). Firms have long depended on data to enhance the quality and efficiency of their products and services (Aaronson, 2018). For instance, personal data is used to better understand user preferences and create more personalised user experiences (Freedman, 2023). Internet users are tracked from site to site by technologies such as “cookies”, and their personal data are utilised to target them with relevant marketing (Chen, 2021). However, big tech, given their vast market share and access to personal data, often occupy the spotlight in states’ concerns regarding their citizens’ personal data.

[Susan Ariel Aaronson on big tech] “The reuse of data is controlled by the giant digital behemoth firms, the 70 platforms that, you know, UNCTAD has identified as the world’s largest platforms. They have the most data, they have the most cloud capacity, they have the best AI capacity, they have the best staff, etc.”

Several incidents have demonstrated the significant influence big tech may exert if left alone to accumulate vast sums of money, data, and power without sufficient government oversight.<sup>9</sup>

---

<sup>9</sup> One example is the Cambridge Analytica scandal, where millions of American Facebook profiles were harvested to develop a software programme that could profile US voters, to target them with personalised political advertisements (Graham-Harrison & Cadwalladr, 2018). The scandal drew rapid backlash from American and British lawmakers who demanded that Facebook explain how

Another issue is that many big tech companies are American firms, which end up processing massive volumes of personal data from citizens in other countries (Tham, 2022). While foreign governments may request for the personal data of their citizens from big tech, these requests are not always fulfilled. This was evident in a study by Surfshark that analysed the user data requests that Apple, Google, Facebook and Microsoft received from 177 countries between 2013 and 2022 (Surfshark, 2022). They found that on average, American companies only partially or fully fulfilled 66 per cent to 73 per cent of the requests over the years. Foreign governments' requests were also not fulfilled if they contravened US laws — essentially making the US the arbiter on whether requests would be granted (Tham, 2022). Moreover, a study by TechRobot found that between 2019 and 2020, the US both requested and was granted the most access to its citizens' data by big tech companies (Hellerud, 2022). Hence, it has been perceived that certain companies and states have far too much control over the personal data of citizens from all over the world.

Consequently, states have increasingly stressed the need to regain control over their citizens' personal data. Data protection and privacy laws may enable governments to establish meaningful constraints and oversight over how technology companies access, store and utilise citizens' personal information (Shahbaz & Funk, 2021). In general, they seek to ensure that personal information is lawfully obtained — typically through freely given consent — and for a specific purpose, and that it is not used for unauthorised surveillance, profiling, or unconnected purposes without consent (World Bank, n.d). They also endow individuals with certain rights over their data, such as the ability to access, review, rectify and erase personal information about them (World Bank, n.d.). Hence, such legislations not only allow governments to prescribe how technology companies deal with their citizens' personal data, but they may also increase citizens' control over their personal data. The secondary goal of enhancing citizens' autonomy and influence over their own data has been highlighted in several data protection and privacy legislations, such as the GDPR<sup>10</sup> and Canada's proposed Digital Charter Implementation Act 2020.<sup>11</sup>

The EU has been one of the world's most vocal advocates of digital privacy rights (Walt, 2020), and its "European Declaration on Digital Rights and Principles for the Digital Decade" outlines its commitment to protecting the digital privacy of EU citizens. The declaration asserts that "everyone has the right to the protection of their personal data online", and "everyone should have access to digital technologies, products and services that are safe, secure and privacy-protective by design" (European Commission, 2022a).

Besides the UK, the Indian government has also been a prominent advocate of regaining control over its citizens' data, with "data sovereignty" a central pillar of its foreign policy vision

---

Cambridge Analytica could obtain such information without needing to alert users (Rosenberg & Frenkel, 2018).

<sup>10</sup> For instance, recital 68 of the GDPR states that "to further strengthen the control over his or her own data, where the processing of personal data is carried out by automated means, the data subject should be allowed to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller."

<sup>11</sup> In the Canadian government's news release on the proposed Digital Charter Implementation Act 2020, it states that the legislation will "increase control and transparency when Canadians' personal information is handled by companies." For the full news release, refer to Innovation, Science and Economic Development Canada (2020).

(Basu, 2021). This emphasis was evident in India's draft National e-Commerce Policy 2019, which declared, "India and its citizens have a sovereign right to their data. This right cannot be extended to non-Indians" (Department for Promotion of Industry and Internal Trade, 2019).

### 3.3 Digital sovereignty in practice

States have employed a range of different strategies to achieve their digital sovereignty-related goals. This review has identified three strategies that many states have employed to address the objectives discussed in the preceding sections.

#### 3.3.1 Enhancing cybersecurity

The importance of cybersecurity has been increasingly emphasised by states across the world (see Section 3.2.1). Cybersecurity may be understood as "the art of protecting networks, devices, and data from unauthorised access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information" (Cybersecurity and Infrastructure Agency, 2021). A similar definition by the UK's National Cyber Security Centre (NCSC) defines cybersecurity as "how individuals and organisations reduce the risk of cyber-attack" (National Cyber Security Centre, n.d.). States are increasingly prioritising cybersecurity in order to defend against the burgeoning number of modern-day cyber threats, especially cyber-enabled foreign interference. Across the globe, at least 114 states have adopted cybersecurity strategies,<sup>12</sup> while 118 states have established national Computer Emergency Response Teams (CERTs) (Gillani et al., 2022). National CERTs are organisations dedicated towards the coordination of preventative measures and incident responses across the nation.

Examples of cybersecurity strategies from states across the world can be found in Table 1 below. We highlight Estonia's cybersecurity strategy due to its status as a small state that has become a leading cybersecurity norm entrepreneur at the UN and other international organisations (Crandall & Allan, 2015). Germany has been described as the most active advocate of digital sovereignty in the EU (Lambach & Oppermann, 2022; Pohle, 2020), and Lithuania was ranked highly on two cybersecurity indices.<sup>13</sup> Based on the same two indices, Malaysia was also analysed as it obtained, on average, the highest ranking across the Southeast Asian region.<sup>14</sup>

---

<sup>12</sup> Among the 118 states, 17 are from Sub-Saharan Africa, 18 from the Americas, 11 from the Arab states, 21 from the Asia-Pacific, 41 from Europe, and six from the Commonwealth of Independent States.

<sup>13</sup> Lithuania ranked 3rd in the e-Governance Academy's National Cyber Security Index (NCSI) 2021, and 6<sup>th</sup> in the Global Cybersecurity Index (GCI) by the International Telecommunication Union (ITU).

<sup>14</sup> Malaysia was the highest ranked Southeast Asian state in the NCSI, where it obtained the 20<sup>th</sup> position. It was also the 2nd highest ranked Southeast Asian state in the GCI, where it placed 6<sup>th</sup>.

Table 1. Examples of cybersecurity strategies

Country	Example of cybersecurity strategy	Key scope
Estonia	Cybersecurity Strategy 2019-2022	<ol style="list-style-type: none"> <li>1. To achieve a sustainable digital society with strong technological resilience and readiness to cope with crises.</li> <li>2. To achieve a strong, innovative, research-based and globally competitive enterprise and R&amp;D in the cybersecurity sector, covering the key competencies that are important for Estonia.</li> <li>3. To remain a credible and strong partner in the international arena.</li> <li>4. To achieve a cyber-literate society and ensure a future supply of specialists in the field.</li> </ol>
Germany	Cyber Security Strategy for Germany 2021	<ol style="list-style-type: none"> <li>1. To remain safe and autonomous in a digital environment.</li> <li>2. To strengthen the cybersecurity in private industry and critical infrastructures, and enhance cooperation between the government and industry.</li> <li>3. To develop a strong and sustainable cybersecurity architecture for every level of government.</li> <li>4. To strengthen Germany's active role in European and international cybersecurity policy.</li> </ol>
Lithuania	National Cyber Security Strategy (2018)	<ol style="list-style-type: none"> <li>1. To strengthen cybersecurity of the country and the development of cyber defence capabilities.</li> <li>2. To ensure prevention and investigation of criminal offences in cyber space.</li> <li>3. To promote cybersecurity culture and development of innovation.</li> <li>4. To strengthen a close cooperation between private and public sectors.</li> <li>5. To enhance international cooperation and ensure the fulfilment of international obligations in the field of cybersecurity.</li> </ol>
Malaysia	Malaysia Cyber Security Strategy 2020-2024	<ol style="list-style-type: none"> <li>1. To create effective governance and management.</li> <li>2. To strengthen legislative framework and enforcement.</li> <li>3. To catalyse world class innovation, technology, R&amp;D and industry.</li> <li>4. To enhance capacity and capability building, awareness and education.</li> <li>5. To strengthen global collaboration.</li> </ol>

[Ploy Chanprasert on the rise of cybersecurity laws] “In countries across Southeast Asia, you observe a wave of cybersecurity laws being adopted, or being proposed. Firstly, it was adopted in Vietnam, and then in Thailand, and then the idea expanded to Myanmar and Cambodia as well.”

Multilateral efforts have also been undertaken to strengthen cybersecurity across the globe. The EU has introduced the NIS 2 Directive, which establishes the baseline for cybersecurity risk management measures and reporting obligations across sectors in the EU, such as energy, transport, and digital infrastructure (Cyber Risk GmbH, n.d.-a). It aims to reduce divergences in cybersecurity requirements and implementation across member states, whereby they are required to adopt and publish the measures necessary for compliance by October 2024.

Meanwhile, the Economic Community of West African States (ECOWAS) also implemented its Regional Cybersecurity and Cybercrime Strategy in 2021. It seeks to improve the national cybersecurity and cybercrime mechanisms in member states, which will in turn strengthen the resilience and security of essential infrastructure and services in the region (ECOWAS, 2021). One of its objectives is for member states to adopt and update their national cybersecurity and cybercrime policy and strategy at least every five years. Another is for member states to each establish a national cybersecurity authority and national CERTs, and to develop a general security baseline with “legal force” (ECOWAS, n.d.).

As for the Association of Southeast Asian Nations (ASEAN), it recently launched the ASEAN Cybersecurity Cooperation Strategy 2021–2025, which builds on its past 2017–2020 strategy (ASEAN, n.d.-a). The strategy aims to build a cyberspace that is “open, secure, stable, accessible, interoperable and peaceful,” based on the “voluntary, non-binding norms of responsible State behaviour.” Its initiatives include the development of regional cybersecurity standards, multistakeholder regional capacity building programmes, and a regional CERT. ASEAN’s regional CERT covers eight functions, such as facilitating the coordination and information-sharing between member states’ national-level CERTs (CSA, 2022c).

### 3.3.2 Data localisation requirements

To address concerns over the lack of oversight and control over citizens’ data (see Section 3.2.4), many states have implemented data localisation requirements. In general, data localisation requires data to be stored and processed domestically, with the main objective of enhancing a state’s sovereign control over its citizens’ data (Wu, 2021). They have been increasingly utilised by governments to target a growing range of data types and categories deemed as “important”, “sensitive” or relevant to national security (Cory & Dascoli, 2021). Data localisation requirements have gained significant traction after the Snowden revelations (Mishra, 2015), whereby countries such as Brazil, Germany and India began considering enacting data localisation laws (Hill, 2014). Such policies are often justified by the need to prevent foreign surveillance or safeguard the privacy and security of personal data (Chander & Lê, 2015; Bauer et al., 2015). However, data localisation requirements may also be motivated by the desire to benefit domestic industries and the local economy (see Sections 3.2.2 and 3.2.3) — though such a goal may not be made explicit (Chander & Lê, 2015). Specifically, they may be used as non-tariff barriers that disadvantage foreign competitors in favour of domestic technology companies.

However, whether implementing data localisation confers economic advantages is highly contentious. One argument against data localisation is that local data centres may have to charge higher prices to local businesses and Internet users to store data, as compared with efficient global data centres which enjoy economies of scale (Selby, 2017). Another possibility



is that local businesses will be denied access to global services that may enhance their productivity (Chander & Lê, 2015).

[Jeff Paine's critique on data localisation] "Data localisation definitely increases costs, and the other issue is cybersecurity. It's one thing if you have sets of data all over the place, are you ensuring that the cybersecurity is really up to par?"

[Ploy Chanprasert's critique on data localisation] "Data localisation comes with costs. Big companies may be able to do it because they have more money compared to a smaller tech company.... In reality, it's not that easy just to say to localise data, it comes with higher costs."

Despite numerous counter-arguments, many countries have implemented data localisation requirements. According to the Information Technology and Innovation Foundation, the number of data localisation measures in force around the world has more than doubled from 67 to 144 between 2017 and 2021 (Cory & Dascoli, 2021). Moreover, at the time of writing, another 38 data localisation policies had either been proposed or were under consideration. China, India and Turkey in particular, were considered the "world leaders" in data localisation requirements (Cory & Dascoli, 2021). However, countries as varied as Australia, Brunei, Canada, Indonesia, Nigeria, South Korea and Vietnam have also introduced data localisation laws or restrictions on the free flow of data (Kyger, 2019; Mishra, 2015). Despite the growing trend, it appears that states are still navigating data localisation requirements. For instance, in 2019, Indonesia revoked its Government Regulation 82 of 2012, a provision that necessitated economy-wide data localisation (Li, 2022), although it has enacted localisation in specific sectors (e.g., finance) and is contemplating doing so in other areas (e.g., public service providers) (Cory, 2022).

Given their widespread implementation, data localisation requirements vary across the world. According to Wu (2021), most requirements tend to fall within three broad categories.

- The first and strictest type of localisation policy requires local-only storing, transmission and processing, which generally prohibits the transfer of data to other countries. An example is Russia's Federal Law No. 242-FZ, whereby operators must ensure that the recording, systematisation, accumulation, storage, adjustment and retrieval of personal data of Russian citizens is performed through database servers located within the territory (Golovanova, 2020).
- The second category requires companies to keep a local copy of data in local servers or data centres, granting governments easier access for regulation or law enforcement purposes. One example is the Indian Personal Data Protection Bill 2019, whereby sensitive personal data must be stored in India, but a copy may be transferred outside of India — subject to certain data transfer requirements (Lee et al., 2020).
- The last category involves the imposition of narrower, conditional restrictions, where data can only be transferred internationally if certain conditions are met by the

transferee and receiving country. For instance, Section 12 of Argentina's Data Protection Law forbids international data transfer to countries that do not provide "adequate levels of protection". Protection is deemed as adequate if it is derived directly from the legal order, self-regulatory measures or contractual clauses that include specific data protection provisions (Furman et al., 2022).

It should be noted that Argentina's Data Protection Law was also motivated by the desire to align the country's data protection law with the EU's GDPR (Microsoft, 2022), which has been an extremely influential data regulation (Larsen, 2022). Like the Argentinian law, the GDPR also permits the conditional transfer of personal data outside of the EU. Specifically, data may be transferred when the recipient territory possesses a level of data protection equivalent to that of the EU (Hirdaramani, 2022).

### 3.3.3 Data protection and privacy legislation

A growing number of governments are also implementing data protection and privacy legislations to protect personal data (see Section 3.2.1). According to the UN Conference on Trade And Development (UNCTAD), by the end of 2021, 137 out of 194 countries worldwide had implemented legislation to secure the protection of data and privacy (UNCTAD, n.d.). At the time of writing, another 9 per cent of all countries across the world were also in the process of drafting data protection and privacy legislation. However, adoption appears to be unevenly distributed around the globe — only 61 per cent of countries in Africa and 57 per cent of countries in Asia have adopted data protection and privacy legislation.

Despite their growing prevalence, data protection and privacy laws are not without their limitations and risks. Notably, the Office of the UN High Commissioner for Human Rights (OHCHR) has warned that data protection laws are often "inadequate or make broad exceptions for law enforcement and intelligence services" (OHCHR, 2022, p.13). Moreover, general data privacy laws typically "do not provide detailed guidance to ensure limitations on the use of specific surveillance tools" (OHCHR, 2022, p.13). Thus, the Office has stressed the need for dedicated legal instruments, particularly for surveillance done in the context of law enforcement and national security. They also recommended that laws and regulations have clearly determined and strict limitations on the access and merging of government databases.

[Jeff Paine's on the risks of data protection laws] "Some of the challenges that we see in [Southeast Asia] is the personal data protection laws, for example. They can grant excessive power to local authorities to exercise more control over the Internet. And that really can impact user confidence, and also the security and privacy of online communications. It also allows the state to have a lot more control of the digital space. And that really gives them the ability to tighten surveillance and impact online freedoms."

[Ploy Chanprasert on the limitations of data protection laws] "The personal data protection [laws] that are currently in place are not really enough, because usually, they exclude the government and state agencies.... Usually, countries have laws that allow the government to do a lawful interception.... So, when you have a data protection [law] in place, usually the law will have to exclude

the government because it would [contradict] with those existing laws that allow the lawful interception to happen.”

Several states have taken centre stage in the drive toward regaining control over their citizens’ data. The EU’s GDPR has been one of the most influential data protection and legislation, which has inspired similar regulations from other parts of the world. They include California’s Privacy Rights Act (Keane, 2021), Brazil’s Lei Geral de Proteção de Dados Pessoais (Carrillo & Jackson, 2022), and China’s Personal Information Protection Law (Borak, 2021). It has also had the “Brussels effect”, whereby the regulation has extended beyond EU borders because market mechanisms externalise domestic laws — for instance, rather than maintain different sites for varying regions, websites opt to apply EU requirements globally (Elms, 2021a). The GDPR has replaced the previous, disparate data protection laws existing across Europe, serving as a new framework for legislation across the EU (Burgess, 2020). Notably, the GDPR also claims extraterritorial jurisdiction, whereby it applies to organisations outside of the EU if two conditions are met: (i) the organisation offers goods or services to people in the EU, or (ii) the organisation monitors their online behaviour (Wolford, n.d.-a).

[Ingrid Volkmer on the extraterritoriality of the GDPR] “With the [GDPR], and this is the idea of the data subject in Europe, it also overrides other sovereign understanding[s], because all of a sudden, a European citizen living in Australia, targeted by an Australian advertising company who is monitoring his or her behaviour, needs to comply with the EU data regulation, because they are looking at the European citizen. So, there are these new formations of this sort of extraterritorial sovereignty, what we see in the EU.”

Table 2 below summarises the key features of the GDPR, based on information extracted from the European Parliament and European Council (2016) and Wolford (n.d.-b).

*Table 2. Key features of the GDPR*

Key definitions	<ul style="list-style-type: none"> <li>• Personal data: any information relating to an identified or identifiable natural person (“data subject”).</li> <li>• Controller: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.</li> <li>• Processor: a natural or legal person, public authority, agency or other body with processes personal data on behalf of the controller.</li> </ul>
Data protection principles	<ol style="list-style-type: none"> <li>1. Lawfulness, fairness and transparency: processing must be lawful, fair and transparent to the data subject.</li> <li>2. Purpose limitation: personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes.</li> <li>3. Data minimisation: personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.</li> <li>4. Accuracy: personal data must be accurate and, where necessary, kept up to date.</li> </ol>

	<p>5. Storage limitation: personal data may be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.</p> <p>6. Integrity and confidentiality: personal data must be processed in a manner that ensures security, integrity and confidentiality of the personal data, using appropriate technical or organisational measures.</p> <p>7. Accountability: the controller is responsible for and should be able to demonstrate compliance with all the principles.</p>
Rights of the data subject	<ul style="list-style-type: none"> <li>• The right to be informed</li> <li>• The right of access</li> <li>• The right to rectification</li> <li>• The right to erasure (“right to be forgotten”)</li> <li>• The right to restriction of processing</li> <li>• The right to data portability</li> <li>• The right to object</li> <li>• Rights in relation to automated decision making and profiling</li> </ul>
Key obligations	<p>Responsibility of the controller:</p> <ul style="list-style-type: none"> <li>• The controller shall implement appropriate technical and organisational measures to ensure and be able to demonstrate that processing is performed in accordance with the GDPR.</li> </ul> <p>Data protection by design and by default:</p> <ul style="list-style-type: none"> <li>• The controller shall, both when determining the means for processing and during the processing itself, implement appropriate technical and organisational measures (e.g., pseudonymisation) designed to implement the data protection principles.</li> <li>• The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.</li> </ul> <p>Processor:</p> <ul style="list-style-type: none"> <li>• When processing is to be carried out on behalf of a controller, the controller shall use only processors that provide sufficient guarantees to implement appropriate technical and organisational measures that meet the requirements of the GDPR.</li> </ul>

[Jeff Paine on the influence of the GDPR] “If you look at the EU, they had the GDPR. And I think that a lot of people at APEC then started trying to adapt their privacy rules based off GDPR. In some cases, they would cherry pick the parts that they liked, when setting up their own privacy regimes in Southeast Asia.”

The Indian government has also taken notable steps in terms of data protection legislation. It recently withdrew the Personal Data Protection Bill 2019, with the aim of replacing it with more comprehensive data protection (Verma, 2022). The new proposed bill, the Digital Personal Data Protection Bill (2022), covers personal data collected online and personal data collected offline but is digitised for processing (Goyal, 2022). A key feature of the bill is its proposal to

set up a Data Protection Board of India, which will monitor and assess non-compliance, as well as impose penalties. Technology companies such as Amazon and Meta will also be mandated to appoint data protection officers based in India (Pradhan & Kumar, 2022). India's Digital Personal Data Protection Bill is expected to have considerable influence on subsequent laws in other countries, given to its large population and influence in the global data economy (Keane, 2021).

## 4. Singapore's performance on global indices and benchmarks related to digital sovereignty

The previous sections of the review unpacked the concept of digital sovereignty, by analysing it from a theoretical perspective, as well as identifying trends in its application across different states. This next section examines how Singapore is doing in terms of safeguarding its sovereignty (i.e., protecting its cybersecurity and citizens' data and privacy) while harnessing the benefits of the cyberspace (i.e., growing its digital economy and cross-border data flows).

During our review, we found only one index that specifically analysed states' performance on digital sovereignty, the European Council on Foreign Relation's *European Sovereignty Index* (Puglierin, 2022). The index scored EU member states based on their contribution to European sovereignty across six terrains, including technology. However, as the index specifically examines EU member states, it is not directly applicable to non-EU states like Singapore. The scope of the index is also limited to a specific aspect of digital sovereignty and focuses on the regulation and capacity-building of "critical technologies", rather than other aspects of the digital sphere.

However, as discussed in the preceding sections, digital sovereignty is a multifaceted concept that encompasses other domains such as increasing the independence and competitiveness of local industries, and strengthening data protection and privacy. Hence, we selected global indices and benchmarks pertaining to the different domains of digital sovereignty, based on their recency and global scope. Where data was available, we also compared Singapore's performance on the indices to two digitally advanced states that have taken concerted efforts to enhance their digital sovereignty — Australia and Germany (see Table 3). Australia was identified as a country that had taken notable steps<sup>15</sup> towards pursuing digital sovereignty while striking the fine balance between guarding national interests with the pursuit of free digital trade policies (Internet Society, 2022; Department of Foreign Affairs and Trade, 2021). Germany was also examined given its status as one of the earliest and most prominent proponents of digital sovereignty in the EU (Internet Society, 2022; Lambach & Oppermann, 2021).

---

<sup>15</sup> Some notable initiatives include its whole-of-government Hosting Strategy to address "risks to data sovereignty, data centre ownership and the supply chain" (Australian Government, n.d.-a), and its appointment of an inaugural Ambassador for Cyber Affairs and Critical Technology (Wong, 2023).

Table 3. Global indices related to digital sovereignty

Domain	Index	Organisation	Singapore	Australia	Germany
Cybersecurity	Global Cybersecurity Index 2020	International Telecommunication Union (ITU)	4th	12th	13th
	Global Cyber Risk Literacy Index 2021	Oliver Wyman Forum	2nd	4th	11th
	National Cyber Security Index 2023	e-Governance Academy	31st	40th	5th
	National Cyber Power Index 2022	Belfer Center	18th	1st	10th
Digital economy	World Digital Competitiveness Ranking 2022	International Institute for Management Development (IMD)	4th	14th	19th
	Network Readiness Index 2022	Portulans Institute	1st	14th	8th
Cross-border data flows	Cross-Border Data Flows Index 2021	Salesforce	3rd	7th	7th
Data protection and privacy	Data Protection Index 2020	TRPC	4th	4th	4th
	Privacy Index	DataGuidance	Scored 5 out of 5	-	-
	Data Confidence Index	Global Web Index	Scored 1.5	Scored 1.6	Scored 1.3

Additionally, the following sections will also review the key measures that Singapore has implemented in the four different domains of digital sovereignty, to identify the gaps that should be addressed.

## 4.1 Guarding against cyber-enabled foreign interference

### 4.1.1 What Singapore has done to secure its infrastructure

Cybersecurity has long been a priority of the Singaporean government, with cybersecurity-related legislation dating back to the late 20th century. For instance, the Computer Misuse Act (CMA) was introduced in 1993 to criminalise access or modification of computer material, and other computer crimes (Ministry of Home Affairs [MHA], 2017). By the early 21st century, the government had begun implementing policies to coordinate cybersecurity efforts across the

government. These include its first Infocomm Security Masterplan (2005-2007) (Tan, 2005),<sup>16</sup> the Infocomm Security Masterplan (2008-2012) and the National Cyber Security Masterplan (NCSM2018) (CSA, 2016a).

The decade that followed witnessed a flurry of cybersecurity-related strategies and legislation. Notably, the CSA was established in 2015, with the mission of keeping Singapore's cyberspace "safe and secure to underpin our National Security, power a Digital Economy, and protect our Digital way of Life" (CSA, n.d.-a). Singapore's Cybersecurity Strategy 2016 was introduced a year after, which sought to build a resilient infrastructure, create a safer cyberspace, develop a vibrant cybersecurity ecosystem, and strengthen international partnerships (CSA, 2016a).<sup>17</sup> The CSA has since introduced initiatives to strengthen the cybersecurity of Singaporean companies. Some of these initiatives are presented in Table 4 below.

Table 4. Examples of cybersecurity initiatives by the CSA

Name	Year implemented	Details	Target group(s)
<a href="#">SG Cyber Safe cybersecurity toolkits</a>	2021	Tailored cybersecurity toolkits to provide information on cybersecurity issues and threats and enable organisations to adopt cybersecurity measures pertinent to their job roles.	Large enterprise leaders, SME owners, IT teams and employees
<a href="#">Cyber Essentials Mark</a>	2022	A cybersecurity certification for organisations embarking on their cybersecurity journeys, to enable them to prioritise the cybersecurity measures needed to safeguard their systems and operations from common cyber-attacks.	SMEs
<a href="#">Cyber Trust Mark</a>	2022	A cybersecurity certification for organisations with more extensive digitalised business operations. It adopts a risk-based approach to guide them in understanding their risk profiles and identify relevant cybersecurity preparedness areas required to mitigate these risks.	Larger or more digitalised organisations

More importantly, recognising the importance of partnerships to strengthen its cybersecurity, Singapore has also embarked on bilateral efforts like the Memorandums of Understanding (MOUs) with several countries. These include MOUs signed with India in 2015 (CSA, 2015), the Netherlands in 2016 (CSA, 2016b), Australia in 2017 (CSA, 2017) and Canada in 2018 (CSA, 2018). These MOUs formalise Singapore and its partner countries' commitment to

<sup>16</sup> The Masterplan was a strategic roadmap outlining national efforts to develop capabilities that would prevent cybersecurity incidents, protect Critical Information Infrastructure (CII) from cyber threats, and recover swiftly from actual attacks.

<sup>17</sup> This was later updated with the Singapore Cybersecurity Strategy 2021, which adopted a broader, more proactive and multistakeholder approach to cybersecurity.

cooperating in the domain of cybersecurity and establish collaborative measures such as information exchange and sharing on cyber threats and cyber-attacks, as well as joint cybersecurity exercises.

Lastly, ASEAN has also been a platform by which Singapore has sought to enhance its national and regional cybersecurity. Notably, the Singapore government has committed \$30 million to fully fund the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE), a “cyber think-tank” located within the CSA’s premises. The centre provides virtual cyber defence training and exercises for the national CERTs of ASEAN member states, as well as promotes open-source information sharing on cyber threats, attacks, and best practices among them (Chee, 2021a; Baharudin, 2018).

#### 4.1.2 Singapore’s performance on cybersecurity indices

Singapore has had a mixed performance on indicators pertaining to cybersecurity. In terms of indices that it placed well in, Singapore ranked joint 4<sup>th</sup> on the ITU’s *Global Cybersecurity Index (GCI) 2020*, alongside South Korea and Spain (see Table 5). It was ahead of Australia and Germany, which placed 12<sup>th</sup> and 13<sup>th</sup> respectively. The index examined 194 countries based on their commitment to cybersecurity across five pillars:

1. Legal: Measures the laws and regulations on cyber-crime and cybersecurity.
2. Technical: Measures the implementation of technical capabilities through national and sector-specific agencies.
3. Organisational: Measures the national strategies and organisations implementing cybersecurity.
4. Capacity development: Measures awareness campaigns, training, education and incentives for cybersecurity capacity development.
5. Cooperation: Measures partnerships between agencies, firms and countries.

Table 5. Countries ranked highest in the GCI 2020

Country	GCI score in 2020	GCI rank in 2020	GCI rank in 2018
US	100	1	2
UK	99.54	2	1
Saudi Arabia	99.54	2	13
Estonia	99.48	3	5
South Korea	98.52	4	15
Singapore	98.52	4	6
Spain	98.52	4	7
Russian Federation	98.06	5	26
United Arab Emirates	98.06	5	33
Malaysia	98.06	5	8

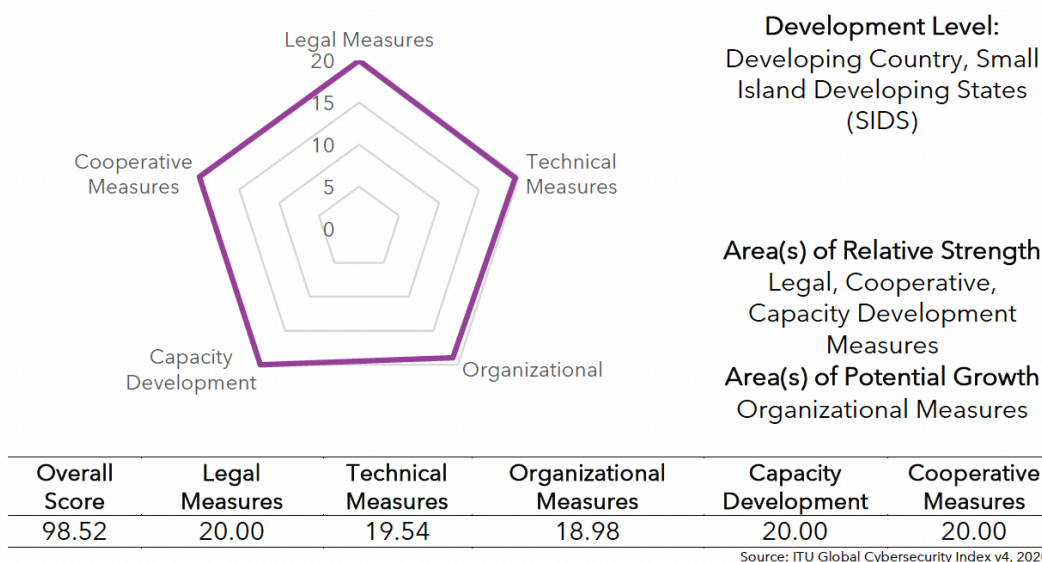
Singapore’s performance in 2020 (4) was an improvement from its 2018 position (6). In terms of its strengths, Singapore obtained perfect scores on the legal, capacity development, and cooperative measures pillars (see Figure 2). However, its lowest score was in the organisational measures pillar. This may partially be because Singapore appears to lack any



metrics for assessing (i) cyberspace associated risks or (ii) the level of cybersecurity development at the national level.

Figure 2. Singapore's scores across the five pillars of the 2020 GCI

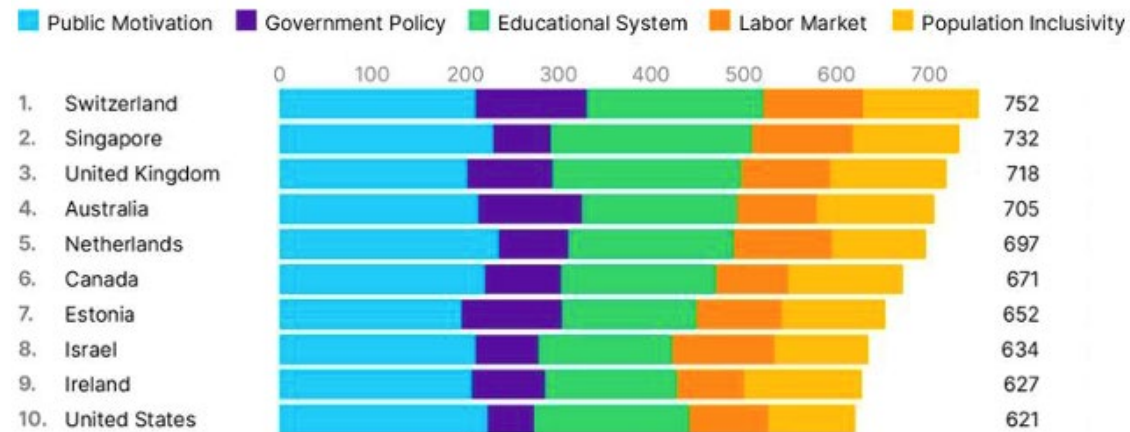
*Singapore (Republic of)*



Singapore also placed 2<sup>nd</sup> in Oliver Wyman Forum's Global Cyber Risk Literacy Index 2021, after Switzerland (See Figure 3). In comparison, Australia was ranked 4<sup>th</sup> and Germany 11<sup>th</sup>. The index aims to measure a population-wide average of cyber literacy across 50 geographies, including the EU. It examines five key drivers of cyber risk literacy and education:

1. Public motivation: Measures the population's commitment to practicing cybersecurity, including metrics such as the rate of adherence to specific cyber practices.
2. Government policy: Evaluates government policies to improve cyber risk literacy and education, including evaluation of metrics that assess the geography's national cybersecurity strategy.
3. Educational system: Measures the extent to which cyber risk instruction is encouraged or mandated, includes metrics that assess primary and secondary school curricula.
4. Labour market: Measures the degree to which employers drive demand for cyber literacy skills, including metrics such as the uptake of cybersecurity-related roles and the number of cybersecurity start-ups.
5. Population inclusivity: Measures degree of equal access to digital technologies and formal education in a geography, including metrics such as Internet access and school completion rates.

Figure 3. Top 10 countries in Global Cyber Risk Literacy Index, with weight driver scores



As evident in Figure 3, Singapore scores particularly well in the public motivation, educational system and labour market drivers, where it ranks 3<sup>rd</sup>, 1<sup>st</sup> and 2<sup>nd</sup> respectively. However, Singapore's weakest performance was in the government policy pillar, where it placed 19<sup>th</sup>. One reason may be the lack of "measurable and accountable goals" on cyber risk literacy and education in the country's national cybersecurity strategy.

Conversely, Singapore was ranked 31<sup>st</sup> in the e-Governance Academy's *National Cyber Security Index (NCSI) 2023*. Belgium, Lithuania and Estonia led the rankings, whereas Germany placed 5<sup>th</sup> and Australia 40<sup>th</sup>. By focusing on measurable cybersecurity aspects implemented by the government, the global index measures the preparedness of countries to prevent cyber threats and manage cyber incidents. Among the capacities examined, Singapore received the lowest scores for its protection of digital services (0 per cent) and military cyber operations (33 per cent). Table 6 below summarises the factors underlying Singapore's weaker performance on the two capacities:

Table 6. Breakdown of indicators that Singapore did not perform well in for the NCSI 2021

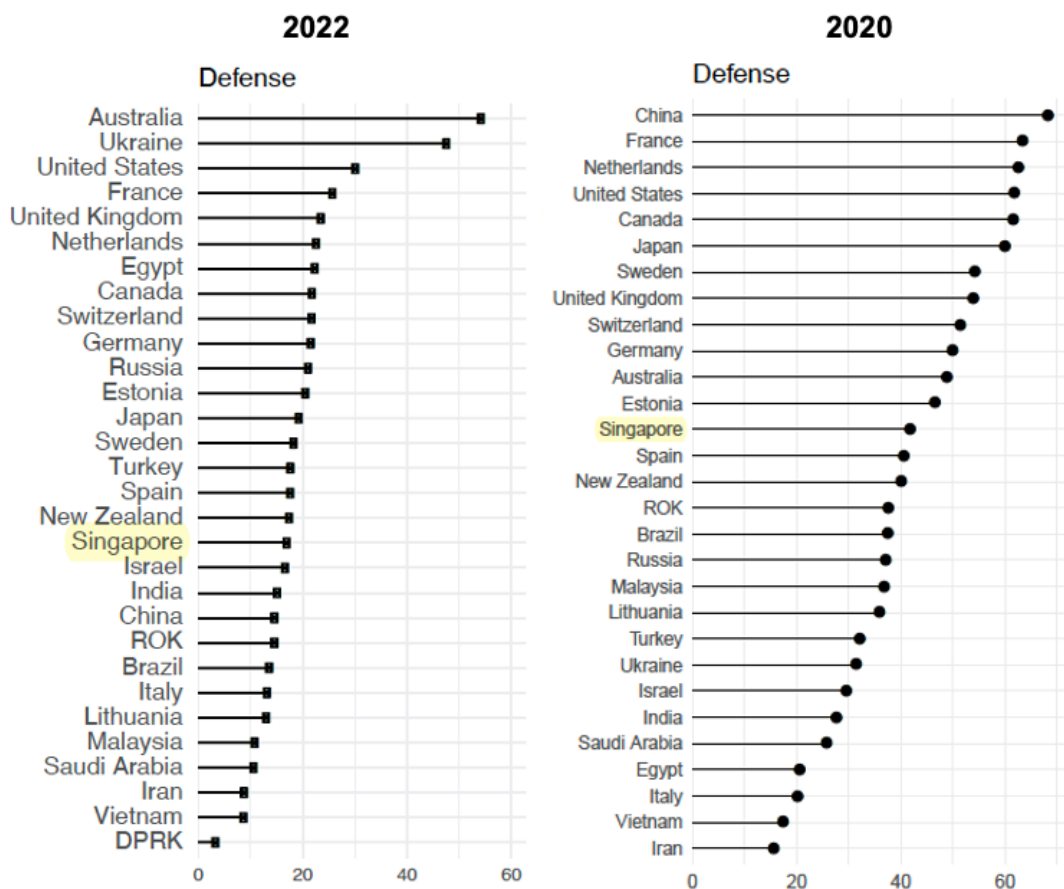
Capacity	Indicator
Protection of digital services	<ul style="list-style-type: none"> <li>No cyber security responsibility for digital service providers</li> <li>Lack of cyber security standard for the public sector</li> <li>No competent supervisory authority for public and private digital service providers.</li> </ul>
Cyber operations unit	<ul style="list-style-type: none"> <li>No cyber operations military unit</li> <li>Lack of participation in international cyber exercises in the last 3 years.</li> </ul>

However, Singapore's ranking on the *NCSI* was based on data last updated in October 2021, and hence it does not factor in subsequent policy developments in Singapore. Singapore has since established a cyber operations military unit, the Digital and Intelligence Service (Ministry of Defence [MINDEF], 2022). The Singapore government is also currently working on new cybersecurity legislation for digital service providers, or specifically what it refers to as foundational digital infrastructure and key digital services (Chee, 2022). This new legislation

would require online service and applications which are widely used to comply with government cybersecurity rules, similar to the requirements that CII's must adhere to.

Singapore also ranked 18<sup>th</sup> for the “strengthening and enhancing cyber defenses” objective of Belfer Center’s *National Cyber Power Index (NCPI) 2022* (See Figure 4). Australia and Germany both ranked above Singapore, placing at the 1<sup>st</sup> and 10<sup>th</sup> position respectively. The index compares 30 states based on the extent to which they have “prioritised enhancement of the defence of government and national assets and systems, and improved national cyber hygiene and resilience.” This includes measures to actively defend government assets, promote cybersecurity and cyber hygiene to key industries and the general population, and raise national awareness of cyber threats.

Figure 4. Ranking of 30 states on the “strengthening and enhancing cyber defenses” objective



Singapore’s 2022 rank (18) was a slight drop from its 2020 position (13). One key reason is that Singapore is relatively vulnerable to cyber threats — for example, due to its high percentage of ICT imports,<sup>18</sup> and its large proportion of citizens that use the Internet.<sup>19</sup> This has been corroborated by reports from Cybereason (Kurohi, 2022) and Check Point Research

<sup>18</sup> This is because, according to the NCPI, “the more information and communication technology that is imported, the market need for domestic solutions may decrease, and the state may incur higher supply chain risk within its domestic cyber infrastructure.”

<sup>19</sup> This is because, according to the NCPI, “more individuals on the Internet (in many cases) may result in a greater amount of the domestic populace vulnerable to foreign disinformation campaigns cybercrime or cyber espionage attempts.”

Team (2021) which highlight that Singapore is especially susceptible to cyber threats such as ransomware attack, as compared to its regional or even global peers. Another reason may be that although Singapore has a national cybersecurity strategy, its strategy does not include a detailed success criteria to assess the extent to which its goals are met.

## 4.2 Growing the digital economy

### 4.2.1 What Singapore has done in terms of the digital economy

Embracing the use of technology has long been a critical component of the Singapore government's development strategy (Chong, 2021). Since the late 1970s, the government recognised that the small island could not compete with its larger regional neighbours in labour intensive industries and determined that it should instead develop its competitive edge by concentrating on capital- and technology-intensive activities (Hioe, 2001; Tan, 1999). Consequently, the government has consistently undertaken concerted efforts to "become a world-class adopted of IT" (Tan & Zhou, 2018) — such as through its National Computerisation Plan in 1980,<sup>20</sup> the 1986 National IT Plan (NITP)<sup>21</sup> and the Intelligent Nation (iN2015) 10-year masterplan.<sup>22</sup> These efforts have been instrumental in developing and maintaining Singapore's reputation as a technology and communications hub (Chong, 2021).

At present, Singapore's most recent whole-of-nation digitalisation masterplan is its Smart Nation initiative launched in 2015 (Smart Nation and Digital Government Office [SNGDO], 2018).<sup>23</sup> Of particular relevance to this review is the Digital Economy pillar, which seeks to capitalise on the latest digital technologies to digitalise processes and promote business growth, as well as attract foreign investment to create new jobs and opportunities for Singaporeans (SNDGO, n.d.-a). The Digital Economy Framework For Action by the Infocomm and Media Development Authority (IMDA) (2018) further outlines the three key strategies for Singapore to develop a thriving digital economy:

1. To accelerate economic growth by digitalising industries and businesses.
2. To develop an ecosystem that promotes the vibrancy and competitiveness of businesses.
3. To transform the Infocomm Media industry to be a key growth driver of the Digital Economy.

---

<sup>20</sup> The five-year plan focused primarily on three areas: (i) embarking on a Civil Service Computerisation Programme (CSCP) to computerise the major functions in every government ministry, (ii) facilitating the growth and development of the local IT industry, and (iii) developing an IT talent pool to meet the future needs of the industry.

<sup>21</sup> The 10-year plan aims to transform Singapore into an "intelligent island" over the next 15 years, by capitalising upon rapidly advancing IT to deliver high-quality living and spearhead economic competitiveness.

<sup>22</sup> iN2015 consisted of four main objectives: (i) to establish an ultra-high speed, pervasive, intelligent and trusted infocomm infrastructure; (ii) to develop a globally competitive infocomm industry; (iii) to develop an infocomm-savvy workforce and globally competitive infocomm manpower; and (iv) to spearhead the transformation of key economic sectors, government and society through more sophisticated and innovative use of infocomm.

<sup>23</sup> The initiative outlines its vision of a "digital-first Singapore" where a Digital Government, Digital Economy, and Digital Society harness technology to transform health, transport, urban living, government services and businesses.

As part of the Smart Nation Initiative, the government has introduced a range of initiatives to support the digitalisation of Singaporean companies. SMEs, which employ 72 per cent of the workforce and account for 99 per cent of all enterprises in Singapore (Fu & Lim, 2022), have been a key target of governments initiatives. In 2017, the government launched the SMEs Go Digital programme, to help SME use digital solutions and strengthen their capacity to seize growth opportunities in the digital economy (IMDA, n.d.-a). By March 2022, more than 80,000 SMEs had adopted digital solutions under the programme (Teo, 2022a). Table 7 presents some of these solutions offered to SMEs.

Table 7. Key initiatives offered to SMEs

Name	Key details
<a href="#">Chief Technology Officer-as-a-Service (CTO-as-a-Service)</a>	SMEs can access CTO-as-a-Service, a one-stop platform allowing them to: <ol style="list-style-type: none"> <li>1. Perform a self-assessment of their digital readiness and identify their digitalisation needs and gaps</li> <li>2. Learn from other SMEs that have successfully implemented digitalisation projects</li> <li>3. Receive recommendations of digital solutions based on their business needs and profile</li> <li>4. Compare digital solutions, by functions and costs</li> </ol>
<a href="#">Grow Digital</a>	SMEs can participate in Business-to-Business (B2B) and Business-to-Consumer (B2C) e-commerce platforms to sell overseas without the need for a physical presence.
<a href="#">Advanced Digital Solutions (ADS)</a>	SMEs can adopt advanced technologies (e.g., AI, Robotics, Blockchain and Internet of Things), and integrated digital solutions (e.g., B2B solutions that integrate inventory management, e-invoicing and digital payments) that address common enterprise-level challenges at scale.

However, despite the various initiatives available, supporting the digitalisation of SMEs has been not without its challenges. In fact, a joint study by Boston Consulting Group (BCG) and IMDA found that more than 60 per cent of Singaporean SMEs are still digital starters. In contrast, the figure was less than 20 per cent for large companies (Chan, 2022). To address this gap, the Rapid and Immersive Skill Enhancement (Rise) for Business programme was launched in September 2022. Under the programme, SMEs can work directly with BCG to identify their digital business challenges and related skills gaps. After which, their employees will be placed in one of three tracks, where they will learn and apply the necessary digital skills under the guidance of industry experts and practitioners.

Singapore has also sought to maximise the potential of data as a strategic asset in its digital economy, while ensuring that security and privacy is safeguarded (Lim, 2019; Prime Minister's Office Singapore [PMO], 2019). This has included efforts to increase data sharing across the nation. First, the government has been promoting a cultural shift away from individuals being mere consumers to active co-creators and contributors of data. For instance, the public can harness data sets collected by public agencies through online platforms like [data.gov.sg](#), which is a one-stop portal to publicly available datasets from 70 public agencies (SNDGO, n.d.-b). In cases where there is public interest and benefit to Singapore and Singaporeans,

the government has also facilitated the sharing of government-verified data with the private sector (SNDGO, 2018). One example is the Myinfo platform, a service which allows businesses to retrieve the personal data of Singapore citizens and residents from government data bases, thus completing the “Know-Your-Customer” (KYC) process without the need for customers to provide additional verification documents (Government Technology Agency [GovTech], n.d.).

#### 4.2.2 Singapore’s performance on digital economy indices

Singapore has ranked highly on indices assessing the competitiveness of countries’ digital economy. Firstly, the country placed 4<sup>th</sup> on the IMD’s *World Digital Competitiveness Ranking (WDC) Ranking 2022* (See Table 8), ahead of both Australia (14) and Germany (19). The ranking analysed and ranked 63 countries based on the extent to which they adopt and explore digital technologies leading to transformation in government practices, business models and society in general. It examined countries according to three main factors, which are each divided into three sub-factors:

1. Knowledge: Know-how necessary to discover, understand and build new technologies — comprising talent, training and education, and scientific concentration.
2. Technology: Overall context that enables the development of digital technologies — comprising regulatory framework, capital, and technological factors.
3. Future readiness: Level of country preparedness to exploit digital transformation — comprising adaptive attitudes, business agility, IT integration.

Table 8. Top 10 countries in WDC 2022

Rank	Country	Score	Change from 2021 score
1	Denmark	100.00	+3
2	US	99.81	-1
3	Sweden	99.81	0
4	Singapore	99.48	+1
5	Switzerland	98.23	+1
6	Netherlands	97.85	+1
7	Finland	96.60	+4
8	South Korea	95.20	+4
9	Hong Kong	94.36	-7
10	Canada	94.15	+3

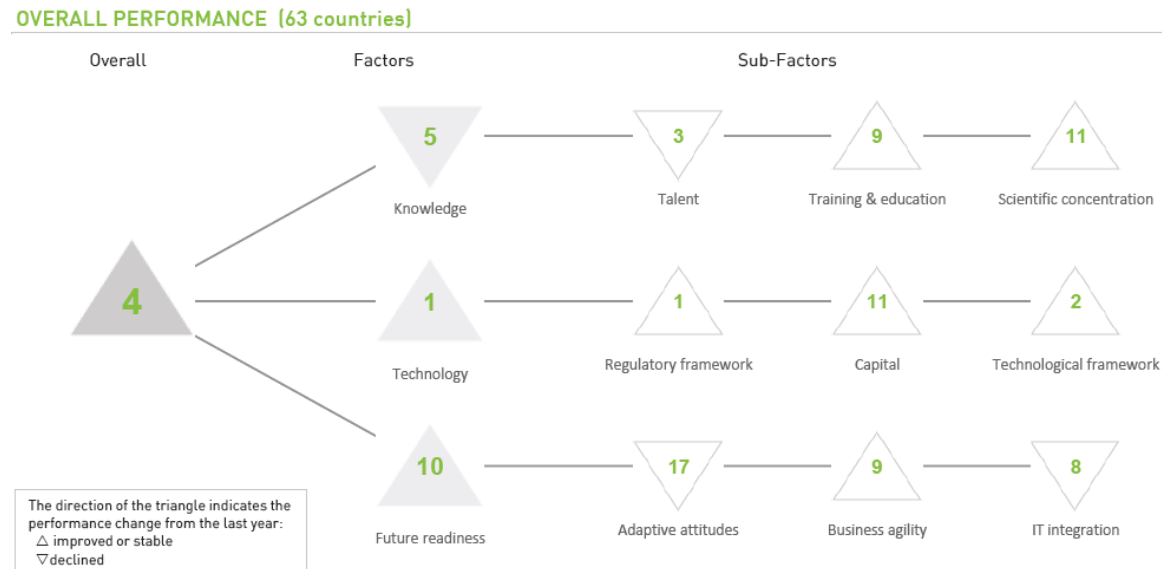
Singapore’s 2022 rank was a slight improvement from its 2021 ranking of 5<sup>th</sup> place. The country topped the technology factor (See Figure 5), primarily due to gains in the regulatory framework<sup>24</sup> and technological framework sub-factors.<sup>25</sup> Specifically, Singapore scored highly

<sup>24</sup> The regulatory framework sub-factor is based on the following indicators: Starting a business, Enforcing contracts, Immigration laws, Development and application of tech, Scientific research legislation, and Intellectual property rights.

<sup>25</sup> The technology framework sub-factor is based on the following indicators: Communications technology, Mobile Broadband subscribers, Wireless broadband, Internet users, Internet bandwidth speed, and High-tech exports.

for its ease of starting a business (3),<sup>26</sup> enforcing contracts (1)<sup>27</sup> and Internet bandwidth speed (1).

Figure 5. Breakdown of Singapore's performance on the WDC 2022



However, Singapore's key weaknesses were in its number of female researchers (42) and immigration laws (43). Firstly, Singapore was observed to have a smaller proportion of female researchers mainly or partially employed in research and development (R&D). In fact, the Main Science and Technology Indicators by the Organisation for Economic Co-operation and Development (OECD) indicates that the number has hovered at approximately 30 per cent between 2015 to 2019. Meanwhile, Singapore's poorer score on immigration laws may be attributed to its tightening of foreign worker policies over recent years to promote local employment, such as by raising the minimum qualifying salaries for new Employment Pass (EP) and S Pass applicants (Mahmud, 2022).

As for Portulans Institute's *Network Readiness Index (NRI) 2022*, Singapore obtained the second highest position (See Figure 6). Germany and Australia placed below Singapore at the 8<sup>th</sup> and 14<sup>th</sup> rank respectively. The NRI assessed 131 countries across various components of digital readiness, through the use of four pillars:

1. Technology: Assesses the level of technology that is a sine qua non for a country to participate in the global economy, based on three sub-pillars: (i) access, (ii) content and (iii) future technologies.
2. People: Measures how people apply ICT at three levels of analysis: (i) individuals, (ii) businesses and (iii) governments.
3. Governance: Concerns the establishment and accessibility of systems that promote activity within the network economy across three levels: (i) trust, (ii) regulation and (iii) inclusion.

<sup>26</sup> Taken from the World Bank's *Doing Business 2020*, the starting a business indicator considers the procedures, time, cost and paid-in minimum capital needed to start a limited liability company.

<sup>27</sup> Taken from the World Bank's *Doing Business 2020*, the enforcing contracts indicator considers the time and cost needed to resolve a commercial dispute and the quality of judicial processes.



4. Impact: Assesses the economic, social and human impact of participation in the network economy across three levels: (i) economy, (ii) quality of life and (iii) Sustainable Development Goals (SDG) contribution.

Figure 6. Top 10 countries in NRI 2022

Country	NRI rank	NRI score	Pillars			
			Technology	People	Governance	Impact
United States	1	80,30	1	2	7	20
Singapore	2	79,35	4	4	10	2
Sweden	3	78,91	8	5	5	1
Netherlands	4	78,82	3	14	4	4
Switzerland	5	78,45	2	11	12	5
Denmark	6	78,26	11	7	2	7
Finland	7	77,90	13	6	3	3
Germany	8	76,11	7	9	14	8
Korea, Rep.	9	75,95	14	1	22	13
Norway	10	75,68	12	12	1	14

In the *NRI 2022*, Singapore moved up five positions to earn a place among the top five for the first time since 2020. The country performed particularly well on the Technology, People and Impact pillars (See Figure 6). Specifically, Singapore ranked highly for its wide-sweeping access and adoption of future technologies (2),<sup>28</sup> and the impact of network technologies on the overall Economy (3).<sup>29</sup>

But despite Singapore's strong overall performance, there are still areas for improvement. Notably, under the Governance pillar, the country obtained a low score for the gender gap in Internet use indicator where it placed 54<sup>th</sup>. Similarly, under the Impact pillar, the country obtained its poorest score for the women's economic opportunity indicator (65)<sup>30</sup> — suggesting a lack of legal equality between working men and women.

## 4.3 Facilitating cross-border data flows

### 4.3.1 What Singapore has done to enhance cross-border data flows

As one of the most globally connected countries in the world, encouraging the free flow of data across borders has been a significant priority of the Singapore government. Its importance was articulated by Yeong Zee Kin, Deputy Commissioner of the Personal Data Protection Commission (PDPC), who emphasised that “data flows are foundational to the digital economy, and there has never been a more compelling time for economies to build common

<sup>28</sup> Future technologies, which is a sub-pillar of the Technology pillar, comprises the following components: Adoption of emerging technologies, Investment in emerging technologies, Robot density and Computer software spending.

<sup>29</sup> Economy, which is a sub-pillar of the Impact pillar, comprises the following components: High-tech and medium-high-tech manufacturing, High-tech exports, PCT patent applications, Domestic market size, Prevalence of gig economy, and ICT services exports.

<sup>30</sup> Women's economic opportunity indicator is based on the Women, Business and Law Index 2020. The index assesses laws and regulation on women's economic partnership based on eight areas: Mobility, Workplace, Pay, Marriage, Parenthood, Entrepreneurship, Assets and Pensions.



standards and principles together, to allow data to flow smoothly and safely across borders” (Yeong, 2021).

As such, Singapore has maintained a long-standing policy against data localisation.<sup>31</sup> Instead, the country seeks to maintain a “balanced approach”, one that enables the cross-border flow of data while ensuring that appropriate safeguards to protect individuals are in place (Teo, 2022b). For instance, Singapore’s PDPA (See Sub-section 4.4 for more details on the act) allows personal data to be transferred outside of Singapore if certain prescribed conditions are met (Wong, 2020).<sup>32</sup> Singapore is also exploring innovative domestic initiatives to facilitate the trusted flow of data across borders (See Table 9 for examples).

*Table 9. Initiatives to facilitate cross-border data flows*

Name	Key details
<a href="#">Privacy Enhancing Technologies (PETs) Sandbox</a>	Enables companies who wish to experiment with PETs to work with trusted PET digital solution providers to develop use cases and pilot PETs.
<a href="#">Singapore Trade Data Exchange (SGTraDex)</a>	A public digital infrastructure that aims to allow data connection to be made to a wide range of data contributors and data users within Singapore and across the world. It functions as a “Data Highway” that allows for the streamlined and rapid transfer of encrypted information between willing and consenting parties.

Singapore has also placed a strong emphasis on inter-governmental cooperation. One of the country’s most renown initiatives is its digital economy agreements (DEAs), which have been lauded as “innovative” and “comprehensive” agreements that establish trade rules and facilitate interoperability between Singapore and other digital economies (Warren & Fan, 2022). At present, Singapore has signed four DEAs (MTI, n.d.-a):

1. The Digital Economy Partnership Agreement (DEPA) with Chile and New Zealand
2. The Singapore-Australia Digital Economy Agreement (SADEA)
3. The United Kingdom-Singapore Digital Economy Agreement (UKSDEA)
4. The Korea-Singapore Digital Partnership Agreement (KSDPA)

DEAs can be understood as somewhat bespoke, as they may differ in their specific details and processes with regards to enforcing and enhancing them (Tay & Wu, 2022). Nonetheless, Singapore’s DEAs generally contain many similar features.<sup>33</sup> They seek to address barriers

<sup>31</sup> For instance, in a joint statement with the US Treasury Department in 2020, the MAS asserted that “data localisation requirements can increase cybersecurity and other operational risks, hinder risk management and compliance, and inhibit financial regulatory and supervisory access to information.” For the full statement, refer to MAS (2020).

<sup>32</sup> These conditions seek to ensure that “organisations provide a standard of protection to personal data so transferred that is comparable” to the protection conferred by the PDPA. Information taken from Wong (2020).

<sup>33</sup> The MTI’s website includes a list of “modules”, or policy areas for alignment, which are included in some or all of Singapore’s DEAs. This includes the facilitation of initiatives that promote compatibility between different digital identity regimes, prohibiting the localisation of data except for legitimate

such as data localisation and fragmented data protection laws, by establishing common frameworks and rules for digital trade that enable Singaporean companies to connect more easily and efficiently with their overseas partners (MTI, n.d.-a).

The success of DEAs has been evident by the fact that other countries have shown an interest in entering such an agreement. For instance, China officially applied to join the DEPA in 2021 (Elms, 2021b), while Canada, Japan and South Korea have also expressed their interest in joining the agreement (Heisler, 2021). At the time of writing, Singapore was also in the midst of negotiating a DEA with the European Free Trade Association (EFTA) (MTI, 2023).

[Jeff Paine on the strength of DEAs] “Digital economy agreements are becoming a lot more important because the data principles in those agreements are really important to provide safety. So, it gives the local government of whatever country the safety and assurance to know that their citizens will have a safe online environment. So having these established rules, and I think that’s what the EU is trying to do.”

In addition, Singapore has also pursued notable regional trade agreements (FTAs) to reduce barriers to digital trade. It signed the Comprehensive Progressive Agreement for Trans-Pacific Partnership (CPTPP) in 2018, alongside ten other Asia-Pacific Economic Cooperation (APEC) members including Australia, Mexico and Canada (MTI, n.d.-b). Its key features include provisions restricting data localisation and the imposition of requirements on the cross-border transfer of data.<sup>34</sup> Singapore is also part of the Regional Comprehensive Economic Partnership (RCEP) Agreement signed in 2020, which is the world’s largest FTA comprising approximately 30 per cent of the global economy (MTI, n.d.-c). While RCEP’s provisions regarding cross-border data flows are based on the CPTPP framework, it provides more flexibility for members to introduce restrictive measures necessary for “essential security interests” or “legitimate public policy objective(s)”.<sup>35</sup> Figure 7 below provides an overview of the members of the CPTPP and RCEP.

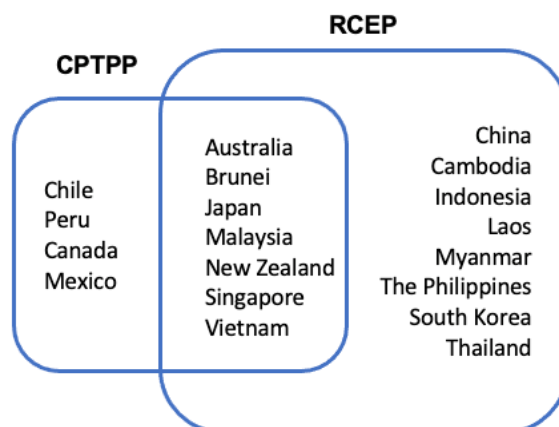
---

purposes, and enabling interoperability of payment systems. Taken from <https://www.mti.gov.sg/Trade/Digital-Economy-Agreements>.

<sup>34</sup> Article 14.11 of the CPTPP establishes that while each party may have its own regulatory requirements for cross-border data flows, in principle, the cross-border transfer of information by electronic means should be permitted. The only exception is for special circumstances, such as to achieve legitimate public policy goals. But these exceptional measures should not be arbitrary, discriminatory, or disguised, and must pass a necessity test. Information taken from Chin & Zhao (2022).

<sup>35</sup> RCEP includes prohibitive provisions on data localisation, such as Article 14(2) of Chapter 12 which states that “no Party shall require a covered person to use or locate computing facilities in that Party’s territory as a condition for conducting business in the Party’s territory.” However, Chapter 12 also includes exception clauses for “any measures necessary to achieve a legitimate public policy objective” or “essential security interests”.

Figure 7. Members of the CPTPP and RCEP



[Jeff Paine on Singapore's strengths] "Singapore is very forward-looking by being members of CPTPP, being members of RCEP, which are two big multilateral trade deals. I don't know of any country that has more digital economy agreements than Singapore."

ASEAN has also been an important platform through which Singapore has sought to enhance cross-border regional data flows. For example, the country led efforts to develop the ASEAN Framework on Digital Data Governance, which was endorsed in 2018 (SNDGO, 2018). The framework outlines the strategic priorities, principles and initiatives to guide member states in their policy and regulatory approach towards data, which are depicted in Figure 8 below. One of these initiatives included the development of an ASEAN Cross Border Data Flows Mechanism, and ASEAN has since published the ASEAN Model Contractual Clauses (MCCs) for Cross Border Data Flows (ASEAN, 2021).<sup>36</sup>

Figure 8. ASEAN Framework on Digital Data Governance

	Data Life Cycle and Ecosystem		Cross-Border Data Flows		Digitalisation and Emerging Technologies		Legal, Regulatory, and Policy
<b>Outcomes:</b>	<ul style="list-style-type: none"> <li>Data governance through the data lifecycle (e.g. collection, use, access, storage)</li> <li>Adequate protection for different types of data</li> </ul>	<b>Outcomes:</b>	<ul style="list-style-type: none"> <li>Business certainty on cross-border data flows</li> <li>No unnecessary restrictions on data flows</li> </ul>	<b>Outcomes:</b>	<ul style="list-style-type: none"> <li>Data capacity (infrastructure and skills) development</li> <li>Leveraging new technologies</li> </ul>	<b>Outcomes:</b>	<ul style="list-style-type: none"> <li>Harmonised legal and regulatory landscapes in ASEAN (including personal data protection)</li> <li>Development and adoption of best practices</li> </ul>
<b>Initiative:</b>	<ul style="list-style-type: none"> <li>ASEAN Data Classification Framework</li> </ul>	<b>Initiative:</b>	<ul style="list-style-type: none"> <li>ASEAN Cross-Border Data Flows Mechanism</li> </ul>	<b>Initiative:</b>	<ul style="list-style-type: none"> <li>ASEAN Digital Innovation Form</li> </ul>	<b>Initiative:</b>	<ul style="list-style-type: none"> <li>ASEAN Data Protection and Privacy Forum</li> </ul>

<sup>36</sup>The MCCs are templates that outline the responsibilities, required personal data protection measures and related obligations of parties transferring personal data across borders between ASEAN member states. Its use is voluntary and helps ensure that the transfer of personal data is done in a manner that complies with the ASEAN member states' legal and regulatory requirement and protects the data of Data Subjects based on the principles of the 2016 ASEAN Framework on Personal Data Protection.

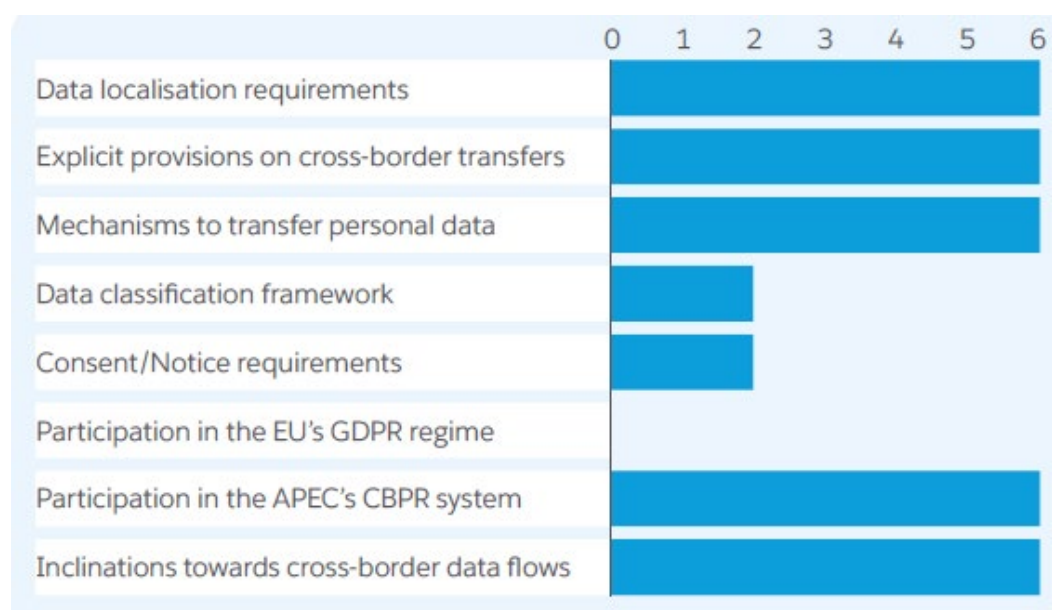
### 4.3.2 Singapore's performance on cross-border data flows indices and benchmarks

Singapore ranked 3<sup>rd</sup> on the Salesforce's *Cross-Border Data Flows Index (CBDFI) 2021*, with a score of 34 points. Only Japan and the UK scored higher, while Australia and Germany tied at 7<sup>th</sup> place with 30 points each. The index quantified and evaluated eight regulatory dimensions that either restrict or enhance the volume and variety of cross-border data flows for G20 economies. The eight dimensions assessed were:

1. Data localisation requirements which can limit the import and export of foreign-sourced data processing and data-storage services.
2. Explicit provisions allowing for international or extraterritorial transfers of personal data.
3. Existence of specific mechanisms by which personal data is allowed to be transferred.
4. Presence of a data classification framework which enables cross border data flows.
5. Consent requirements for the cross-border collection, storage, and dissemination of personal data.
6. Participation in the EU's GDPR regime, or meeting GDPR adequacy requirements.
7. Participation in the APEC Cross Border Privacy Rules (CBPR) or similar regional system.
8. Whether a government has offered indications of being favourably or unfavourably positioned on supporting cross-border data flows.

Singapore received perfect scores in five of the dimensions (see Figure 9). The country was praised for its strong data protection regulation and guidelines, yet open and forward-looking approach to enabling the secure and seamless flow of data across borders. For instance, Singapore's PDPA does not impose any overarching data localisation requirements and provides transparent and consistent rule for businesses transferring data outside of Singapore.

Figure 9. CBDFI 2021 score for Singapore



However, Singapore scored less well on three dimensions. Firstly, Singapore does not have a data classification framework specifically for enabling cross-border data flows. Another weakness was the area of consent/notice requirements, specifically, that businesses which choose to rely on consent for transferring personal data must provide the individual with a “reasonable summary in writing of the extent to which [their] data... will be protected to a standard comparable to the protection under the PDPA” (PDPC, 2017). This was deemed as a practically challenging requirement, as businesses may struggle to provide such detailed information given that recipient countries may differ in their regulation of personal data (Asian Business Law Institute, 2020). Lastly, Singapore also lost points as it does not meet GDPR adequacy requirements.

## 4.4 Protecting citizens’ data and privacy

### 4.4.1 What Singapore has done in terms of data privacy and protection

The Singapore government has employed a range of initiatives to protect its citizens’ data and privacy. The PDPC is Singapore’s main authority on personal data protection in the private sector, which was established in January 2013 (PDPC, n.d.-a).<sup>37</sup> It also represents Singapore internationally on data protection-related affairs. Notably, the primary objective of the PDPC is to administer and enforce the PDPA, which is Singapore’s principal data protection legislation, consisting of various requirements governing the collection, use, disclosure, and care of personal data by any private “organisation” in Singapore (PDPC, n.d.-b). It also applies to organisations without any physical presence in Singapore, so long as they collect, use, or disclose data within Singapore (DLA Piper, n.d.). The PDPA was later amended in November 2020 (PDPC, n.d.-b), with additions such as a mandatory data breach notification requirement, and three new offenses for the mishandling of personal data (Lui et al., 2022).

Alongside its domestic initiatives, the Singapore government has also undertaken bilateral and multilateral efforts to enhance the personal data protection of its citizens, an approach that is consistent with its emphasis on collaboration and cooperation. The PDPC has signed MOUs with data protection authorities from several countries, including The Philippines (PDPC, 2019), Hong Kong (PDPC, 2022), as well as the UK (DataGuidance, 2020). Singapore also joined the APEC CBPR System (APEC Electronic Commerce Steering Group, 2018) and APEC Privacy Recognition for Processors (PRP) System (IMDA, n.d.-b) in 2018. The systems require participating companies to demonstrate their ability to implement data privacy policies in accordance with the APEC Privacy Framework (IMDA, n.d.-b). By joining these systems, Singaporean companies can transfer personal data to overseas certified recipients without needing to meet additional requirements, and vice-versa.

### 4.4.2 Singapore’s performance on data protection and privacy indices

Singapore ranked highly on two indices pertaining to cybersecurity. In TRPC’s *Data Protection Index (DPI) 2020*, Singapore placed joint 4<sup>th</sup> with a score of 9.2, sharing its position with Germany, Australia, Estonia, Mexico, and the UK. The *DPI 2020* assessed 30 economies’

---

<sup>37</sup> Its functions include the implementation of policies regarding personal data protection, conducting educational and outreach activities, and overseeing Singapore’s Do Not Call Registry.

data protection laws and regulatory environment, based on the seven principles of personal data protection in the 2016 ASEAN Framework of Personal Data Protection:

1. Consent, Notification and Purpose
2. Accuracy of Personal Data
3. Security Safeguards
4. Access and Correction
5. Transfers to Another Country or Territory
6. Retention
7. Accountability

Singapore was the highest scoring ASEAN state in the *DPI 2020*, which was attributed to its strong data protection law and well-established data protection agency. However, Singapore failed to obtain a perfect score because it did not meet GDPR adequacy requirements. This means that Singapore has not undergone an adequacy decision and is thus not formally recognised by the European Commission as providing an equivalent level of protection for personal data as the EU does (ICO, n.d.-b). Being recognised as adequate would mean that personal data can flow from the EU to a third country without the need for further safeguards, whereby the third country would be essentially assimilated into intra-EU transmissions of data (European Commission, n.d.-a).

Singapore also obtained a perfect score of 5 on DataGuidance's *Privacy Index*, indicating a comprehensive overall data protection framework. The index identifies and compares the principal data protection requirements across countries, based on a range of topics including DPO appointment, data transfers and security controls. Singapore received high scores for its implementation of data subject rights, establishment of restrictions and mechanisms regarding data transfers without localisation requirements, and detailed requirements for technical and organisational security measures (e.g., encryption, pseudonymisation). Conversely, Singapore was noted as having generic or basic, rather than detailed, requirements for when Data Protection Impact Assessments are required, the content of assessments, and prior consultation with the relevant authority.

In the Global Web Index's *Data Confidence Index 2019*, Singapore obtained a score of 1.5, one of the highest scores in the ranking (See Table 10). In comparison, Australia received a higher score of 1.6, whereas Germany a lower score of 1.3. The index is a measure of expressed privacy concerns against online behaviours, whereby the higher the index number for a country, the less likely Internet users in that country are confident in acting on their privacy concerns online by engaging in privacy behaviours, and vice-versa. Results were drawn from online questionnaires with 391,130 Internet users aged 16 to 64 across 45 markets.

Table 10. Markets with the highest and the lowest scores in the Data Confidence Index 2019

Most data-confident markets (i.e., Markets with the 3 lowest scores)		Least data-confident markets (i.e., Markets with the 3 highest scores)	
Market	Score	Market	Score
Sweden	0.6	Taiwan	1.9
Indonesia	0.9	Spain	1.9
Austria	1.1	Russia	1.8
Brazil	1.1	Japan	1.8
Denmark	1.1	Hong Kong	1.8
Romania	1.1	Australia	1.6
Saudi Arabia	1.1		
Switzerland	1.1		
Thailand	1.1		
Vietnam	1.1		

The index suggests that there is a discrepancy between Singapore Internet users' concerns and their actions towards online privacy. Specifically, Singaporeans consistently reported relatively high levels of (i) concern over company use of personal data,<sup>38</sup> (ii) desire for anonymity online,<sup>39</sup> and (iii) concern over the Internet eroding personal privacy.<sup>40</sup> Similar results were found in studies by YouGov (Tan, 2023) and Wirecard and Blackbox (2020), which observed that most Singaporeans are concerned about how their personal data is being collected and used.

However, the index indicates that Singaporeans are not acting in accordance with their high levels of privacy concerns. The index found that 23 per cent of Singaporean respondents did not engage in any online privacy behaviour such as deleting cookies or using an ad-blocker. This disconnect between attitudes and behaviour was also apparent in a recent OpenText study (Data&Storage ASEAN, 2022). Specifically, while 85 per cent of Singaporeans know how to keep their data secure on applications, email accounts, and social media, less than half regularly check to ensure that they are following data privacy and security best practices, for instance, switching off geo-location, or turning on privacy settings.

## 5. Safeguarding Singapore's digital future

This last section examines how Singapore can safeguard its future in an increasingly fragmented global landscape. It does so by considering how Singapore can strike the intricate balance between safeguarding its own national interests and maximising the benefits of a

<sup>38</sup> The average agreement score for the statement "I worry about how my personal data is being used by companies" was 1.3 amongst Singaporean respondents, the 4<sup>th</sup> highest score amongst the 45 markets. Only eight markets obtained a higher average agreement score.

<sup>39</sup> The average agreement score for the statement "I prefer to be anonymous when using the Internet" was 1.2 amongst Singaporean respondents, the highest score amongst the 45 markets. Only one other market, Poland, obtained the same score.

<sup>40</sup> The average agreement score for the statement "I am concerned about the Internet eroding my personal privacy" was 1.2 amongst Singaporean respondents, the 2<sup>nd</sup> highest score amongst the 45 markets. Only one country, Taiwan, obtained a higher agreement score.

connected digital space. The recommendations adopt an ecosystem approach, examining the measures that can be adopted at different levels — specifically, at the level of the individual, the organisation, the nation and the region.

## 5.1 At the individual level

### 5.1.1 Increasing vigilance and care among Singaporeans

At the individual level, one key gap that needs to be addressed is the inadequacy of data protection and privacy practices amongst Singaporeans. For instance, a Google study found that while nearly 60 per cent of Singaporean Internet users have experienced a personal data breach or know someone who has, the vast majority (94 per cent) still admitted to practising poor password habits (Wong, 2021). Likewise, passive or complacent attitudes among some Singaporeans was also observed in the CSA's nation-wide Cybersecurity Awareness Survey 2020 (Chee, 2021b). For instance, the survey found that while most Singaporeans were concerned that their financial information would be obtained by others without their consent, only 40 per cent thought it was somewhat or extremely likely to happen to them (Chee, 2021b). This phenomenon is known as the privacy paradox, whereby users claim to be very concerned about their privacy yet do very little to actually protect their personal data (Barth & de Jong, 2017).

As insufficient awareness does not appear to be the primary issue, there is a need for policymakers to explore other avenues of promoting a culture of care and vigilance towards personal data among Singaporeans. One avenue that may provide new insights is to examine the psychological processes underlying individuals' behaviour, such as those outlined in the Theory of Planned Behaviour (Ajzen, 1991). The theory posits that intentions are a key indicator of whether an individual will perform a particular behaviour. Intentions are in turn determined by three factors: (i) attitude toward the behaviour, (ii) subjective norm, and (iii) perceived behavioural control. Subjective norms refer to the perceived social pressure individuals experience to perform or not perform a specific behaviour (Ajzen, 1991). Numerous empirical studies have highlighted that subjective norms may be an important predictor of individuals' intention to engage in behaviours that safeguard their personal data and privacy (e.g., Fan et al., 2020; Foltz et al., 2016; Martens et al., 2019; Alanazi et al., 2022). For example, a study by Schmidt et al. (2022) found that subjective norms<sup>41</sup> regarding the use of Twitter's options to increase user privacy were direct predictors of Twitter users' intentions to use these options. Hence, policymakers can explore implementing awareness campaigns that emphasise subjective norms regarding data protection and privacy behaviours.

At present, national awareness campaigns in Singapore seem to be more focused on increasing knowledge about cyber threats and providing Singaporeans with information on what they should do. For instance, the CSA's recent "Better Cyber Safe than Sorry" campaign emphasised four practices, such as the use of a strong password, which would safeguard

---

<sup>41</sup> Subjective norms were assessed through four items, whereby participants indicated the extent of their agreement using a 7-point scale. Examples of items included "I believe that most people who are important to me think that I should make use of the privacy options of Twitter" and "most people I respect and admire use one or more of the options, on Twitter, to improve their privacy."



Singaporeans against personal data breaches (CSA, 2021). Figure 10 depicts the posters that were used for the campaign:

Figure 10. Posters from the “Better Cyber Safe than Sorry” campaign



To augment the effectiveness of national campaigns in fuelling behaviour change, policymakers could consider emphasising subjective norms surrounding data protection and privacy. Table 11 provides examples of the types of messages that the campaign can incorporate.<sup>42</sup>

Table 11. Examples of messages using subjective norms

Type of messaging	Possible applications
Provide information about others' behaviour	Indicate the extent to which others perform a particular data protection and privacy behaviour.
Provide information about others' approval	Provide information about how others could judge or approve of an individual's data protection and privacy behaviour.  Emphasise the societal expectation that individuals should take responsibility of their own personal data.
Provide opportunities for social comparison	Provide examples of individuals with positive or negative data protection and privacy behaviour.

Alongside the exploration of different types of messages, it is also important to constantly assess the effectiveness of national awareness campaigns. Such evaluations may be highly complex, expensive, and would require considerable access to the target population. (McCulloch & Watts, 2021) However, such an endeavour is important to assess the outcomes of previous awareness campaigns and enhance the effectiveness of subsequent ones.

<sup>42</sup> The table is adapted from the behaviour change techniques used by Kothe et al. (2012)

## 5.2 At the organisational level

### 5.2.1 Introducing differentiated levels of digitalisation support for SMEs

At the organisation level, one important gap is the uneven levels of digitalisation among Singapore companies, where a disproportionate number of SMEs have remained digital starters compared to their larger counterparts. However, the government has in fact introduced a wide range of funding schemes and programmes to support technology adoption, particularly among SMEs. Hence, there is a need to identify and address the barriers which may be hindering the adoption or effectiveness of existing government initiatives.

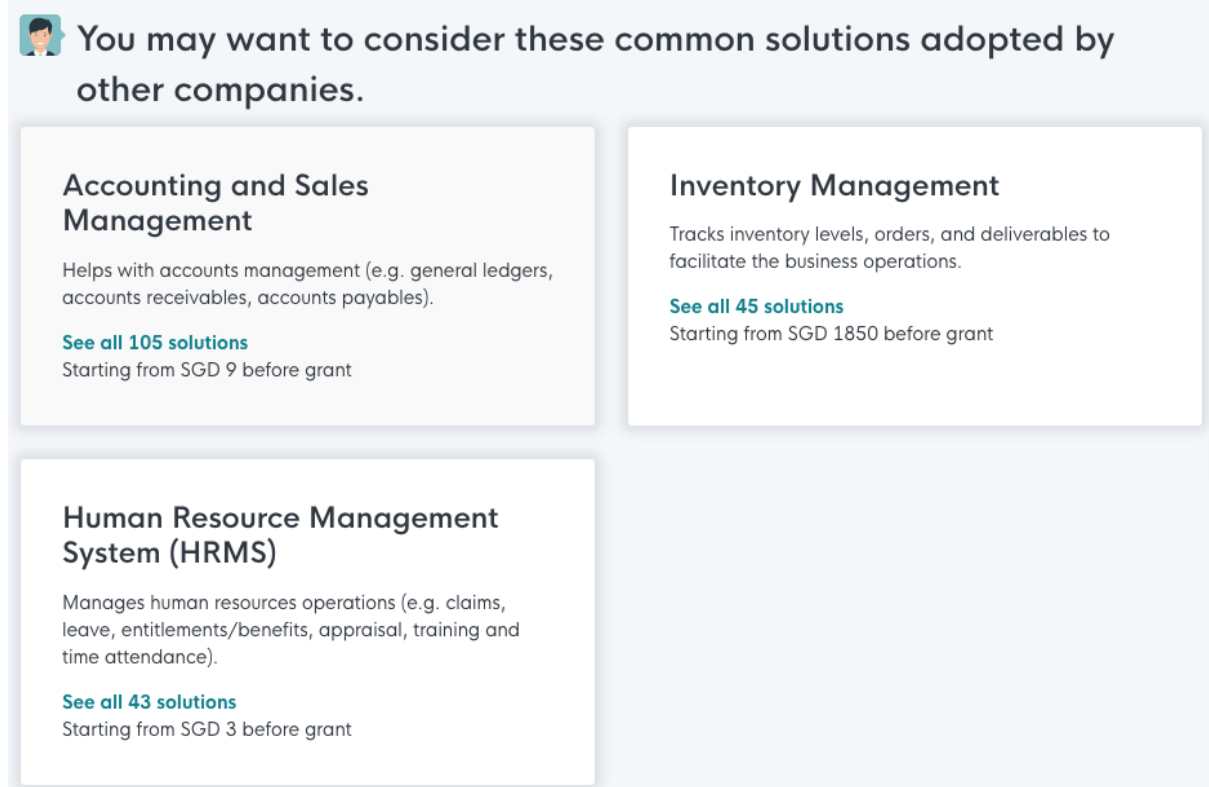
One reason which may be hindering SMEs' uptake is decision fatigue, particularly for those at the start of their digitalisation journeys. SMEs may find themselves inundated with a wide range of schemes available and lack the necessary knowledge or confidence to select the appropriate programmes or digital solutions. For instance, a study conducted by United Overseas Bank (UOB) (2022a) found that only 43 per cent of SMEs that had leveraged digital technologies felt they had achieved considerable or complete success. One reason for this may be that SMEs are not choosing suitable schemes or technologies. Decision fatigue may even deter some SMEs from utilising the schemes available. This may partially explain findings by QBE Insurance (2023) that although most SMEs (89 per cent) reported being aware that government support packages and initiatives were available, only half actually applied for them.


The Singapore government has attempted to provide SMEs with greater guidance when selecting digital solutions. In particular, through the CTO-as-a-Service programme, SMEs are able to perform a Digital Readiness Self-Check, after which they will be recommended different types of digital solutions (see Figure 11 for an example). However, given that there are more than 400 digital solutions and software available under the programme (IMDA, n.d.-c), some SMEs may still be overwhelmed by the range of solutions they are recommended. It should be noted that the CTO-as-a-Service programme does provide digital consultancy services at no cost to eligible SMEs, whereby they can access a digital consultant to advise them on selecting and implementing the optimal digital solution. However, the complementary digital consultancy service is restricted to a single use by SMEs.<sup>43</sup> This could limit the effectiveness of the programme as some SMEs may require more extensive and longer-lasting guidance. Such a need may be greater for smaller SMEs, which are more limited in terms of finances and manpower. For instance, the same UOB study found that among smaller SMEs — those with an annual sales turnover of less than \$1 million — only one quarter reported success in its digital adoption journey (UOB, 2022b). Hence, smaller SMEs may require greater levels of support, such as more opportunities to access the digital consultancy services, given that they likely lack the in-house knowledge or finances to afford such services.

---

<sup>43</sup> The eligibility criteria for digital consultancy services requires the business to have “not used the services of CTO-as-a-Service digital consultancy previously.” Refer to <https://services2.imda.gov.sg/CTOaaS/Consultants> for more information.

Figure 11. Example of the solutions recommended for a food manufacturing SME with low levels of digital readiness



 **You may want to consider these common solutions adopted by other companies.**

### Accounting and Sales Management

Helps with accounts management (e.g. general ledgers, accounts receivables, accounts payables).

[See all 105 solutions](#)  
Starting from SGD 9 before grant

### Inventory Management

Tracks inventory levels, orders, and deliverables to facilitate the business operations.

[See all 45 solutions](#)  
Starting from SGD 1850 before grant

### Human Resource Management System (HRMS)

Manages human resources operations (e.g. claims, leave, entitlements/benefits, appraisal, training and time attendance).

[See all 43 solutions](#)  
Starting from SGD 3 before grant

## 5.2.2 Incentivising the private sector to prioritise data protection and privacy

Private sector organisations can also be a steppingstone for cultivating a culture of data protection and privacy in Singapore. As Singaporean consumers' have grown increasing wary about how companies are using their personal data (Data&Storage ASEAN, 2022), companies are now more incentivised to address their concerns. Indeed, more companies are recognising that consumer distrust towards their personal data use and protection policies may jeopardise their reputation and growth (Gueham, 2017). A study by Microsoft and International Data Corporation (IDC) (2019) highlighted the value that companies stand to gain by prioritising consumers' trust in their digital services. Specifically, the study found that only five per cent of Singaporean consumers would prefer to transact with an organisation that offers a lower cost but is a less trusted digital platform. Conversely, more than half (56 per cent) agreed that they would recommend a trusted digital platform to others, even if it were more expensive. Hence, it is likely that most Singaporean consumers are willing to pay more for digital services which seem more trustworthy, such as those that have implemented explicit data protection and privacy measures. Likewise, a report by Cisco (2020) found that for every dollar that companies invest in privacy, they receive a \$2.70 worth of benefit.

The Singapore government has also recognised that companies with transparent and accountable personal data practices stand to gain a competitive advantage. This is evident in the development of the Data Protection Trustmark (DPTM) by the IMDA. The DPTM is a voluntary enterprise-wide certification which organisations can obtain to demonstrate that they have accountable data protection practices in place (IMDA, n.d.-d). However, as of April 2023, only approximately 149 companies have obtained DPTM certification in Singapore. These

companies tend to come from specific sectors like the technology, finance, transport and utilities sectors.<sup>44</sup> Many are also larger corporations, such as multinational banks and global technology providers. However, as a wide range of companies routinely collect the personal data of consumers, they also stand to benefit from and hence, should be encouraged to implement clear personal data practices. Hence, there is a need to encourage uptake of the DPTM among more companies, particularly those in sectors where uptake has been lower, like retail companies, law firms and social service agencies.

This may require research to identify the key barriers hindering specific companies or sectors from investing in the DPTM. While it is possible that financial constraints are a barrier, funding support has already been introduced to help companies defray up to 80 per cent of the cost of DPTM certification (IMDA, n.d.-d). Hence, financial constraints are likely not the only impediment. One possible barrier may be the lack of knowledge regarding the economic and reputational benefits of investing in data protection and privacy; hence, organisations do not perceive value in the DPTM certification. If such is the case, then efforts must be taken to raise awareness among companies about the many benefits that they stand to gain from such an investment.

Encouraging more companies to invest in data protection and privacy also provides the added benefit of educating more Singaporeans about the measures they can take to safeguard their personal data. For example, when companies obtain DPTM certification, they are required to communicate data protection policies and practices to all employees, as well as implement data protection training for all relevant internal stakeholders (IMDA, n.d.-e). These employees may then be able to apply the knowledge and skills learnt to safeguard their data and privacy in their everyday lives.

### 5.2.3 Encouraging data sharing by the private sector

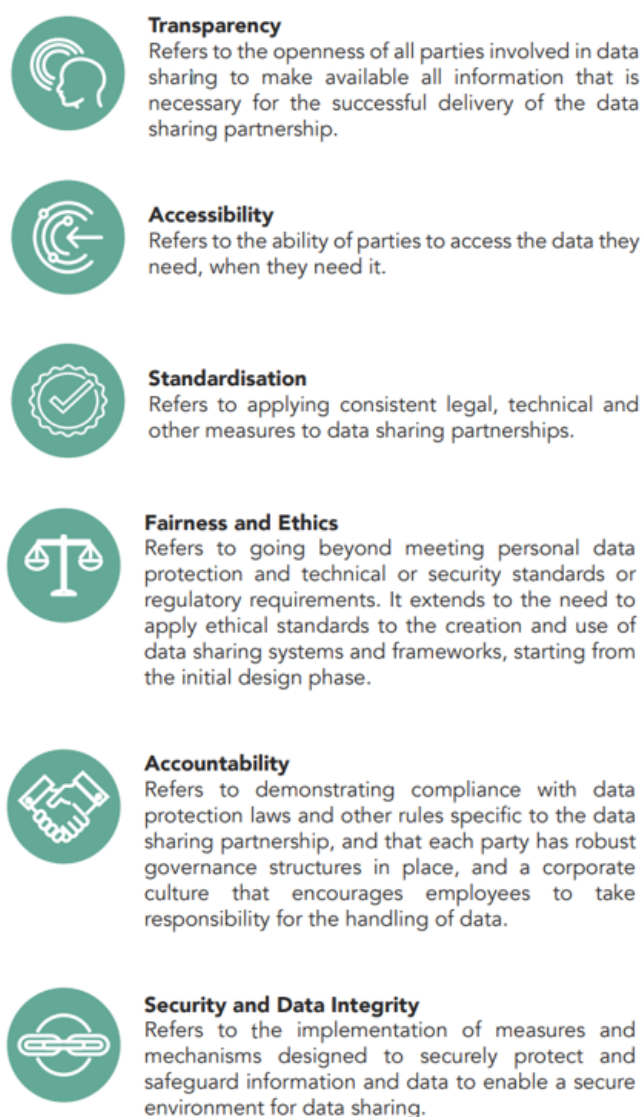
Given the vast benefits of cross-sectoral data sharing, policymakers can also consider introducing multisectoral data-sharing initiatives that includes sharing by the private sector. A key benefit of data lies in its non-rivalrous nature, where one set of data can be used by many different parties simultaneously without being depleted; hence, its repeated use leads to increasing returns (Jones & Tonetti, 2020). In fact, according to the OECD (2019), data can potentially create 10 to 20 times more value by being accessed and use by other parties, which in turn produces 20 to 50 times more value for the broader economy. Hence, data can be maximised when it is widely shared among different parties in society and can benefit from the various resources and expertise they possess. The Singapore government recognises the value of data sharing and has implemented numerous data-sharing initiatives, some of which were discussed in Section 4.2.1. However, it has yet to introduce initiatives that specifically encourage the private sector to share its data with the public sector and people sector. This represents a large yet under-utilised pool of data, given that private sector organisations routinely collect and harness a vast array of consumer data. Hence, Singapore's digital economy can stand to benefit from multisectoral data-sharing initiatives which also encourage the private sector to share its own data with others.

---

<sup>44</sup> This observation is based on the List of Data Protection Certified Organisations (as of 11 Apr 2023) by the IMDA, available at <https://www.imda.gov.sg/-/media/Imda/Files/Programme/DPTM/DPTM-Certified-Organisations.pdf>.

Companies and individuals may have numerous legitimate concerns about the risks surrounding sharing data, such as the possibility of data breaches that could undermine individuals' privacy and companies' commercial interests (OECD, 2019). Hence, it is critical to engage all relevant stakeholders in the development of any multi-sectoral data-sharing initiative. Multistakeholder engagement is necessary to understand the various concerns that different stakeholders may possess, so that policymakers can determine the acceptable levels of risk and take steps to effectively address their concerns. As participation in the multisectoral initiative cannot be mandatory, it is vital to ensure that the various stakeholders truly believe in the value and security of data sharing and are willing to actively participate. Singapore can also draw on its existing Trusted Data Sharing Framework, which aims to guide organisations through their data-sharing journeys and highlights the key considerations that they should consider when planning data partnerships (IMDA & PDPC, 2019). Notably, the framework is built around six trust principles, which are vital to forming any trusted data-sharing partnership (see Figure 12 below). The multisectoral data-sharing initiative can also build on these six principles, to develop an initiative grounded in trust whereby the different stakeholders can be assured that their data will be protected.

Figure 12. Six trust principles outlined in the Trusted Data Sharing Framework



Most countries with data-sharing initiatives have focused on enabling access to public sector data, while a few have also introduced initiatives that facilitate data sharing within the public sector. However, the EU is among the first to have taken legislative steps to facilitate multisectoral data sharing across the region. This is through two main legislations, the Data Governance Act and the Data Act. The Data Governance Act was introduced in 2020, with the aim of making more data available by (i) regulating the re-use of publicly/held, protected data, (ii) promoting data sharing through the regulation of novel data intermediaries, and (iii) encouraging data sharing for altruistic purposes (European Commission, n.d.-b). The Act encompasses both personal and non-personal data — though the GDPR must apply in cases that involve personal data. It seeks to facilitate the development of trustworthy data-sharing systems through four broad sets of measures (Cyber Risk GmbH, n.d.-b):

1. Mechanisms to facilitate the reuse of certain public sector data that cannot be made available as open data.
2. Measures to ensure that data intermediaries will function as trustworthy organisers of data sharing and pooling within common data spaces.<sup>45</sup>
3. Measures to make it easier for citizens and businesses to make their data available for the benefit of society.
4. Measures to facilitate data sharing, in particular to make it possible for data to be used across sectors and borders, and to enable the right data to be found for the right purpose.

While the Data Governance Act seeks to establish processes and structures to facilitate data sharing by companies, individuals and the public sector, the Data Act implemented in 2022 clarifies who can create value from data, and under what conditions (European Commission, 2022b). Figure 13 provides an overview of the EU's approach towards data sharing, and examples of the Data Act's applications.

---

<sup>45</sup> Through European data spaces, the EU hopes to “foster an ecosystem (of companies, civil society and individuals) creating new products and services based on more accessible data.” (European Commission, 2020). At present, the EU seeks to create data spaces in ten strategic fields, such as health, agriculture and manufacturing (European Commission, 2022b).



Figure 13. Overview of the Data Act



[Susan Ariel Aaronson on multisectoral data sharing] “When I say data sharing, I don’t mean public sector shares with the private sector. I mean, the private sector shares with smaller firms, bigger firms, the government, or non-governmental organisations (NGOs) like human rights organisations. I really mean that there is this multisectoral sharing, it can’t be mandated, but it needs to be encouraged. And if you do that, they you are saying, ‘I get the multidimensional nature of data. And I’m going to set people free to utilise data in ways that I can’t anticipate.’”

In addition to legislative measures, Singapore can also consider the use of digital badge to reward companies that engage in data-sharing practices. One example where digital badges have been effectively used to encourage data-sharing behaviour involved an 18-month

experiment by the journal *Psychological Science* (Baker, 2016). In 2014, the journal announced that it would award colourful badges to publications that made relevant data or research material publicly available. By the first half of 2014, the number of articles in *Psychological Science* that declared that data was available rose to approximately 40 per cent, whereas rates in four other psychology journals remained at less than 10 per cent. To further incentivise companies, digital badges can also be marketed as a form of corporate social responsibility, whereby companies are giving back to the individuals from which the data is obtained by maximising its societal benefits.

[Susan Ariel Aaronson on the need to incentivise companies] “[Linnet Taylor], a professor in the Netherlands.... She says look, companies control and, in a sense, own this data. And so, we have to incentivise them to share the data.... And I agree with that.”

## 5.3 At the national level

### 5.3.1 Developing national-level metrics

At the national level, one of the most pressing challenges Singapore faces is the need to strengthen its cybersecurity. Findings from the indices examined in Section 4.2.1 suggest that there are still gaps in Singapore’s cybersecurity legislation and strategies, particularly in the area of benchmarking (see Section 4.1.2). At present, the Singapore government uses the Readiness Maturity Index (RMI) framework to assess the readiness of CII sectors to manage cyber threats (CSA, 2016a). Under the Cybersecurity Act 2018, CII owners are also required to conduct a cybersecurity audit at least once every two years (CSA, n.d.-b).<sup>46</sup> However, given the pervasiveness of cyber threats across the country, where many Singaporean SMEs and individuals are being targeted (CSA, 2022a), there is a need for quantitative assessments on the broader national level. This would enable the Singapore government to more accurately assess the current cyber threats and risks faced, the level of cybersecurity development, and hence, key priority areas to safeguard the nation’s cybersecurity.

One example that Singapore can refer to is the National Cybersecurity Platform, a project funded by Poland’s National Centre for Research and Development. The project aims to develop and implement “a joint static and dynamic risk assessment methodology that take[s] into account the specificity of individual sectors, critical infrastructure operators, operators of essential services and digital service providers... for the purpose of cybersecurity management at the national level” (Ministry of Digital Affairs, n.d.). Information that may be used to analyse and calculate the risk level includes vulnerabilities, Indicators of Compromise (IoC) and incidents reported by the platform’s participants (Janiszewski et al., 2019).

Singapore’s most recent cybersecurity strategy also does not include a clear timeline or success criteria to evaluate the extent to which its objectives were met. However, establishing

---

<sup>46</sup> The audit involves adopting both compliance and risk-based approaches. For the compliance-based approach, the auditor is expected to carry out a compliance test to ascertain the adequacy and effectiveness of the controls applied in the CII to comply with the Act, subsidiary legislations, applicable written directions, Code of Practice (CoP), and standard operating procedure (SoP). For the risk-based approach, the auditor should identify the risks and threats that the CII faces, and ascertain if the controls put in place are appropriate to mitigate the known risks and threats.



a timeline and quantitative indicators of progress is critical to be able to monitor and assess the extent to which the strategy was successfully executed and effective (ITU, 2021). It is also important to periodically assess the implementation of the cybersecurity strategy and evaluate them against the objectives that were originally set. In fact, the ITU's guidelines on developing a national cybersecurity strategy highlight that strategies should include KPIs which are SMARTT:

- Specific: Target a specific area for improvement and focus on the change that is expected
- Measurable: Quantify or at least suggest an indicator of progress
- Achievable: State what results can realistically be achieved, given available resources
- Relevant: Focus on specific indicators of progress
- Responsible: Specify who will do it
- Time-related: Specify when the result(s) can be achieved

One cybersecurity strategy that includes detailed timelines and quantitative indicators is Estonia's Cybersecurity Strategy (2019–2022). Figure 14 shows an example of the country's performance indicators for its objective of achieving "a cyber-literate society".

Figure 14. Examples of the performance indicators in Estonia's Cybersecurity Strategy (2019–2022)

**Performance indicators:**

Indicator	Starting level	Target levels	Source
Percentage of those who sustained losses from being exposed to a security vulnerability online (%) <sup>71</sup>	44.8% (2010) 27.7% (2015)	≤ 20% (2022)	Statistics Estonia
Use of an officially confirmed ICT security policy in companies (%) <sup>72</sup>	16.9% (2015)	≥ 25% (2022)	Statistics Estonia
Level of cyber awareness and skills among employees at government institutions and local governments, measured on the basis of a practical skills test	N/A (2018) <sup>73</sup>	≥ 75% level satisfactory (2022)	State Information System Authority
Estimated workforce deficit <sup>74</sup>	/to be determined/	/to be determined/	Study of workforce needs in the cyber field: Praxis 2018

An alternative example that Singapore can refer to is Australia's Cyber Security Strategy 2020. Australia topped the "strengthening and enhancing cyber defenses" objective of the *NCP/ 2022*, whereas Singapore ranked 18th. While Australia's cybersecurity strategy does not include a quantitative success criterion, it clearly describes the various markers that the

government will use to measure its success in implementation (Figure 15), offering an alternative approach that Singapore can also consider.

Figure 15. Examples of the metrics used in Australia's Cyber Security Strategy 2020

## Metrics

Initiative	How the Australian Government will measure success
<b>Actions by governments</b>	
Protect critical infrastructure in a national emergency	<ul style="list-style-type: none"> <li>– Arrangements are in place for the Australian Government to respond to a cyber security emergency in a timely and effective manner.</li> <li>– There is increased visibility of threats to critical infrastructure and systems of national significance, with information available in near-real-time for those who need it to actively defend networks.</li> </ul>
Enhance incident response procedures	<ul style="list-style-type: none"> <li>– Updated Cyber Incident Management Arrangements outline how governments and businesses will increase their readiness to respond collectively to a significant national incident.</li> <li>– More government agencies and private sector organisations have strengthened their readiness and resilience.</li> </ul>

### 5.3.2 Advancing gender equality in STEM fields

Another challenge that the country faces is a marked gender gap in certain fields of employment. Females appear to be significantly under-represented in the R&D and STEM fields in Singapore, representing a loss of value manpower for talent-scarce sectors. Addressing the STEM gender gap is critical for the continued growth of Singapore's digital economy. According to the Ministry of Manpower, females comprised only one-third (32.4 per cent) of the total number of STEM employees in 2021 (Chew, 2022). This gender gap implies the loss of valuable human capital in the knowledge workforce, who could contribute to greater innovation and economic growth for the country (Lee & Pollitzer, 2016). In fact, the European Institute for Gender Equality (n.d.) estimates the closing the gender gap in STEM would lead to a rise in national income by €610 to €820 billion in 2050, demonstrating the vast economic benefits that increasing female representation in the STEM field can yield.

The Singapore government has recognised the importance of greater gender equality in STEM fields. For instance, it has helped to fund the Promotion of Women in Engineering, Research, and Science (POWERS) programme driven by Women@NTU, which seeks to encourage more women to pursue their studies and careers in STEM fields (Nanyang Technological University [NTU], 2021). It aims to foster a more supportive ecosystem, conduct research to address diversity barriers, and provide education and skills training for career advancement in STEM. However, the stark gender gap in STEM careers, whereby the number of female employees has increased by less than 3 per cent between 2015 and 2020 (Chew, 2022), suggests that more coordinated and intensive efforts are required.

Singapore could consider developing a national strategy aimed at increasing gender equity in STEM careers, or the workplace more broadly. National strategies play a critical role in establishing a country's vision, policy priorities and strategies. The gender gap in STEM fields is a highly complex issue, encompassing factors such as educational access, personal beliefs

and societal stereotypes (Teng, 2022). Hence, a national strategy focused on gender equality would enable Singapore to develop a more cohesive and targeted approach towards tackling the multifaceted challenge. Here, Singapore can again look to Australia for reference, where increasing the representation of females in STEM fields has become a national imperative (Latimer et al., 2019). For instance, the government publishes a yearly STEM Equity Monitor, which includes a large range of gender equity metrics (Australian Government, 2022). It has also released two guiding frameworks — the Advancing Women in STEM Strategy, and the Women in STEM Decadal Plan, which outline the government and sector's respective commitments to improving gender equity in STEM fields in the country (Australian Government, n.d.-b). This has culminated in its 2020 Action Plan (See Figure 16), which identifies early priorities and strategies based on the Australian government's strategy and decadal plan.

Figure 16. Australia's 2020 Action Plan



Another area that has been less focused on is the involving of male allies to promote gender equality in STEM fields. Male leaders are especially important, as leadership has a large and

direct effect on company culture. Leaders have such an effect by embodying the beliefs, values and practices of the company (Craig, 2018). Hence, it is vital to engage male leaders in STEM industries as part of the solution, such that they can promote a more gender-inclusive working environment. Singapore can again look to Australia as an example, whereby the government supported the launch of the Champions of Change STEM group in 2016 (Champions of Change Coalition, n.d.-a). The group consists of male and female members that lead a diverse range of STEM organisations, who recognise the impact of visible leadership and have committed to driving change in their organisations (Champions of Change Coalition, n.d.-b). The group also conducts research and provides online resources for other leaders to spearhead greater gender equality in their own organisations. Establishing a similar coalition in Singapore may provide an avenue for motivated male leaders in STEM industries to step up and be recognised as champions of gender equality in Singapore.

### 5.3.3 Implementing a data classification framework for cross-border data flows

To facilitate the cross-border flow, Singapore can consider implementing a risk-based data classification framework that enables cross-border data flows. Risk-based data classification frameworks establish specific procedures on how different tiers of data should be managed based on security requirements (Asian Development Bank [ADB] & Amazon Web Services [AWS] Institute, 2022). One common approach is a three-tier classification system based on risks associated with harm to society or risk to the operation of the enterprise (Salesforce, 2019):

1. Low: If the loss of confidentiality, integrity or availability could be expected to have a limited adverse impact
2. Moderate: If the loss could be expected to have a serious adverse impact
3. High: If the loss could be expected to have a severe or catastrophic adverse impact

Data classification frameworks establish clear, harmonised standards on data security, reducing uncertainty amongst organisations regarding how data should be stored, transferred or processed (ADB & AWS Institute, 2022). This enables organisations to concentrate their protection and security efforts appropriately, such that they can divert more resources to protect information that is considered more sensitive, while allowing for the flow of the larger proportion of less-sensitive data across borders (Salesforce, 2019). However, Singapore currently does not have any data classification framework pertaining to cross-border data flows. The government did introduce the Information Sensitivity Framework (ISF) in 2018, which is intended to guide public agencies in developing measures specific to the protection of personal and business data, and calibrate the measures based on the severity of harm to individuals and entities upon unauthorised disclosure of the data (Public Sector Data Security Review Committee, 2019). However, the ISF is intended for use within and between public agencies, and hence is of limited applicability for cross-border data flows. The government should consider implementing a data classification framework that aligns with Singapore's overarching privacy regulations and policies (e.g., the PDPA) to further facilitate the cross-border flow of data.

A country that Singapore can draw reference from is the Philippines. The Philippines has developed a data classification framework which has been regarded as "based on the

international best practice of observing a minimal number of tiers”, which reduces complications and the risk of misfiling (ADB & AWS Institute, 2022). Its framework classifies data according to four tiers, based on factors such as the data’s level of sensitivity, the risk of breach in the confidentiality, integrity or availability of the data, and the potential impact thereof (Department of Information and Communications Technology, 2020). Each tier is associated with different baseline controls and security protocols for safeguarding data, which are summarised in Table 12 below.

*Table 12. Summary of The Philippines’ data classification framework*

Tier	Non-Sensitive Data	Sensitive Data	Highly Sensitive or Above-Sensitive Data
Type of data	Open, publicly available, and unclassified information	Restricted data (e.g., financial and medical records)	Classified information (e.g., vital military and diplomatic information)
Requirements	Storage on accredited public cloud or the Philippine GovCloud	Store on accredited public cloud or the Philippine GovCloud and has encryption requirements	Requires private and on-site cloud deployment, storage onshore, and has encryption requirements

Source: Adapted from ADB & AWS Institute (2022)

The UK, which was ranked 2nd in the Cross-Border Data Flows Index 2021, is another state that has developed and implemented a data classification framework known as the Government Security Classifications. The framework comprises three tiers, as shown in Table 13 below (Cabinet Office, 2018). Each tier is also associated with a baseline set of personnel, physical and information security controls, that offers an appropriate level of protection against typical threats.

*Table 13. Three tiers of the UK’s Government Security Classifications*

Tier	Official	Secret	Top secret
Type of data	Most of the information that is created or processed by the public sector. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile.	Very sensitive information that justifies heightened protective measures to defend against determined and highly capable threat actors (e.g., compromise could significantly damage military capabilities, international relations, or the investigation of serious organised crime).	Most sensitive information requiring the highest level of protection from the most serious threats (e.g., compromise could cause widespread loss of life or could threaten the security or economic well-being of the country or friendly nations).

## 5.4 At the regional level

ASEAN is an invaluable multilateral platform through which Singapore — a small country limited in its size and resources — can safeguard its sovereignty and pursue its national interests. The regional organisation is collectively the fifth largest economy in the world, with a vast population of over 660 million (To & Cheung, 2023). Moreover, ASEAN has immense growth potential, and has been projected to surpass Germany and become the fourth largest economy by 2030 (Chew, 2023). To enhance the competitiveness and resilience of the region, ASEAN has also progressively taken steps to increase the interconnectedness of the region — as outlined in its Master Plan on ASEAN Connectivity 2025 (ASEAN, 2016a).<sup>47</sup> Hence, as ASEAN becomes increasingly interdependent, Singapore should spearhead efforts to further increase regional cooperation and integration, for the benefit of the region and its own economy.

[Jeff Paine on Singapore's role in ASEAN] "Singapore's policies have always been seen as forward-looking and act as a reference point to other ASEAN member states. Given this, Singapore has a responsibility to deter any ineffective policy contagion effect in ASEAN.... Singapore in its leadership position, I think, carries a lot of weight."

### 5.4.1 Growing regional cybersecurity capacity

Singapore could drive regional efforts to strengthen Southeast Asia's cybersecurity ecosystem, as doing so would also enhance the country's own cybersecurity. In recent years, ASEAN has taken significant steps to increase regional cooperation in the domain of cybersecurity. Notably Singapore, as a relatively technologically mature country, has spearheaded regional efforts such as the ASEAN Cyber Capacity Programme (ACCP) (The NATO Cooperative Cyber Defence Centre of Excellence [CCDCOE] n.d.) and the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE). However, cybersecurity regulations are still unevenly distributed across the ASEAN member states, and most ASEAN member states are still in the early stages of developing data security measures and internal adoption of cybersecurity standards (Suvannaphakdy, 2022). Another challenge is that many members have nascent local cybersecurity industries that lack homegrown capabilities and expertise (Dobberstein et al., 2018). While the Philippines, Vietnam, Singapore and Laos have introduced comprehensive cybersecurity regulatory frameworks, they are less developed among the other ASEAN member states. Given the ever-increasing interconnectedness of ASEAN member states, varying levels of cybersecurity escalates the overall systemic risk in the region (Raska & Ang, 2018). Moreover, uneven levels of cybersecurity development may impede trust in information-sharing among member states, and deter other collaborative cybersecurity efforts (Un, 2020). Hence, there is a critical need to enhance the policy, technical and legal capacity of member states lagging in this domain.

One possible area to target is the cybersecurity talent gap in Southeast Asia, and to ensure that talent development programmes are tailored to meet the specific needs of the region. Singapore has led such initiatives — one example being the recently announced Mastercard-

---

<sup>47</sup> The Master Plan identified five strategic areas that ASEAN will focus on to increase its physical, institutional and people-to-people linkages by 2025. The five strategic areas are: sustainable infrastructure, digital innovation, seamless logistics, regulatory excellence and people mobility.

NTU Joint Lab, whereby government support and facilitation was crucial to enable the partnership (Economic Development Board [EDB], 2022). Through the initiative students and mid-career professionals from around the region will be able to apply for an advanced 12-week joint Mastercard-NTU cybersecurity curriculum. However, for such initiatives to effectively strengthen Southeast Asia's cybersecurity ecosystem, they must be tailored to meet the needs of individual industries across the region (Dobberstein et al., 2018). Hence, there is the need for coordinated efforts to identify the skills and expertise needed by the region's cybersecurity ecosystem, so that appropriate talent development initiatives can be developed.

One initiative that ASEAN can draw inspiration from is the European Cybersecurity Skills Framework (ECSF). It was produced through the combined effort of the European Union Agency for Cybersecurity (ENISA) and the ENISA Ad-hoc working group on Cybersecurity Skills Framework, comprising 17 experts from 14 member states (ENISA, 2022). The framework identifies 12 cybersecurity-related roles, as well as the key responsibilities, skills, synergies and interdependencies associated with each profile (see Figure 17 for an example). The ECSF was accompanied by a user manual, which serves as a practical guide to its utilisation, based on examples and use cases (ENISA, n.d.). Hence, ASEAN can consider developing a similar framework, to develop a shared understanding of the cybersecurity field in the region and identify priority areas that talent development programmes should target.



Figure 17. Example of a profile in the ECSF

Profile Title	Cybersecurity Educator	
Alternative Title(s)	Cybersecurity Awareness Specialist Cybersecurity Trainer Faculty in Cybersecurity (Professor, Lecturer)	
Summary statement	Improves cybersecurity knowledge, skills and competencies of humans.	
Mission	Designs, develops and conducts awareness, training and educational programmes in cybersecurity and data protection-related topics. Uses appropriate teaching and training methods, techniques and instruments to communicate and enhance the cybersecurity culture, capabilities, knowledge and skills of human resources. Promotes the importance of cybersecurity and consolidates it into the organisation.	
Deliverable(s)	<ul style="list-style-type: none"> <li>• Cybersecurity Awareness Program</li> <li>• Cybersecurity Training Material</li> </ul>	
Main task(s)	<ul style="list-style-type: none"> <li>• Develop, update and deliver cybersecurity and data protection curricula and educational material for training and awareness based on content, method, tools, trainees need</li> <li>• Organise, design and deliver cybersecurity and data protection awareness-raising activities, seminars, courses, practical training</li> <li>• Monitor, evaluate and report training effectiveness</li> <li>• Evaluate and report trainee's performance</li> <li>• Finding new approaches for education, training and awareness-raising</li> <li>• Design, develop and deliver cybersecurity simulations, virtual labs or cyber range environments</li> <li>• Provide guidance on cybersecurity certification programs for individuals</li> <li>• Continuously maintain and enhance expertise; encourage and empower continuous enhancement of cybersecurity capacities and capabilities building</li> </ul>	
Key skill(s)	<ul style="list-style-type: none"> <li>• Identify needs in cybersecurity awareness, training and education</li> <li>• Design, develop and deliver learning programmes to cover cybersecurity needs</li> <li>• Develop cybersecurity exercises including simulations using cyber range environments</li> <li>• Provide training towards cybersecurity and data protection professional certifications</li> <li>• Utilise existing cybersecurity-related training resources</li> <li>• Develop evaluation programs for the awareness, training and education activities</li> <li>• Communicate, present and report to relevant stakeholders</li> <li>• Identify and select appropriate pedagogical approaches for the intended audience</li> <li>• Motivate and encourage people</li> </ul>	
Key knowledge	<ul style="list-style-type: none"> <li>• Pedagogical standards, methodologies and frameworks</li> <li>• Cybersecurity awareness, education and training programme development</li> <li>• Cybersecurity-related certifications</li> <li>• Cybersecurity education and training standards, methodologies and frameworks</li> <li>• Cybersecurity related laws, regulations and legislations</li> <li>• Cybersecurity recommendations and best practices</li> <li>• Cybersecurity standards, methodologies and frameworks</li> <li>• Cybersecurity controls and solutions</li> </ul>	
e-Competences (from e-CF)	D.3. Education and Training Provision D.9. Personnel Development E.8. Information Security Management	Level 3 Level 3 Level 3

### 5.4.2 Greater coordination against cybercrime

Besides capacity-building, Singapore should also advocate for greater regional coordination against cybercrime, which is vital to effectively combat cybercrime given their transnational nature. As digitalisation levels have grown across Asia, the Southeast Asian region has become not only a prime target for cyber criminals, but increasingly a launchpad for cyber-attacks. For instance, Indonesia, Malaysia and Vietnam have become the global hotspots for malware attacks (Dobberstein et al., 2018). Hence, as Southeast Asian countries become more and more digitally interconnected, this raises the overall systemic risk of cyber threats



throughout the region. It is imperative that ASEAN member states strengthen regional coordination so as to effectively prevent or address cybercrimes throughout the region. However, there is currently no general overarching cybercrime legislation in the region (Raemdonck, 2021). While most ASEAN member states have adopted cybercrime legislation in certain key areas, such as the criminalisation of child pornography (Benincasa, 2021; Smith, 2020), these vary significantly across the region (Smith, 2020). For example, ASEAN member states differ in their definition of criminal conduct in cyberspace, and their process of obtaining electronic evidence to assist in cybercrime investigations (Benincasa, 2021). These legislative differences cause cross-border cooperation on cybercrime investigations to be protracted and challenging (Benincasa, 2021). ASEAN has in fact recognised this difficulty and attempted to increase regional cooperation to better deal with cybercrimes. For instance, it released the ASEAN Declaration to Combat Cybercrime in 2017, which affirmed that member states “acknowledge the importance of harmonisation of laws related to cybercrime and electronic evidence” (ASEAN, 2017).

At present, there is no internationally recognised legal framework for the expedited sharing of evidence. While there is one legally binding international treaty concerning cybercrimes, known as the Budapest Convention, the Philippines is the only Southeast Asian state that has ratified it (Gillani et al., 2022). Instead, the primary way ASEAN member states obtain cross-border evidence for cybercrime investigations is through the regional Treaty on Mutual Legal Assistance in Criminal Matters (MLA Treaty) which was entered into force in 2013 (ASEAN, n.d.-b). However, it is limited in its applicability towards cybercrimes, due to its lack of provisions that account for the transnational nature of cybercrime (Benincasa, 2020). For instance, it lacks provisions concerning the retention of and access to e-evidence, which poses an issue because countries’ cybercrime investigations typically require access to e-evidence that is stored by service providers outside of that country. The MLA Treaty’s limitations are especially apparent when compared to the Budapest Convention, as the former lacks numerous provisions that are important to effectively conduct cybercrime investigations; for instance, provisions on the expedited disclosure of preserved traffic data, and mutual assistance in the real time collection of traffic data (Benincasa, 2020).

Hence, one way to enhance regional coordination is to amend the MLA Treaty to include cybercrime provisions. Such an amendment could draw reference from the provisions outlined in the Budapest Convention which has been ratified by at least 66 states. The Budapest Convention is a “substantive criminal law” that covers a wide range of offenses, such as “offences against the confidentiality, integrity and availability of computer data and systems” and “computer-related offences” (Council of Europe [COE], 2001).

Another option that ASEAN can consider is the establishment of an Independent Prosecutor Office, set up specifically to investigate and prosecute cyber criminals (Iu & Wong, 2022). The office must be able to operate independently, without any organisational or governmental influence, and should have the authority to initiate cybercrime investigations at its own discretion based on the existing information it has collected (Schjolberg, 2011). This was achieved by the COE in 2010, whereby it introduced an Information Technology and Cyber Crime Investigation Section, an independent structural subdivision of the Prosecutor General’s Office (COE, n.d.). The section is in-charge of the criminal investigation and prosecution of cybercrimes, according to the offences covered under Articles 2 to 10 of the Budapest

Convention, as well as associated offences against, or with the use of computer systems and data.

### 5.3.3 Greater harmonisation on regional data privacy and protection laws

Singapore should also advocate for the greater harmonisation of data privacy and protection laws throughout the Southeast Asian region. It should be acknowledged that ASEAN has in fact taken numerous steps to promote greater convergence in member states' national data privacy and protection laws. Since the launch of the 2016 ASEAN Framework on Personal Data Protection (ASEAN, 2016b), it has also published the 2018 ASEAN Framework on Digital Data Governance (National Privacy Commission, 2019), and more recently the 2021 ASEAN Data Management Framework. The latter aims to provide "key resources and tools for ASEAN businesses to utilise in their data-related business operations", by providing a step-by-step guide for them to implement a data management system (PDPC, n.d.-c). ASEAN's adoption of these three frameworks is indicative of its continued and solidifying commitment to strengthen personal data protection through regional collaboration. However, these frameworks are fundamentally not legally binding agreements, and do not establish rights or obligations that ASEAN member states must adhere to (Lim, 2021). As a result, data privacy and protection legislations are still unevenly distributed across the region — for instance, in terms of the adoption of data protection laws across sectors, and the impositions of limitations on data storage (Suvannaphakdy, 2022).

ASEAN could consider the implementation of a regional data privacy and protection regulation. Doing so would greatly facilitate cross-border data flows and benefit the economies of the region, by enhancing trust among member states that the data transferred will be adequately protected, and thus dissuading attempts to impose restrictions on data flows. Moreover, having to navigate different data privacy and protection regimes is highly challenging for companies, as they are unable to apply a consistent set of compliance processes due to variation and inconsistency between jurisdictions (Asian Business Law Institute, 2020). Hence, ASEAN should consider introducing a regional data privacy and protection regulation, which can be based on the seven principles outlined in its 2016 Framework on Personal Data Protection. Given that ASEAN member states have differing levels of digitalisation, a regional data privacy and protection legislation would need to be implemented in a phased manner. This was achieved with RCEP, an agreement which accounts for varying level of technological development among states, by providing some with a five-to-eight-year buffer period (Chin & Zhao, 2022). Member states that are more digitalised, including Singapore, should also pledge capacity-building assistance to less-digitalisation member states — for example, Cambodia, Laos and Myanmar (Suvannaphakdy, 2022).

[Jeff Paine on the benefits of harmonisation] "If you're a business and you're operating in 10 nations in ASEAN, having a harmonised policy set would be ideal. Because then you'd be able to comply in a much easier way. That's not necessarily the case. You know, you have different policy regimes in every country. So, to be able to operate successfully, first, you have to understand what the rules and regulations are to operate in the country. And if it differs, then that creates a challenge.... If you're going to have digital sovereignty, you

want to have something that's going to be internationally accepted [as] standards and norms."

## 6 Conclusion

The Internet revolution in the late 20th century gave rise to visions of an open, interconnected world integrated by technology among academics, technology professionals and civil society advocates. However, this vision has been progressively challenged by the growing demands for digital sovereignty that have emerged across many countries. The pursuit of digital sovereignty has threatened the global interconnectivity brought about by digital technologies, as countries increasingly undertake independent, often diverging regulatory and policy approaches to safeguard their digital sovereignty.

In this review, we unpacked the rise and manifestations of digital sovereignty across the globe and explored its implications for Singapore. The increasingly unilateral actions taken by states as they intervene in the digital sphere undoubtedly poses significant challenges to the security, stability and development of Singapore. Hence, it is imperative that the country, more than ever before, actively advocates for and explores additional ways of facilitating cross-border data flows and collaboration, while simultaneously safeguarding its own sovereignty and interests.

Singapore is a "price-taker" and not a "price setter" in the global landscape, as its small market size and resources means that the country has limited influence over global affairs. Nonetheless, the country should not be considered entirely helpless in the face of an increasingly fragmented, protectionist global landscape. There are still concrete measures that Singapore can undertake to protect its own sovereignty and pursue its national interests, even as digital sovereignty gains momentum among states across the world. This review recommends a series of measures that Singapore can pursue at different levels — at the level of the individual, organisation and nation — to safeguard its digital future.

The scope of this review is by no means exhaustive, as it focused specifically on digital sovereignty and its manifestations at the state level. However, as noted in the introduction, digital sovereignty is a widely used concept that has been employed by a wide range of stakeholders, such as individual Internet users, activist groups and civil society organisations. Hence, further insights on the implications of digital sovereignty for Singapore can be gleaned by examining the concept from other perspectives. For instance, digital sovereignty also manifests at the individual level, which touches on areas such as online harms and digital skills. Nonetheless, we are hopeful that this review sheds light on the evolving development that is digital sovereignty and presents a realistic yet optimistic perspective that while Singapore cannot prevent Internet fragmentation, there is much it can do to navigate the challenges that arise.

## 7 References

- Aaronson, S. A. (2018). Data is different: Why the world needs a new approach to governing cross-border data flows. *CIGI Papers No. 197*. Centre for International Governance Innovation.
- Aaronson, S. A. (2021). Data is disruptive: How data sovereignty is challenging data governance. Hinrich Foundation.
- Aaronson, S. A. (2022). A future built on data: Data strategies, competitive advantage and trust. *CIGI Papers No. 266*. Centre for International Governance Innovation.
- Aaronson, S. A. (2023). Could a global “wicked problems agency” incentivize data sharing? *CIGI Papers No. 273*. Centre for International Governance Innovation.
- Abrams, A. (2019, April 18). Here’s what we know so far about Russia’s 2016 meddling. *Time*. <https://time.com/5565991/russia-influence-2016-election/>
- Adonis, A. A. (2019). Critical engagement on digital sovereignty in international relations: Actor transformation and global hierarchy. *Global: Jurnal Politik Internasional*, 21(2), 262. <https://doi.org/10.7454/global.v21i2.412>
- Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179–211. [https://doi.org/10.1016/0749-5978\(91\)90020-t](https://doi.org/10.1016/0749-5978(91)90020-t)
- Alanazi, M., Freeman, M., & Tootell, H. (2022). Exploring the factors that influence the cybersecurity behaviors of young adults. *Computers in Human Behavior*, 136, 107376. <https://doi.org/10.1016/j.chb.2022.107376>
- Ang, P. H. (2008). International regulation of internet content: Possibilities and limits. In William J. Drake and Ernest J. Wilson III, *Governing Global Electronic Networks* (pp. 305–330). Online edn, MIT Press EBooks. <https://doi.org/10.7551/mitpress/9780262042512.003.0228>
- Asia-Pacific Economic Cooperation Electronic Commerce Steering Group. (2018, March 7). *Singapore joins APEC data privacy system* [Press release]. [https://www.apec.org/press/news-releases/2018/0307\\_cbpr](https://www.apec.org/press/news-releases/2018/0307_cbpr)
- Asian Business Law Institute. (2020). *Transferring personal data in ASEAN: A path to legal certainty and regional convergence*.
- Asian Development Bank & Amazon Web Services Institute. (2022). *Data management policies and practices in government*. <http://dx.doi.org/10.22617/TCS220582-2>
- Association of Southeast Asian Nations. (2016a). *Master Plan on ASEAN Connectivity 2025*. <https://asean.org/wp-content/uploads/2018/01/47.-December-2017-MPAC2025-2nd-Reprint-.pdf>
- Association of Southeast Asian Nations. (2016b). *Framework on Personal Data Protection*. <https://asean.org/wp-content/uploads/2012/05/10-ASEAN-Framework-on-PDP.pdf>
- Association of Southeast Asian Nations. (2017). *ASEAN Declaration to Prevent and Combat Cybercrimes*. <https://asean.org/wp-content/uploads/2017/11/ASEAN-Declaration-to-Combat-Cybercrime.pdf>

- Association of Southeast Asian Nations. (2021). *ASEAN model contractual clauses for cross border data flows*. [https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows\\_Final.pdf](https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf)
- Association of Southeast Asian Nations. (n.d.-a). *ASEAN Cybersecurity Cooperation Strategy (2021–2025)*. [https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025\\_final-23-0122.pdf](https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf)
- Association of Southeast Asian Nations. (n.d.-b). *Treaty of Mutual Legal Assistance in Criminal Matters*. <https://asean.org/our-communities/asean-political-security-community/rules-based-people-oriented-people-centred/treaty-on-mutual-legal-assistance-in-criminal-matters/>
- Australian Government. (2022). *The state of STEM gender equity in 2022*. Department of Industry, Science and Resources. <https://www.industry.gov.au/news/state-stem-gender-equity-2022>
- Australian Government. (n.d.-a). *Overview*. Digital Transformation Industry. <https://www.dta.gov.au/our-projects/hosting-strategy/overview>
- Australian Government. (n.d.-b). *2020 Action Plan*. Department of Industry, Science and Resources. <https://www.industry.gov.au/publications/advancing-women-stem-strategy/2020-action-plan>
- Autolitano, S., & Pawlowska, A. (2021). Europe's quest for digital sovereignty: GAIA-X as a case study. Istituto Affari Internazionali. <https://www.iai.it/en/pubblicazioni/europes-quest-digital-sovereignty-gaia-x-case-study>
- Baezner, M., & Robin, P. (2018). *Cyber Sovereignty*. (Zurich: Center for Security Studies [CSS], ETH Zürich). <https://doi.org/10.3929/ethz-b-000314398>
- Baharudin, H. (2018, September 19). Singapore to spend \$30 million over next 5 years to fund new regional cyber security centre. *The Straits Times*. <https://www.straitstimes.com/singapore/singapore-to-spend-30-million-over-next-5-years-to-fund-new-regional-cyber-security-centre>
- Baker, M. (2016). Digital badges motivate scientists to share data. *Nature*. <https://doi.org/10.1038/nature.2016.19907>
- Ball, J. (2022, March 17). Russia is risking the creation of a “splinternet” — and it could be irreversible. *MIT Technology Review*. <https://www.technologyreview.com/2022/03/17/1047352/russia-splinternet-risk/>
- Barlow, J. P. (1996, February 8). *A declaration of the independence of cyberspace*. Electronic Frontier Foundation. <https://www.eff.org/cyberspace-independence>
- Barriuso, D. (2022, July 7). Only cross-border, cross-sector collaboration will be enough to beat cybercrime. World Economic Forum. <https://www.weforum.org/agenda/2021/07/cross-border-cross-sector-collaboration-cybercrime/>
- Bartelson, J. (2006). The concept of sovereignty revisited. *European Journal of International Law*, 17(2), 463–474. <https://doi.org/10.1093/ejil/chl006>

- Barth, S., & de Jong, M. D. T. (2017). The privacy paradox — Investigating discrepancies between expressed privacy concerns and actual online behavior — A systematic literature review. *Telematics and Informatics*, 34(7), 1038–1058. <https://doi.org/10.1016/j.tele.2017.04.013>
- Basu, A. (2021). Sovereignty in a “datafied” world. *Issue Brief No. 501*. Observer Research Foundation. <https://www.orfonline.org/research/sovereignty-in-a-datafied-world/>
- Bauer, M., Lee-Makiyama, H., Van Der Marel, E., & Verschelde, B. (2015). The costs of data localisation: Friendly fire on economic recovery. *ECIPE Occasional Papers*. European Centre for International Political Economy.
- Benincasa, E. (2020). *The role of regional organizations in building cyber resilience: ASEAN and the EU*. Pacific Forum. [https://pacforum.org/wp-content/uploads/2020/06/issuesinsights\\_Vol20WP3-1.pdf](https://pacforum.org/wp-content/uploads/2020/06/issuesinsights_Vol20WP3-1.pdf)
- Benincasa, E. (2021, January 19). ASEAN needs to enhance cross-border cooperation on cybercrime. *The Strategist*. <https://www.aspistrategist.org.au/asean-needs-to-enhance-cross-border-cooperation-on-cybercrime/>
- Besson, S. (n.d.). Sovereignty. *Oxford Public International Law*. <https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1472>
- Borak, M. (2021, August 26). China’s privacy law borrows a page from Europe’s GDPR but it goes further as Beijing shores up data security. *South China Morning Post*. <https://www.scmp.com/tech/tech-war/article/3146523/chinas-privacy-law-borrows-page-europes-gdpr-it-goes-further-beijing>
- Borschberg, P. (2016). Singapore’s historical journey toward a global trading hub: An introductory overview.
- Bosoer, L. (2022). Beyond sovereignty: Strategies for digital autonomy in the Southern Cone [Master’s thesis, European University Institute]. European University Institute. <https://hdl.handle.net/1814/74780>
- Bradshaw, S., & Howard, P. (2017). Troops, trolls and troublemakers: A global inventory of organized social media manipulation. In *Computational Propaganda Research Project* (pp. 1–37). Oxford Internet Institute. <https://ora.ox.ac.uk/objects/uuid:cef7e8d9-27bf-4ea5-9fd6-855209b3e1f6>
- Brannon, I., & Schwartz, H. (2018). The new perils of data localization rules. *Regulation*, 12–13. CATO Institute. <https://www.cato.org/regulation/summer-2018/new-perils-data-localization-rules>
- Bria, F. (2015). *Public policies for digital sovereignty*. Platform Cooperativism Conference, New York.
- Budnitsky, S., & Jia, L. (2018). Branding Internet sovereignty: Digital media and the Chinese-Russian cyberalliance. *European Journal of Cultural Studies*, 21(5), 594–613. <https://doi.org/10.1177/1367549417751151>
- Burgess, M. (2020, March 24). What is GDPR? The summary guide to GDPR compliance in the UK. *WIRED UK*. <https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018>

- Burwell, F. G., & Propp, K. (2020). The European Union and the search for digital sovereignty: Building “Fortress Europe” or preparing for a new world? *Issue Brief*. Atlantic Council. <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/the-european-union-and-the-search-for-digital-sovereignty/>
- Cabinet Office. (2018). *Government security classifications*. <https://www.gov.uk/government/publications/government-security-classifications>
- Cai, C. (2018). Global cyber governance: China’s contribution and approach. *China Quarterly of International Strategic Studies*, 04(01), 55–76. <https://doi.org/10.1142/s2377740018500069>
- Campbell-Kelly, M., & Garcia-Swartz, D. D. (2013). The history of the Internet: The missing narratives. *Journal of Information Technology*, 28(1), 18–33. <https://doi.org/10.1057/jit.2013.4>
- Canadian Centre for Cyber Security. (2021). *Cyber threats to Canada’s democratic process*. <https://www.cyber.gc.ca/en/guidance/cyber-threats-canadas-democratic-process-july-2021-update>
- Carrillo, A. J., & Jackson, M. (2022). Follow the leader? A comparative law study of the EU’s General Data Protection Regulation’s impact in Latin America. *Vienna Journal on International Constitutional Law*, 16(2), 177–262. <https://doi.org/10.1515/icl-2021-0037>
- Champions of Change Coalition. (n.d.-a). *Champions of change STEM*. <https://championsofchangecoalition.org/groups/champions-of-change-stem/>
- Champions of Change Coalition. (n.d.-b). *Take action*. <https://championsofchangecoalition.org/take-practical-action/>
- Chan, C. S. (2022, September 27). SMEs going digital, workings aiming to hone skill can get help under new schemes. *The Business Times*. <https://www.businesstimes.com.sg/singapore/smes/smes-going-digital-workers-aiming-hone-skills-can-get-help-under-new-schemes>
- Chandel, S., Zang, J., Yu, Y., Sun, J., & Zhang, Z. (2019). The Golden Shield Project of China: A decade later — an in-depth study of the Great Firewall. *2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*, 111–119. <https://doi.org/10.1109/cyberc.2019.00027>
- Chander, A. & Lê, U. P. (2015). Data nationalism. *Emory Law Journal*, 64(3), 677.
- Check Point Research Team. (2021, May 27). Check Point research: Asia Pacific experiencing a 168% year on year increase in cyberattacks in May 2021 [Blog]. <https://blog.checkpoint.com/security/check-point-research-asia-pacific-experiencing-a-168-year-on-year-increase-in-cyberattacks-in-may-2021/>
- Chee, K. (2021a, October 6). Asean-S’pore centre for training national cyber-security teams opens new campus. *The Straits Times*. <https://www.straitstimes.com/tech/tech-news/asean-spore-centre-for-training-national-cyber-security-teams-opens-new-campus>
- Chee, K. (2021b, June 28). More S’poreans hit by cyber attacks; CSA launches awareness campaign. *The Straits Times*. <https://www.straitstimes.com/tech/tech-news/more-sporeans-hit-by-cyber-attacks-csa-launches-awareness-campaign>

- Chee, K. (2022, March 4). Budget debate: Widely used services, apps soon to comply with govt cyber-security rules. *The Straits Times*.  
<https://www.straitstimes.com/singapore/politics/budget-debate-widely-used-services-apps-soon-to-comply-with-govt-cyber-security-rules>
- Chen, B. X. (2021, September 16). The battle for digital privacy is reshaping the Internet. *The New York Times*. <https://www.nytimes.com/2021/09/16/technology/digital-privacy.html>
- Chew, H. M. (2022, January 12). Employment rate for Singapore women rose in past decade, share among PMETs also up: MOM. CNA.  
<https://www.channelnewsasia.com/singapore/employment-rate-singapore-women-rose-past-decade-share-among-pmet-ministry-manpower-2430196>
- Chew, M. Y. (2023, March 8). Capturing the rise of Asean amid economic resilience and growing wealth. *The Business Times*. <https://www.businesstimes.com.sg/wealth/wealth-investing/whos-who-private-banking-mar-2023/capturing-rise-asean-amid-economic>
- Chia, O. (2022, October 25). Divided Internet could lead to fewer economic opportunities and more security threats, say panellists. *The Straits Times*.  
<https://www.straitstimes.com/tech/divided-internet-could-lead-to-fewer-economic-opportunities-and-more-security-threats-say-panellists>
- Chin, Y. C., & Zhao, J. (2022). Governing cross-border data flows: International trade agreements and their limits. *Laws*, 11(4), 63. <https://doi.org/10.3390/laws11040063>
- Chong, A. (2021). Smart city, small state: Singapore's ambitions and contradictions in digital transnational connectivity. *Journal of International Affairs*, 74(1), 243.
- Choudhury, S. R. (2019, March 28). Former Australian PM Turnbull explains why his government banned Huawei, ZTE from selling 5G equipment. CNBC.  
<https://www.cnn.com/2019/03/28/malcolm-turnbull-on-australias-decision-to-ban-chinas-huawei-and-zte.html>
- Christl, W. (2017a). How companies use personal data against people. Cracked Labs.  
[https://crackedlabs.org/dl/CrackedLabs\\_Christl\\_DataAgainstPeople.pdf](https://crackedlabs.org/dl/CrackedLabs_Christl_DataAgainstPeople.pdf)
- Christl, W. (2017b). *Corporate surveillance in everyday life*. Cracked Labs.  
<https://crackedlabs.org/en/corporate-surveillance>
- Chua, M. (2013). How should the Singapore government regulate online news sites? Lee Kuan Yew School of Public Policy. [https://lkyspp.nus.edu.sg/docs/default-source/case-studies/how-should-the-singapore-government-regulate-online-news-sites.pdf?sfvrsn=183b960b\\_2](https://lkyspp.nus.edu.sg/docs/default-source/case-studies/how-should-the-singapore-government-regulate-online-news-sites.pdf?sfvrsn=183b960b_2)
- Chua, N. (2022, May 18). Cross-border and multi-agency efforts needed to tackle crimes like scams: Ex-police chief. *The Straits Times*.  
<https://www.straitstimes.com/singapore/courts-crime/cross-border-and-multi-agency-efforts-needed-to-tackle-crimes-like-scams-ex-police-chief>
- Chung, L. H., & Hetherington, W. (2018, November 5). China targets polls with fake accounts. *Taipei Times*.  
<https://www.taipeitimes.com/News/front/archives/2018/11/05/2003703618>



- Cisco. (2020). From privacy to profit: Achieving positive returns on privacy investments: CISCO data privacy benchmark study 2020. [https://www.cisco.com/c/dam/global/en\\_uk/products/collateral/security/2020-data-privacy-cybersecurity-series-jan-2020.pdf](https://www.cisco.com/c/dam/global/en_uk/products/collateral/security/2020-data-privacy-cybersecurity-series-jan-2020.pdf)
- Coleman, D. (2019). Digital colonialism: The 21st century scramble for Africa through the extraction and control of user data and the limitations of data protection laws. *Michigan Journal of Race & Law*, 24(2), 417. <https://doi.org/10.36643/mjrl.24.2.digital>
- Collins, T. & AFP. (2019, April 11). Rise of the “splinternet”: Experts warn the world wide web will break up and fragment as governments set their own rules to filter and restrict content. *Mail Online*. <https://www.dailymail.co.uk/sciencetech/article-6905695/Breaking-internet-new-regulations-imperil-global-network.html>
- Cong, W., & Thumfart, J. (2022). A Chinese precursor to the digital sovereignty debate: Digital anti-colonialism and authoritarianism from the post-Cold War era to the Tunis Agenda. *Global Studies Quarterly*, 2(4). <https://doi.org/10.1093/isagsq/ksac059>
- Bjola, C. (2021). The European Union’s quest for digital sovereignty and its implications for the transatlantic relationship. *Working Paper No 5*. Oxford Digital Diplomacy Research Group. <http://www.qeh.ox.ac.uk/sites/www.odid.ox.ac.uk/files/DigDiploROxWP5.pdf>
- Cory, N. (2022, December 21). Indonesia’s data privacy law avoids costly and misguided localization. *The Jakarta Post*. <https://www.thejakartapost.com/opinion/2022/12/21/indonesias-data-privacy-law-avoids-costly-and-misguided-localization-.html>
- Cory, N., & Dascoli, L. (2021). *How barriers to cross-border data flows are spreading globally, what they cost, and how to address them*. Information Technology & Innovation Foundation (ITIF). <https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/>
- Council of Europe. (n.d.). *Prosecutor General’s Office MD*. <https://www.coe.int/fr/web/cybercrime/prosecutor-general-s-office-md>
- Council of Europe. (2001). *The Budapest Convention (ETS No. 185) and its Protocols*. <https://www.coe.int/en/web/cybercrime/the-budapest-convention>
- Couture, S., & Toupin, S. (2019). What does the notion of “sovereignty” mean when referring to the digital? *New Media & Society*, 21(10), 2305–2322. <https://doi.org/10.1177/1461444819865984>
- Craig, W. (2018, September 5). The role leadership has in company culture. *Forbes*. <https://www.forbes.com/sites/williamcraig/2018/09/05/the-role-leadership-has-in-company-culture/>
- Crandall, M., & Allan, C. (2015). Small states and big ideas: Estonia’s battle for cybersecurity norms. *Contemporary Security Policy*, 36(2), 346–368. <https://doi.org/10.1080/13523260.2015.1061765>
- Creemers, R. (2020). China’s approach to cyber sovereignty. Konrad-Adenauer-Stiftung.
- Cyber Risk GmbH. (n.d.-a). *NIS 2 Directive*. <https://www.nis-2-directive.com/>

Cyber Risk GmbH. (n.d.-b). *The European Data Governance Act (DGA)*.  
<https://www.european-data-governance-act.com/>

<https://www.csa.gov.sg/News/Press-Releases/establishment-of-asean-regional-computer-emergency-response-team>

Cyber Security Agency of Singapore. (2016a). *Singapore's Cybersecurity Strategy*.

Cyber Security Agency of Singapore. (2016b, July 12). *Singapore and the Netherlands to strengthen cyber security cooperation* [Press release].  
<https://www.csa.gov.sg/news/press-releases/csa-signs-mou-with-the-netherlands-to-strengthen-cyber-security-cooperation>

Cyber Security Agency of Singapore. (2017, June 2). *Singapore signs MOU with Australia to enhance cybersecurity collaboration* [Press release].  
<https://www.csa.gov.sg/news/press-releases/singapore-signs-mou-with-australia-to-enhance-cybersecurity-collaboration>

Cyber Security Agency of Singapore. (2018, November 14). *Singapore signs Memorandum of Understanding with Canada on cybersecurity cooperation* [Press release].  
<https://www.csa.gov.sg/news/press-releases/singapore-signs-memorandum-of-understanding-with-canada-on-cybersecurity-cooperation>

Cyber Security Agency of Singapore. (2021, June 28). *"Better cyber safe than sorry" campaign*. <https://www.csa.gov.sg/Tips-Resource/Resources/gosafeonline/2021/bettercybersafethansorry>

Cyber Security Agency of Singapore. (2022a). *Singapore cyber landscape 2021*.  
<https://www.csa.gov.sg/Tips-Resource/publications/2022/singapore-cyber-landscape-2021>

Cyber Security Agency of Singapore. (2022b). *Singapore's counter ransomware task force report*. [https://www.csa.gov.sg/docs/default-source/publications/2022/counter-ransomware-task-force-report.pdf?sfvrsn=4fb257bb\\_1](https://www.csa.gov.sg/docs/default-source/publications/2022/counter-ransomware-task-force-report.pdf?sfvrsn=4fb257bb_1)

Cyber Security Agency of Singapore. (2022c, October 20). *Establishment of ASEAN Regional Computer Emergency Response Team (CERT)* [Press release].

Cyber Security Agency of Singapore. (n.d.-a). *Mission, vision and values*.  
<https://www.csa.gov.sg/Explore/who-we-are/mission-vision-and-values>

Cyber Security Agency of Singapore. (n.d.-b). *Cybersecurity audit for CII*.  
<https://www.csa.gov.sg/faq/cybersecurity-audit-for-cii>

Cybersecurity and Infrastructure Agency. (2021, February 1). *What is cybersecurity?*  
<https://www.cisa.gov/uscert/ncas/tips/ST04-001>

Daniels, L. (2017, April 23). How Russia hacked the French election. *Politico*.  
<https://www.politico.eu/article/france-election-2017-russia-hacked-cyberattacks/>

Data&Storage ASEAN. (2022, November 24). *OpenText research shows 85% of Singapore consumers are concerned about how companies use their data* [Press release].  
<https://datastorageasean.com/news-press-releases/opentext-research-shows-85-singapore-consumers-are-concerned-about-how-companies>

- DataGuidance. (2020, August 4). *PCPD and ICO sign MoU on regulatory, enforcement, and research cooperation regarding citizens data risks*.  
<https://www.dataguidance.com/news/international-pcpd-and-ico-sign-mou-regulatory>
- Deibert, R. J., & Crete-Nishihata, M. (2012). Global governance and the spread of cyberspace controls. *Global Governance: A Review of Multilateralism and International Organizations*, 18(3), 339–361. <https://doi.org/10.1163/19426720-01803006>
- Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (2008). *Access denied: The practice and policy of global internet filtering*. MIT Press.
- Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (2011). *Access contested: Security, identity, and resistance in Asian cyberspace*. MIT Press.
- Department for Promotion of Industry and Internal Trade. (2019). *Draft national e-commerce policy: India's data for India's development*. <https://dipp.gov.in/whats-new/draft-national-e-commerce-policy-stakeholder-comments>
- Department of Foreign Affairs and Trade. (2021). *Australia's international cyber and critical tech engagement strategy*.  
<https://www.internationalcybertech.gov.au/sites/default/files/2021-05/21066%20DFAT%20Cyber%20Affairs%20Strategy%202021%20update%20Internals%201%20Acc.pdf>
- Department of Information and Communications Technology. (2020). *Amendments to the Department Circular No. 2017 - 002, Re: Prescribing the Philippines government's Cloud First policy*.  
[https://www.dataguidance.com/sites/default/files/department\\_circular\\_no\\_10\\_amendments\\_to\\_dc\\_no\\_2017\\_002\\_re\\_prescribing.pdf](https://www.dataguidance.com/sites/default/files/department_circular_no_10_amendments_to_dc_no_2017_002_re_prescribing.pdf)
- DLA Piper. (n.d.). *Data protection laws of the world: Singapore*.  
<https://www.dlapiperdataprotection.com/index.html?t=law&c=SG>
- Dobberstein, N., Gerdemann, D., Triplett, C., Pereira, G., Hoe, G., & Azhari, S. (2018). *Cybersecurity in ASEAN: An urgent call to action*. ATKearney. <https://www.southeast-asia.kearney.com/documents/1781738/1782318/Cybersecurity+in+ASEAN%E2%80%994An+Urgent+Call+to+Action.pdf/80a880c4-8b70-3c99-335f-c57e6ded5d34>
- Doherty, B. (2019, September 5). Spy chief says foreign espionage and interference an “existential threat” to Australia. *The Guardian*. <https://www.theguardian.com/australia-news/2019/sep/05/spy-chief-says-foreign-espionage-and-interference-an-existential-threat-to-australia>
- Donahoe, E., & Canineu, M. L. (2014, June 18). A year after Snowden, a watershed moment for Internet freedom. *The Globe and Mail*. <https://www.theglobeandmail.com/opinion/a-year-after-snowden-weve-reached-a-watershed-moment-for-web-freedom/article19215294/>
- Dowling, M. E. (2022). Foreign interference and digital democracy: Is digital era governance putting Australia at risk? *Australian Journal of Political Science*, 57(2), 113–128.  
<https://www.tandfonline.com/doi/full/10.1080/10361146.2021.2023093>
- Economic Community of West African States. (2021, January 18). *Information and Communication Technology: ECOWAS adopts a regional strategy for cybersecurity and the fight against cybercrime*. <https://parl.ecowas.int/information-and-communication->

technology-ecowas-adopts-a-regional-strategy-for-cybersecurity-and-the-fight-against-cybercrime/

Economic Community of West African States. (n.d.). *ECOWAS regional cybersecurity and cybercrime strategy*. <https://www.ocwarc.eu/wp-content/uploads/2021/02/ECOWAS-Regional-Cybersecurity-Cybercrime-Strategy-EN.pdf>

Economic Development Board. (2022, December 7). *Mastercard and NTU Singapore collaborate on new cybersecurity training and research partnership*. <https://www.edb.gov.sg/en/about-edb/media-releases-publications/mastercard-and-ntu-singapore-collaborate-on-new-cybersecurity-training-and-research-partnership.html>

Edward Snowden: Leaks that exposed US spy programme. (2014, January 17). BBC News. <https://www.bbc.com/news/world-us-canada-23123964>

Ehrlich, P. (2002). Communications Decency Act 230. *Berkeley Technology Law Journal*, 17(1), 401. <https://doi.org/10.15779/z384x12>

Elms, D. (2021a). *Digital sovereignty: Protectionism or autonomy?* Hinrich Foundation.

Elms, D. (2021b). *China applies to join DEPA*. Asian Trade Centre. <https://asiantradecentre.org/talkingtrade/china-applies-to-join-depa>

European Commission. (2020). *A European strategy for data* (COM/2020/66 final). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066>

European Commission. (2021). *2030 Digital Compass: the European way for the digital decade* (COM/2021/118 final). <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118>

European Commission (2022a). *European Declaration on Digital Rights and Principles for the Digital Decade*. <https://digital-strategy.ec.europa.eu/en/library/declaration-european-digital-rights-and-principles#Declaration>

European Commission. (2022b). *Staff working document on data spaces*. <https://digital-strategy.ec.europa.eu/en/library/staff-working-document-data-spaces>

European Commission. (n.d.-a). *Adequacy decisions*. [https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions\\_en](https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en)

European Commission. (n.d.-b). *Data Governance Act explained*. <https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained>

European Institute for Gender Equality. (n.d.). How gender equality in stem education leads to economic growth. <https://eige.europa.eu/gender-mainstreaming/policy-areas/economic-and-financialaffairs/economic-benefits-gender-equality/stem>

European Parliament & European Council. (2016). Regulation (EU) 2017/679 of the European Union and the Council on the protection of natural persons with regards to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union*. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>

- European Parliament. (2022). *EU must prepare better to fight off foreign interference and disinformation* [Press release]. <https://www.europarl.europa.eu/news/en/press-room/20220304IPR24790/eu-must-prepare-better-to-fight-off-foreign-interference-and-disinformation>
- European Union Agency for Cybersecurity. (n.d.). *European Cybersecurity Skills Framework (ECSF)*. <https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework>
- European Union Agency for Cybersecurity. (2022, September 21). *Developing a strong cybersecurity workforce: Introducing the European Cybersecurity Skills Framework*. <https://www.enisa.europa.eu/news/developing-a-strong-cybersecurity-workforce-introducing-the-european-cybersecurity-skills-framework>
- Evenett, S. J., & Fritz, J. (2022). *Emergent digital fragmentation: The perils of unilateralism*. Centre for Economic Policy Research.
- Facebook. (2021). *Threat report: The state of influence operations 2017–2020*.
- Falk, R. (2001) Sovereignty. In Krieger, J., *The Oxford Companion to Politics in the World* (2nd ed.). Oxford University Press. doi:10.1093/acref/9780195117394.001.0001
- Fan, A., Wu, Q., Yan, X., Lu, X., Ma, Y., & Xiao, X. (2020). Research on influencing factors of personal information disclosure intention of social media in China. *Data and Information Management*, 5(1), 195–207. <https://doi.org/10.2478/dim-2020-0038>
- Ferracane, M. F., & van der Marel, E. (2018). *Do data policy restrictions inhibit trade in services*. European Centre for International Political Economy. <https://ecipe.org/publications/do-data-policy-restrictions-inhibit-trade-in-services/>
- Fleming, S. (2021, March 15). *What is digital sovereignty and why is Europe so interested in it?* World Economic Forum. <https://www.weforum.org/agenda/2021/03/europe-digital-sovereignty/>
- Floridi, L. (2020). The fight for digital sovereignty: What it is, and why it matters, especially for the EU. *Philosophy & Technology*, 33(3), 369–378. <https://doi.org/10.1007/s13347-020-00423-6>
- Foltz, C. B., Newkirk, H. E., & Schwager, P. H. (2016). An empirical investigation of factors that influence individual behavior toward changing social networking security settings. *Journal of Theoretical and Applied Electronic Commerce Research*, 11(2), 2. <https://doi.org/10.4067/s0718-18762016000200002>
- Freedman, M. (2023). How businesses are collecting data (and what they're doing with it). *Business News Daily*. <https://www.businessnewsdaily.com/10625-businesses-collecting-data.html>
- Frontier Economics. (2022, June 1). The extent and impact of data localisation: reports prepared for DCMS.
- Fu, G., & Lim, M. Y. (2022, May 26). SMEs spurring Singapore's green transition. *The Business Times*. <https://www.businesstimes.com.sg/singapore/smes/smes-spurring-singapores-green-transition>

- Furman, A., Zappa, F., & Barrera, R. (2022, October 27). *The privacy, data protection and cybersecurity law review: Argentina*. The Law Reviews. <https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/argentina>
- Gao, H. (2022). *Data sovereignty and trade agreements: Three digital kingdoms*. Hinrich Foundation.
- Gellman, B. & Poitras, L. (2013, June 7). U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. *Washington Post*. [https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497\\_story.html?itid=lk\\_inline\\_manual\\_9](https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?itid=lk_inline_manual_9)
- Gillani, S., Dermish, A., Grossman, J., Rühmann, F., & Macmillan Keck (2022). The role of cybersecurity and data security in the digital economy. *UNCDF Policy Accelerator Brief*. <https://policyaccelerator.uncdf.org/policy-tools/brief-cybersecurity-digital-economy>
- Glasze, G., Cattaruzza, A., Douzet, F., Dammann, F., Bertran, M., Bômont, C., Braun, M., Danet, D., Desforges, A., Géry, A., Grumbach, S., Hummel, P., Limonier, K., Münßinger, M., Nicolai, F., Pétiñaud, L., Winkler, J., & Zanin, C. (2022). Contested spatialities of digital sovereignty. *Geopolitics*, 1–40. <https://doi.org/10.1080/14650045.2022.2050070>
- Gleicher, N. (2019, January 31). *Removing coordinated inauthentic behavior from Iran*. Meta. <https://about.fb.com/news/2019/01/removing-cib-iran/>
- Glowniak, J. V. (1995). An introduction to the Internet, Part 1: History, organization and function. *Journal of Nuclear Medicine Technology*, 23(2), 56–61. <https://tech.snmjournals.org/content/23/2/56.full.pdf>
- Goldfarb, A., & Tucker, C. (2012). Privacy and innovation. In *Innovation Policy and the Economy Volume 12* (pp. 65–90). University of Chicago Press. <https://doi.org/10.1086/663156>
- Golovanova, I. P. (2020, January 3). Russia increases fines for violation of its data localization law. *The National Law Review*. <https://www.natlawreview.com/article/russia-increases-fines-violation-its-data-localization-law>
- Google, Temasek, & Bain & Company. (2022). E-economy SEA 2022: Report highlights. <https://economysea.withgoogle.com/report/>
- Government Technology Agency. (2023, February 24). *Myinfo — A “tell us once” service that facilitates online transactions for individuals*. Singapore Government Developer Portal. <https://www.developer.tech.gov.sg/products/categories/digital-identity/myinfo/overview.html>
- Goyal, T. (2022, November 20). A first look at the new data protection Bill. *The Hindu*. <https://www.thehindu.com/sci-tech/technology/a-first-look-at-the-new-data-protection-bill/article66162209.ece>
- Grabosky, P. (2004). The global dimension of cybercrime. *Global Crime*, 6(1), 146–157. <https://doi.org/10.1080/1744057042000297034>

- Graham-Harrison, E., & Cadwalladr, C. (2018, March 17). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*. <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>
- Gravett, W. (2020). Digital neo-colonialism: The Chinese model of internet sovereignty in Africa. *African Human Rights Law Journal*, 20(1). <https://doi.org/10.17159/1996-2096/2020/v20n1a5>
- Green, C. W., & Ruhleder, K. (1995). Globalization, borderless worlds, and the Tower of Babel. *Journal of Organizational Change Management*. <https://doi.org/10.1108/09534819510090213>
- Greenfield, C. (2018, November 28). New Zealand rejects Huawei's first 5G bid citing national security risk. *Reuters*. <https://www.reuters.com/article/us-spark-nz-huawei-tech-idUSKCN1NX08U>
- Gueham, F. (2017). *Digital sovereignty*. Fondation Pour L'innovation Politique. <https://www.fondapol.org/en/study/digital-sovereignty-steps-towards-a-new-system-of-internet-governance/>
- Hassan, D. (2006). The rise of the territorial state and the treaty of Westphalia. *Yearbook of New Zealand Jurisprudence*, 9, 62. <https://opus.lib.uts.edu.au/bitstream/10453/3289/1/2006006060.pdf>
- Hatem, L., Ker, D., & Mitchell, J. (2020). *A roadmap toward a common framework for measuring the digital economy*. Organisation for Economic Co-operation and Development. <https://www.oecd.org/sti/roadmap-toward-a-common-framework-for-measuring-the-digital-economy.pdf>
- Heisler, J. (2021, April 21). Smaller economies see big opportunities in digital trade pact. *VOA News*. [https://www.voanews.com/a/economy-business\\_smaller-economies-see-big-opportunities-digital-trade-pact/6204836.html](https://www.voanews.com/a/economy-business_smaller-economies-see-big-opportunities-digital-trade-pact/6204836.html)
- Hellerud, A. (2022). Which governments are requesting your data the most? *TechRobot*. <https://techrobot.com/which-governments-requesting-data-the-most/>
- Hermawanto, A., & Anggraini, M. (2020). Globalization and locality: Global communication and digital revolution in the borderless world era. *Proceeding of LPPM UPN "VETERAN" Yogyakarta Conference Series 2020 Political and Social Science Series*. <https://doi.org/10.31098/pss.v1i1.84>
- Hicks, J. (2019, September 29). "Digital colonialism": Why countries like India want to take control of data from Big Tech. *The Print*. <https://theprint.in/tech/digital-colonialism-why-countries-like-india-want-to-take-control-of-data-from-big-tech/298217/>
- Hill, J. F. (2014). The growth of data localization post-Snowden: Analysis and recommendations for U.S. policymakers and business leaders. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.2430275>
- Hioe, W. (2001) National infocomm strategy and policy: Singapore's experience. *ICA Information No. 74*.

- Hirdaramani, Y. (2022, October 3). *Why data localisation may not be a panacea for data privacy woes in ASEAN*. GovInsider. <https://govinsider.asia/data-security/why-data-localisation-may-not-be-a-panacea-for-data-privacy-woes-in-asean/>
- Hummel, P., Braun, M., Tretter, M., & Dabrock, P. (2021). Data sovereignty: A review. *Big Data & Society*, 8(1), 205395172098201. <https://doi.org/10.1177/2053951720982012>
- Infocomm Media Development Authority. (n.d.-a). *SMEs go digital*. <https://www.imda.gov.sg/how-we-can-help/smes-go-digital>
- Infocomm Media Development Authority. (n.d.-b). *APEC Privacy Recognition for Processors (PRP) Certification*. <https://www.imda.gov.sg/How-We-Can-Help/Privacy-Recognition-for-Processors-Certification>
- Infocomm Media Development Authority. (n.d.-c). *CTO-as-a-Service*. <https://services2.imda.gov.sg/CTOaaS/Home>
- Infocomm Media Development Authority. (n.d.-d). *Data Protection Trustmark Certification*. <https://www.imda.gov.sg/how-we-can-help/data-protection-trustmark-certification>
- Infocomm Media Development Authority. (n.d.-e). *Overview of certification requirements*.
- Infocomm Media Development Authority. (2018). *Digital Economy Framework for Action*. <https://www.imda.gov.sg/About-IMDA/Research-and-Statistics/SGDigital/Digital-Economy-Framework-for-Action>
- Infocomm Media Development Authority & Personal Data Protection Commission. (2019). *Trusted Data Sharing Framework*. <https://www.imda.gov.sg/-/media/Imda/Files/Programme/AI-Data-Innovation/Trusted-Data-Sharing-Framework.pdf>
- Information Commissioner's Office. (n.d.-a). *What is personal data*. <https://gdpr-info.eu/issues/personal-data/>
- Information Commissioner's Office. (n.d.-b). *Adequacy*. <https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-and-the-eu-in-detail/adequacy/>
- Innovation, Science and Economic Development Canada. (2020, November 17). *New proposed law to better protect Canadians' privacy and increase their control over their data and personal information*. <https://www.canada.ca/en/innovation-science-economic-development/news/2020/11/new-proposed-law-to-better-protect-canadians-privacy-and-increase-their-control-over-their-data-and-personal-information.html>
- International Telecommunication Union. (2021). *Guide to developing a national cybersecurity strategy (2nd edition)*. <https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2021-ncs-guide.pdf>
- International Trade Administration. (2022, August 11). *Singapore — country commercial guide*. <https://www.trade.gov/country-commercial-guides/singapore-information-and-telecommunications-technology>
- Internet Society. (2022). *Navigating digital sovereignty and its impact on the Internet*.



- Israel, E., & Boadle, A. (2013, October 29). Brazil to insist on local Internet data storage after U.S. spying. *Reuters*. <https://www.reuters.com/article/net-us-brazil-internet-idINBRE99R10Q20131028>
- Iu, K. Y., & Wong, V. M. (2022). The trans-national cybercrime court: Towards a new harmonisation of cyber law regime in ASEAN. *Social Science Research Network*. <https://doi.org/10.2139/ssrn.4265726>
- Jamrisko, M. (2020, January 21). Singapore leaps up the rankings in Bloomberg's Innovation Index. *Bloomberg.com*. <https://www.bloomberg.com/news/articles/2020-01-20/singapore-leaps-in-innovation-index-amid-mixed-picture-in-asia>
- Janiszewski, M., Felkner, A., & Lewandowski, P. (2019). A novel approach to national-level cyber risk assessment based on vulnerability management and threat intelligence. *Journal of Telecommunications and Information Technology*. <https://doi.org/10.26636/jtit.2019.130919>
- Jones, C. I., & Tonetti, C. (2020). Nonrivalry and the economics of data. *The American Economic Review*, 110(9), 2819–2858. <https://doi.org/10.1257/aer.20191330>
- Kaloudis, M. (2021). Digital sovereignty—European Union's action plan needs a common understanding to succeed. *History Compass*, 19(12). <https://doi.org/10.1111/hic3.12698>
- Kanth, D. R. (2019, June 30). India boycotts "Osaka Track" at G20 summit. *Mint*. <https://www.livemint.com/news/world/india-boycotts-osaka-track-at-g20-summit-1561897592466.html>
- Keane, J. (2021, April 8). From California to Brazil: Europe's privacy laws have created a recipe for the world. *CNBC*. <https://www.cnbc.com/2021/04/08/from-california-to-brazil-gdpr-has-created-recipe-for-the-world.html>
- Kennedy, S. (2015, June 1). *Made in China 2025*. Center for Strategic and International Studies. <https://www.csis.org/analysis/made-china-2025>
- Kolozaridi, P., & Muravyov, D. (2021). Contextualizing sovereignty: A critical review of competing explanations of the Internet governance in the (so-called) Russian case. *First Monday*. <https://doi.org/10.5210/fm.v26i5.11687>
- Koskeniemi, M. (2009). *From apology to utopia: The structure of international legal argument*. Cambridge University Press.
- Kothe, E. J., Mullan, B. A., & Butow, P. (2012). Promoting fruit and vegetable consumption: Testing an intervention based on the theory of planned behaviour. *Appetite*, 58(3), 997–1004. <https://doi.org/10.1016/j.appet.2012.02.012>
- Krasner, S. D. (1988). Sovereignty. *Comparative Political Studies*, 21(1), 66–94. <https://doi.org/10.1177/0010414088021001004>
- Kurohi, R. (2022, July 19). S'pore organisations among most targeted in the world by ransomware attacks, study finds. *The Straits Times*. <https://www.straitstimes.com/tech/tech-news/spore-organisations-among-most-targeted-in-the-world-by-ransomware-attacks-study-finds>

- Kwet, M. (2019a, March 13). Digital colonialism is threatening the Global South. *Al Jazeera*. <https://www.aljazeera.com/opinions/2019/3/13/digital-colonialism-is-threatening-the-global-south>
- Kwet, M. (2019b). Digital colonialism: US empire and the new imperialism in the Global South. *Race & Class*, 60(4), 3–26. <https://doi.org/10.1177/0306396818823172>
- Kyger, L. (2019, February 21). “Data localization” and other barriers to digital trade. Hinrich Foundation. <https://www.hinrichfoundation.com/research/tradevistas/digital/data-localization/>
- Lahmann, H. (2021). On the politics and ideologies of the sovereignty discourse in cyberspace. *Duke Journal of Comparative & International Law*, 32(61). [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3834332](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3834332)
- Lai, L. (2019, September 25). Examples of foreign interference in the course of history and in Singapore. *The Straits Times*. <https://www.straitstimes.com/politics/examples-of-foreign-interference-in-the-course-of-history-and-in-singapore>
- Lambach, D., & Oppermann, K. (2022). Narratives of digital sovereignty in German political discourse. *Governance*. <https://doi.org/10.1111/gove.12690>
- Larsen, B. C. (2022, December 8). *The geopolitics of AI and the rise of digital sovereignty*. Brookings. <https://www.brookings.edu/research/the-geopolitics-of-ai-and-the-rise-of-digital-sovereignty/>
- Latimer, J., Cerise, S., Ovseiko, P. V., Rathborne, J. M., Billiards, S. S., & El-Adhami, W. (2019). Australia’s strategy to achieve gender equality in STEM. *The Lancet*, 393(10171), 524–526. [https://doi.org/10.1016/s0140-6736\(18\)32109-3](https://doi.org/10.1016/s0140-6736(18)32109-3)
- Lee, D., Maldoff, G., & Wimmer, K. (2020, March). *Comparison: Indian Personal Data Protection Bill 2019 vs. GDPR*. <https://iapp.org/resources/article/comparison-indian-personal-data-protection-bill-2019-vs-gdpr/>
- Lee, H., & Pollitzer, E. (2016). *Gender in science and innovation as component of inclusive socioeconomic growth*. Portia Ltd. [https://gender-summit.com/images/Gender\\_and\\_inclusive\\_innovation\\_Gender\\_Summit\\_report.pdf](https://gender-summit.com/images/Gender_and_inclusive_innovation_Gender_Summit_report.pdf)
- Lewis, J. A. (2010). Sovereignty and the role of government in cyberspace. *The Brown Journal of World Affairs*, 16(2), 55–65. <http://www.jstor.org/stable/24590909>
- Li, X. (2022, August 10). Indonesia won’t go with the flow on data. *East Asia Forum*. <https://www.eastasiaforum.org/2022/08/10/indonesia-wont-go-with-the-flow-on-data/>
- Lim, D. (2019, August 8). *Bringing data into the heart of digital government*. Civil Service College. <https://www.csc.gov.sg/articles/bring-data-in-the-heart-of-digital-government>
- Lim, J. (2021). Bite the bullet: The future of data protection law and policy in ASEAN. *ASEAN Ideas in Progress Series 4/2021*. Centre for International Law. <https://cil.nus.edu.sg/wp-content/uploads/2021/06/ALA-Ideas-in-Progress-Series-4.-Jonathan-Lim.pdf>
- Liu, R. (2022, March 24). Behind these Singapore tech firms’ successful expansions abroad. *Tech in Asia*. <https://www.techinasia.com/singapore-tech-firms-successful-expansions>

- Low, J. R. (2022, September 19). Commentary: Will the Internet of tomorrow become several intranets instead? Geopolitics could be key. *Today*. <https://www.todayonline.com/commentary/commentary-will-internet-tomorrow-become-several-intranets-instead-geopolitics-could-be-key-1996621>
- Lui, B., Ng, V., Ng, G., & Hirsch, W. R. (2022, August 2). *Singapore Personal Data Protection Act changes have implications for healthcare sector*. Morgan Lewis. <https://www.morganlewis.com/pubs/2022/08/singapore-personal-data-protection-act-changes-have-implications-for-healthcare-sector>
- Madiega, T. (2020). *Digital sovereignty for Europe*. European Parliamentary Research Service.
- Mahmud, A. H. (2022, February 18). Budget 2022: Minimum qualifying salary for new EP, S Pass applicants to go up by S\$500 from September. CNA. <https://www.channelnewsasia.com/singapore/foreign-worker-pass-permit-salary-ep-s-pass-2506511>
- Maizland, L. (2020, August 6). *Huawei: China's controversial tech giant*. Council on Foreign Relations. <https://www.cfr.org/backgrounder/huawei-chinas-controversial-tech-giant>
- Martens, M., De Wolf, R., & De Marez, L. (2019). Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general. *Computers in Human Behavior*, 92, 139–150. <https://doi.org/10.1016/j.chb.2018.11.002>
- Martinet, L. (2021, June 30). Exercising digital sovereignty over blockchains: A case study from France. *Stanford Journal of Blockchain Law & Policy*. <https://stanford-jblp.pubpub.org/pub/digital-sovereignty-and-blockchain/release/1>
- McCulloch, C., & Watts, S. (2021). *Evaluating the effectiveness of public communication campaigns and their implications for strategic competition with Russia*. RAND Corporation. [https://www.rand.org/pubs/research\\_reports/RRA412-2.html](https://www.rand.org/pubs/research_reports/RRA412-2.html)
- McKune, S. L., & Ahmed, S. (2018). The contestation and shaping of cyber norms through China's internet sovereignty agenda. *International Journal of Communication*, 12, 3835–3855. <https://ijoc.org/index.php/ijoc/article/view/8540/2461>
- Meltzer, J. P., & Lovelock, P. (2018, March 20). *Regulating for a digital economy: Understanding the importance of cross-border data flows in Asia*. Brookings. <https://www.brookings.edu/research/regulating-for-a-digital-economy-understanding-the-importance-of-cross-border-data-flows-in-asia/>
- Mercier, L. (1997). The Communications Decency Act, Congress' first attempt to censor speech over the internet. *Loyola Consumer Law Review*, 9(3), 15. <http://lawecommons.luc.edu/lclr/vol9/iss3/15>
- Microsoft & International Data Corporation. (2019, April 16). *Less than 1 in 4 Singapore consumers trust organisations that provide digital services to protect their personal data: Microsoft — IDC Study*. Microsoft. <https://news.microsoft.com/en-sg/2019/04/16/less-than-1-in-4-singapore-consumers-trust-organisations-that-provide-digital-services-to-protect-their-personal-data-microsoft-idc-study/>
- Microsoft. (2022, September 20). *Argentina Personal Data Protection Act (PDPA)*. <https://learn.microsoft.com/en-us/compliance/regulatory/offering-pdpa-argentina>

- Miller, C. C. (2014, March 21). Revelations of N.S.A. spying cost U.S. tech companies. *The New York Times*. <https://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html>
- Milner, E. (2021, August 26). *Cyber-enabled foreign influence and interference*. Australian Army Research Centre. <https://researchcentre.army.gov.au/library/land-power-forum/cyber-enabled-foreign-influence-and-interference>
- Ministry of Defence. (2022, October 28). *Fact sheet: The digital and intelligence service*. [https://www.mindef.gov.sg/web/portal/mindef/news-and-events/latest-releases/article-detail/2022/October/28oct22\\_fs](https://www.mindef.gov.sg/web/portal/mindef/news-and-events/latest-releases/article-detail/2022/October/28oct22_fs)
- Ministry of Digital Affairs. (n.d.). *Cybersecurity Strategy of the Republic of Poland for 2019–2024*. <https://www.gov.pl/attachment/6a4aafc6-e339-4cd5-a8e6-cd47257f02d8>
- Ministry of Foreign Affairs. (2022, February 24). *Singapore's reply to a joint communication from special procedures mandate holders on the foreign interference (Countermeasures) Act*. <https://www.mfa.gov.sg/Overseas-Mission/Geneva/Mission-Updates/2022/02/Sgp-reply-to-a-JC-frm-SPMHs-Foreign-Interference>
- Ministry of Home Affairs. (2017, March 9). *Computer Misuse and Cybersecurity (Amendment) Bill* [Press release]. <https://www.mha.gov.sg/mediaroom/press-releases/computer-misuse-and-cybersecurity-amendment-bill/>
- Ministry of Trade and Industry Singapore. (n.d.-a). What are *Digital Economy Agreements (DEAs)*? <https://www.mti.gov.sg/Trade/Digital-Economy-Agreements>
- Ministry of Trade and Industry. (n.d.-b). *The Comprehensive and Progressive Agreement for Trans-Pacific Partnership*. <https://www.mti.gov.sg/Trade/Free-Trade-Agreements/CPTPP>
- Ministry of Trade and Industry. (n.d.-c). *Regional Comprehensive Economic Partnership (RCEP) Agreement*. <https://www.mti.gov.sg/Trade/Free-Trade-Agreements/RCEP>
- Ministry of Trade and Industry. (2017). *Economic Survey of Singapore: Third Quarter 2017*. <https://www.mti.gov.sg/Resources/Economic-Survey-of-Singapore/2017/Economic-Survey-of-Singapore-Third-Quarter-2017>
- Ministry of Trade and Industry. (2023, February 16). *Singapore and the European Free Trade Association launch negotiations on Digital Economy Agreement* [Press release]. <https://www.mti.gov.sg/Newsroom/Press-Releases/2023/02/Singapore-and-the-European-Free-Trade-Association-Launch-Negotiations-On-Digital-Economy-Agreement>
- Mishra, N. (2015). Data localization laws in a digital world: Data protection or data protectionism? *The Public Sphere*. <https://ssrn.com/abstract=2848022>
- Mishra, N. (2019). Building bridges: International trade law, internet governance, and the regulation of data flows. *Vanderbilt Journal of Transnational Law*, 52, 463. <https://scholarship.law.vanderbilt.edu/vjtl/vol52/iss2/4>
- Moerel, L., & Timmers, P. (2021). Reflections on digital sovereignty. *EU Cyber Direct, Research in Focus series 2021*. <https://ssrn.com/abstract=3772777>

- Monetary Authority of Singapore. (2020, February 6). *United States-Singapore joint statement on financial services data connectivity* [Press release]. <https://www.mas.gov.sg/news/media-releases/2020/united-states-singapore-joint-statement-on-financial-services-data-connectivity>
- Morey, T., Forbath, T., & Schoop, A. (2015, May). Customer data: Designing for transparency and trust. *Harvard Business Review*. <https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust>
- Mozur, P., Kang, C., Satariano, A., & McCabe, D. (2021, April 20). A global tipping point for reining in tech has arrived. *The New York Times*. <https://www.nytimes.com/2021/04/20/technology/global-tipping-point-tech.html>
- Mueller, M. (2002). *Ruling the root: Internet governance and the taming of cyberspace*. MIT Press.
- Mukherjee, S. (2022, June 22). Swedish court upholds ban on Huawei sale of 5G gear. *Reuters*. <https://www.reuters.com/business/media-telecom/swedish-court-upholds-ban-huawei-sale-5g-gear-2022-06-22/>
- Murphy, H., Criddle, C., & McMorow, R. (2023, March 22). TikTok caught in US-China battle over its powerful algorithm. *Financial Times*. <https://www.ft.com/content/b9f3b5a8-19ae-407f-be4b-e2536617b0f8>
- Musiani, F. (2022). *Infrastructuring digital sovereignty: A research agenda for an infrastructure-based sociology of digital self-determination practices*. *Information, Communication & Society*, 25(6), 785–800. <https://doi.org/10.1080/1369118x.2022.2049850>
- Nagan, W. P., & Hammer, C. (2004). The changing character of sovereignty in international law and international relations. *Columbia Journal of Transnational Law*, 43(1), 141–187.
- Nanyang Technological University. (2021, March 5). *New programme to encourage more women to pursue education and careers in STEM* [Press release]. <https://www.ntu.edu.sg/news/detail/new-programme-to-encourage-more-women-to-pursue-education-and-careers-in-stem>
- National Cyber Security Centre. (n.d.). *What is cyber security?* <https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security>
- National Privacy Commission. (2019, August 22). *PH leads ASEAN's move to protect privacy*. <https://www.privacy.gov.ph/2019/08/ph-leads-asean-move-to-protect-privacy/>
- National Research Council. (1999). *Funding a revolution: Government support for computing research*. National Academies Press. <https://doi.org/10.17226/6323>
- Ng, J. S. (2021, February 6). The big read: As tech titans converge in Singapore, can it truly become Asia's Silicon Valley? CNA. <https://www.channelnewsasia.com/singapore/big-read-tech-titans-converge-singapore-asia-silicon-valley-324046>
- Nguyen, P. (2019, May 8). *"Make in Vietnam" campaign targets top 30 IT status*. VN Express. <https://e.vnexpress.net/news/business/industries/make-in-vietnam-campaign-targets-top-30-it-status-3920371.html>

- O'Connor, S., Hanson, F., Currey, E., & Beattie, T. (2020). *Cyber-enabled foreign interference in elections and referendums*. Australian Strategic Policy Institute. <https://www.aspi.org.au/report/cyber-enabled-foreign-interference-elections-and-referendums>
- Office of the United Nations High Commissioner for Human Rights. (2022). *The right to privacy in the digital age* (A/HRC/51/17).
- Organisation for Economic Co-operation and Development. (2019). Economic and social benefits of data access and sharing. In *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*, Chapter 3, OECD Publishing, 2019. [https://www.oecd-ilibrary.org/sites/276aaca8-en/1/2/3/index.html?itemId=/content/publication/276aaca8-en&\\_csp\\_=a1e9fa54d39998ecc1d83f19b8b0fc34&itemIGO=oecd&itemContentType=book](https://www.oecd-ilibrary.org/sites/276aaca8-en/1/2/3/index.html?itemId=/content/publication/276aaca8-en&_csp_=a1e9fa54d39998ecc1d83f19b8b0fc34&itemIGO=oecd&itemContentType=book)
- Oxman, J. (1999). *The FCC and the unregulation of the internet*. Federal Communications Commission. <https://www.fcc.gov/reports-research/working-papers/fcc-and-unregulation-internet>
- Palfrey, J. (2010). Four phases of internet regulation. *Social Research*, 77(3), 981–996. <https://doi.org/10.1353/sor.2010.0021>
- Pankajakshan, B. (2022, August 31). Hyperscalers can redefine mobile telecommunications networks. *Forbes*. <https://www.forbes.com/sites/forbestechcouncil/2022/08/31/hyperscalers-can-redefine-mobile-telecommunications-networks/?sh=db11881418ba>
- Passani, A., Spagnoli, F., Bellini, F., Prampolini, A., & Firus, K. (2015). Collective awareness platform for sustainability and social innovation (CAPS). *Lecture Notes in Information Systems and Organisation*, 103–114. [https://doi.org/10.1007/978-3-319-22921-8\\_9](https://doi.org/10.1007/978-3-319-22921-8_9)
- Pawelec, M. (2022). Deepfakes and democracy (theory): How synthetic audio-visual media for disinformation and hate speech threaten core democratic functions. *Digital Society*, 1(2). <https://doi.org/10.1007/s44206-022-00010-6>
- Perarnaud, C., Rossi, J., Musiani, F., & Castex, L. (2022). *“Splinternets”: Addressing the renewed debate on internet fragmentation* (PE 729.530). European Parliamentary Research Service. [https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729530/EPRS\\_STU\(2022\)729530\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729530/EPRS_STU(2022)729530_EN.pdf)
- Perritt, H. H. Jr. (1998). The internet as a threat to sovereignty? Thoughts on the internet's role in strengthening national and global governance. *Indiana Journal of Global Legal Studies*, 5(2), 423. [https://scholarship.kentlaw.iit.edu/cgi/viewcontent.cgi?article=1497&context=fac\\_schol](https://scholarship.kentlaw.iit.edu/cgi/viewcontent.cgi?article=1497&context=fac_schol)
- Personal Data Protection Commission. (2017). *Advisory Guidelines on Key Concepts in the PDPA*. [https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/the-transfer-limitation-obligation---ch-19-\(270717\).pdf](https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/the-transfer-limitation-obligation---ch-19-(270717).pdf)
- Personal Data Protection Commission. (2019, September 9). *MOU between PH NPC and PDPC*. <https://www.pdpc.gov.sg/news-and-events/announcements/2019/09/mou-between-ph-npc-and-pdpc>

- Personal Data Protection Commission. (2022, July 13). *Hong Kong and Singapore authorities renew MOU to maintain close ties and foster closer collaboration in personal data protection* [Press release]. <https://www.pdpc.gov.sg/news-and-events/press-room/2022/07/hong-kong-and-singapore-authorities-renew-mou-to-maintain-close-ties-and-foster-closer-collaboration-in-personal-data-protection>
- Personal Data Protection Commission. (n.d.-a). *About Us*. <https://www.pdpc.gov.sg/Who-We-Are/About-Us>
- Personal Data Protection Commission. (n.d.-b). *PDPA overview*. <https://www.pdpc.gov.sg/overview-of-pdpa/the-legislation/personal-data-protection-act>
- Personal Data Protection Commission. (n.d.-c). *ASEAN Data Management Framework and model contractual clauses on cross border data flows*. <https://www.pdpc.gov.sg/help-and-resources/2021/01/asean-data-management-framework-and-model-contractual-clauses-on-cross-border-data-flows>
- Peters, A., & Jordan, A. (2019, October 2). *Countering the cyber enforcement gap: Strengthening global capacity on cybercrime*. Third Way Cyber Enforcement Initiative. <https://www.thirdway.org/report/countering-the-cyber-enforcement-gap-strengthening-global-capacity-on-cybercrime>
- Philpott, D. (1995). Sovereignty: An introduction and brief history. *Journal of International Affairs*, 48(2), 353. <https://www.questia.com/library/journal/1G1-16714038/sovereignty-an-introduction-and-brief-history>
- Pohle, J. (2020). *Digital sovereignty: A new key concept of digital policy in Germany and Europe*. Konrad-Adenauer-Stiftung.
- Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, 9(4). <https://doi.org/10.14763/2020.4.1532>
- Pradhan, B., & Kumar, S. (2022, November 18). India to ease data storage rules in relief for Google, Meta. *Bloomberg*. <https://www.bloomberg.com/news/articles/2022-11-18/india-s-new-data-protection-bill-seeks-to-ease-storage-norms>
- Prime Minister's Office Singapore. (2019, November 27). *Government accepts recommendations of the Public Sector Data Security Review Committee*. <https://www.pmo.gov.sg/Newsroom/Govt-Accepts-Recommendations-of-Public-Sector-Data-Security-Review-Committee>
- Public Sector Data Security Review Committee. (2019). *Annexes to the Public Sector Data Security Review Committee Report*. <https://www.smartnation.gov.sg/files/publications/annexes-to-the-psdsr-final-report.pdf>
- Public Service Division. (n.d.). *Establishing our place in the world*. <https://www.psd.gov.sg/HOPS/our-institutions/establishing-our-place-in-the-world/>
- Puglierin, J. (2022, June). *European Sovereignty Index*. European Council on Foreign Relations. <https://ecfr.eu/special/sovereignty-index/>
- Putin signs internet isolation bill into law. (2019, May 1). *The Moscow Times*. <https://www.themoscowtimes.com/2019/05/01/putin-signs-internet-isolation-bill-into-law-a65461>

- QBE Insurance. (2023, March 20). *QBE SME survey: Singapore SMEs not digitalising at full potential, also ignoring threats to their cybersecurity* [Press release].  
[https://www.qbe.com/sg/-/media/singapore/files/sme%20research/2023/qbe%20sme%202023%20release\\_digitalisation\\_14%20mar\\_final\\_combined\\_003.pdf](https://www.qbe.com/sg/-/media/singapore/files/sme%20research/2023/qbe%20sme%202023%20release_digitalisation_14%20mar_final_combined_003.pdf)
- Radu, R. (2019). *Negotiating internet governance*. Oxford University Press.
- Raemdonck, N. V. (2021). *Cyber diplomacy in Southeast Asia*. EU Cyber Direct.  
<https://eucyberdirect.eu/research/cyber-diplomacy-in-southeast-asia>
- Ramos, J. M. (2013). Sovereignty. In *Changing norms through actions: The evolution of sovereignty* (pp.1–22). Oxford Academic.  
<https://doi.org/10.1093/acprof:oso/9780199924844.003.0001>
- Raska, M., & Ang, B. (2018). *Cybersecurity in Southeast Asia*. Asia Centre.  
[https://centreasia.eu/wp-content/uploads/2018/12/NotePre%CC%81sentation-AngRaska-Cybersecurity\\_180518.pdf](https://centreasia.eu/wp-content/uploads/2018/12/NotePre%CC%81sentation-AngRaska-Cybersecurity_180518.pdf)
- Reuters Staff. (2017, July 19). China's cyber watchdog orders top tech platforms to increase self-censorship. *Reuters*. <https://www.reuters.com/article/us-china-censorship-idUSKBN1A41CS>
- Reuters Staff. (2018, November 12). Singapore central bank chief warns of risks to data localisation measures. *Reuters*. <https://www.reuters.com/article/singapore-cenbank-idUSL4N1XN2G9>
- Ringhand, L. A. (2021). Foreign election interference: Comparative approaches to a global challenge. *Election Law Journal: Rules, Politics, and Policy*, 1–9.
- Rolland, N., Horton, C., Cathcart, A., Worden, A., Szczudlik, J., Oud, M., Segal, A., & Pornet, A. (2020). An emerging China-centric order: China's vision for a new world order in practice. *NBR Special Report no. 87*. The National Bureau of Asian Research.  
<https://www.nbr.org/publication/an-emerging-china-centric-order-chinas-vision-for-a-new-world-order-in-practice/>
- Rosenberg, M., & Frenkel, S. (2018, March 18). Facebook's role in data misuse sets off storms on two continents. *The New York Times*.  
<https://www.nytimes.com/2018/03/18/us/cambridge-analytica-facebook-privacy-data.html>
- Rudolph, C. (2005). Sovereignty and territorial borders in a global age. *International Studies Review*, 7(1), 1–20. <https://doi.org/10.1111/j.1521-9488.2005.00455.x>
- Salesforce. (2019). *Data beyond borders: Optimising movement and protection mechanisms for cross-border data flows in G20 economies*.  
[https://www.salesforce.com/content/dam/web/en\\_sg/www/documents/pdf/data-beyond-borders-report.pdf](https://www.salesforce.com/content/dam/web/en_sg/www/documents/pdf/data-beyond-borders-report.pdf)
- Schjolberg, S. (2011). Potential new global legal mechanisms on combating cybercrime and global cyberattacks. *Cybercrime Law*. The ISPAC International Conference on Cybercrime: Global Phenomenon and its Challenges, Courmayeur, Italy.  
<https://cybercrimelaw.net/documents/ISPAC.pdf>



- Schmidt, P., Gordoni, G., Ajzen, I., Beuthner, C., Davidov, E., Silber, H., Steinmetz, H., & Weiß, B. (2022). Twitter users' privacy behavior: A reasoned action approach. *Social Media + Society*, 8(3). <https://doi.org/10.1177/20563051221126085>
- Scott, M., & Cerulus, L. (2019, June 16). Russian groups targeted EU election with fake news, says European Commission. *Politico*. <https://www.politico.eu/article/european-commission-disinformation-report-russia-fake-news/>
- Selby, J. (2017). Data localization laws: Trade barriers or legitimate responses to cybersecurity risks, or both? *International Journal of Law and Information Technology*, 25(3), 213–232. <https://doi.org/10.1093/ijlit/eax010>
- Shahani, A. (2014, June 5). A year after Snowden, U.S. tech losing trust overseas. *NPR*. <https://www.npr.org/sections/alltechconsidered/2014/06/05/318770896/a-year-after-snowden-u-s-tech-losing-trust-overseas>
- Shahbaz, A., & Funk, A. (2021). *The global drive to control big tech*. Freedom House. <https://freedomhouse.org/report/freedom-net/2021/global-drive-control-big-tech>
- Yayboke, E., Ramos, C. G., & Sheppard, L. R. (2021). *The real national security concerns over data localization*. Center for Strategic & International Studies. <https://www.csis.org/analysis/real-national-security-concerns-over-data-localization>
- Sherman, J. J. (2022). China's war for control of global internet governance. *Social Science Research Network*. <https://doi.org/10.2139/ssrn.4174453>
- Singapore the most connected country in the world. (2016, February 26). *Today*. <https://www.todayonline.com/singapore/singapore-most-connected-country-world>
- Smart Nation and Digital Government Office. (n.d.-a). *Digital economy*. <https://www.smartnation.gov.sg/about-smart-nation/digital-economy/>
- Smart Nation and Digital Government Office (n.d.-b). *Data resources & APIs*. <https://www.smartnation.gov.sg/resources/open-data/>
- Smart Nation and Digital Government Office. (2018). *Smart Nation: The way forward*. <https://www.smartnation.gov.sg/files/publications/smart-nation-strategy-nov2018.pdf>
- Smith, R. (2020). Cybercrime in Asean: Anti-child pornography legislation. *Journal of Indonesian Legal Studies*, 5(2), 277–294.
- Steiger, S., Schünemann, W. J., & Dimmroth, K. (2017). Outrage without consequences? Post-Snowden discourses and governmental practice in Germany. *Media and Communication*, 5(1), 7–16. <https://doi.org/10.17645/mac.v5i1.814>
- Stucke, M. E. (2018). Should we be concerned about data-opolies? *Social Science Research Network*. <https://doi.org/10.2139/ssrn.3144045>
- Subhani, O. (2020, December 3). Singapore ranked world's second-most connected country in DHL index. *The Straits Times*. <https://www.straitstimes.com/business/economy/singapore-ranked-worlds-second-most-connected-country-in-dhl-index>
- Surfshark. (2022, July 26). *Government surveillance report*. <https://surfshark.com/user-data-surveillance-report>

- Suvannaphakdy, S. (2022). *2022/67 Better safeguards needed for trusted data use in ASEAN countries*. ISEAS-Yusof Ishak Institute. <https://www.iseas.edu.sg/articles-commentaries/iseas-perspective/2022-67-better-safeguards-needed-for-trusted-data-use-in-asean-countries-by-sithanoxay-suvannaphakdy/>
- Svantesson, D. J. B. (2019). *Internet & jurisdiction global status report 2019*. Internet & Jurisdiction Policy Network. <https://www.internetjurisdiction.net/news/release-of-worlds-first-internet-jurisdiction-global-status-report>
- Swanson, A. (2022, December 16). US cracks down on Chinese companies for security concerns. *The New York Times*. <https://www.nytimes.com/2022/12/15/business/economy/us-china-biden-security.html>
- Swire, P., & Kennedy-Mayo, D. (2022). The effects of data localization on cybersecurity. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.4030905>
- Synergy Research Group. (2020, October 29). Cloud market growth rate nudges up as Amazon and Microsoft solidify leadership. <https://www.srgresearch.com/articles/cloud-market-growth-rate-nudges-amazon-and-microsoft-solidify-leadership>
- Tan, B., & Zhou, Y. (2018). *Urban systems studies: Technology and the city — foundation for a smart nation*. Centre for Liveable Cities. <https://www.clc.gov.sg/research-publications/publications/urban-systems-studies/view/technology-and-the-city>
- Tan, M. (1999). Creating the digital economy: Strategies and perspectives from Singapore. *International Journal of Electronic Commerce*, 3(3), 105–122. <https://doi.org/10.1080/10864415.1999.11518344>
- Tan, S. (2023, February 6). *Data privacy: How concerned are consumers in APAC — and does it affect the devices they buy?* YouGov. <https://sg.yougov.com/en-sg/news/2023/02/06/data-privacy-APAC-devices-Sep2022/>
- Tan, T. K. Y. (2005, February 22). *Launch of the Infocomm Security Masterplan* [Speech]. Infocomm Security Seminar 2005, Singapore. <https://www.imda.gov.sg/content-and-news/press-releases-and-speeches/archived/ida/speeches/2005/20050717163018>
- Tay, S., & Wu, J. (2022). *Asia and digital economy agreements: Necessity and uncertainty*. European University Institute. <https://hdl.handle.net/1814/74766>
- Teng, A. (2022, March 30). Girls fare just as well as boys in science and maths but later feel less confident in their abilities: NTU study. *The Straits Times*. <https://www.straitstimes.com/singapore/girls-fare-just-as-well-as-boys-in-science-and-maths-but-later-feel-less-confident-in-their-abilities-ntu-study>
- Teo, J. (2022a, March 24). *Speech by Mrs Josephine Teo, Minister for Communications and Information, at Future Economy Conference & Exhibition, on 24 March 2022*. Future Economy Conference & Exhibition, Singapore. <https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2022/3/speech-by-minister-josephine-teo-at-future-economy-conference-and-exhibition-on-24-march-2022?category=Infocomm+Media>
- Teo, J. (2022b, December 1). *Speech by Minister of Communications and Information Josephine Teo at the Global Technology Summit on 1 December 2022*. Global Technology Summit, India. <https://www.mci.gov.sg/pressroom/news-and->

stories/pressroom/2022/12/speech-by-minister-of-communications-and-information-josephine-teo-at-the-global-technology-summit-on-1-december-2022

- Thailand's digital transformation boosts data industry. (2021, July 2). *Bangkok Post*. <https://www.bangkokpost.com/business/2142475/thailands-digital-transformation-boosts-data-industry>
- Tham, I. (2022, August 24). Threat of data blackout looms. *The Straits Times*. <https://www.straitstimes.com/opinion/techtalk-threat-of-data-blackout-looms>
- The NATO Cooperative Cyber Defence Centre of Excellence. (n.d.). *ASEAN to focus on cybersecurity capacity- and confidence-building in 2017*. <https://ccdcoe.org/incyder-articles/asean-to-focus-on-cybersecurity-capacity-and-confidence-building-in-2017/>
- The world's most valuable resource is no longer oil, but data. (2017, May 6). *Economist*. [https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data?gclid=CjwKCAjwiOCgBhAgEiwAjv5whLQGSv3kokeHrRounTq90qy-EqECzt-K0KrKI8rsgHtneXy381M1CxoCjZIQAvD\\_BwE&gclsrc=aw.ds](https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data?gclid=CjwKCAjwiOCgBhAgEiwAjv5whLQGSv3kokeHrRounTq90qy-EqECzt-K0KrKI8rsgHtneXy381M1CxoCjZIQAvD_BwE&gclsrc=aw.ds)
- Thumfart, J. (2022). The norm development of digital sovereignty between China, Russia, the EU and the US: From the late 1990s to the COVID crisis 2020/21 as catalytic event. *Hart Publishing EBooks*. <https://doi.org/10.5040/9781509954544.ch-001>
- To, C., & Cheung, H. (2023, February 21). *ASEAN: Market profile*. HKTDC Research. <https://research.hktdc.com/en/article/Mzk5MzcxNjEz>
- Un, C. (2020, October 14). *It's time for the Asia-Pacific to move toward regional cyber norms*. *The Diplomat*. <https://thediplomat.com/2020/10/its-time-for-the-asia-pacific-to-move-toward-regional-cyber-norms/>
- United Nations Conference on Trade and Development. (n.d.). *Data protection and privacy legislation worldwide*. <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>
- United Overseas Bank. (2022a). *Digitalisation for SMEs: How to beat decision fatigue and find the right tech solution*. <https://www.uobgroup.com/techecosystem/news-insights-digitalisation-and-decision-fatigue.html>
- United Overseas Bank. (2022b, March 3). *2 in 3 tech-savvy small businesses bullish on future growth*. <https://www.uobgroup.com/asean-insights/articles/sme-outlook-study-2022-digitalisation.page>
- Verma, R. (2022, September 7). Indian government to come up with a revised data protection bill and telecom bill. *Business Insider*. <https://www.businessinsider.in/india/news/indian-government-to-come-up-with-a-new-iteration-of-the-data-protection-bill-and-telecom-bill/articleshow/94051561.cms>
- Volkmer, I. (2021). Digital sovereignty and approaches to governing globalized data spaces. In *Band 21 cultural sovereignty beyond the modern state* (pp.128–146). De Gruyter. <https://doi.org/10.1515/9783110679151-007>
- Walt, V. (2020, May 6). Europe's digital czar says COVID-19 gives big tech a chance to redeem itself. *Time*.

- Wang, A. (2020). Cyber sovereignty at its boldest: A Chinese perspective. *Ohio State Technology Law Journal*, 16(2), 395–466. <http://hdl.handle.net/1811/92276>
- Wang, O. (2022, December 13). China files WTO suit against US over chip export controls, saying policy is “trade protectionism”. *South China Morning Post*. <https://www.scmp.com/news/china/article/3203066/china-files-wto-suit-against-us-over-chip-export-controls-saying-policy-trade-protectionism>
- Warren, M., & Fan, Z. (2022, August 24). *Digital economy agreements are a new frontier for trade — here’s why*. World Economic Forum.
- Wirecard & Blackbox. (2020). *2020 digital megatrends: Driving digitalization of Singaporean consumers*. [https://blackbox.com.sg/wp-content/uploads/2020/06/wirecard\\_report\\_a4\\_v5\\_\\_19\\_may.pdf](https://blackbox.com.sg/wp-content/uploads/2020/06/wirecard_report_a4_v5__19_may.pdf)
- Wolford, B. (n.d.-a). Does the GDPR apply to companies outside of the EU? *GDPR.EU*. <https://gdpr.eu/companies-outside-of-europe/>
- Wolford, B. (n.d.-b). What is GDPR, the EU’s new data protection law? *GDPR.EU*. <https://gdpr.eu/what-is-gdpr>
- Wong, B. (2020). Data localization and ASEAN Economic Community. *Asian Journal of International Law*, 10(158), 158–180. <https://ssrn.com/abstract=3538943>
- Wong, D. J. (2021, October 28). *Google says 94% of Singaporeans still have crappy password practices*. Mashable SEA. <https://sea.mashable.com/tech/18044/google-says-94-of-singaporeans-still-have-crappy-password-practices>
- Wong, P. (2023, May 25). *Ambassador for Cyber Affairs and Critical Technology*. Minister for Foreign Affairs [Press release]. <https://www.foreignminister.gov.au/minister/penny-wong/media-release/ambassador-cyber-affairs-and-critical-technology>
- Wood, S., McFadden, M., Kaur, A., Schoentgen, A., Wongsaroj, S., Forsyth, G., & Wilkinson, L. (2020, August 5). *Digital sovereignty: The overlap and conflict between states, enterprise and citizens*. Plum Consulting. <https://plumconsulting.co.uk/digital-sovereignty-the-overlap-and-conflict-between-states-enterprise-and-citizens/>
- World Bank (n.d.). *Data protection and privacy laws*. <https://id4d.worldbank.org/guide/data-protection-and-privacy-laws>
- World Intellectual Property Organisation. (2023, February 21). Global Innovation Index 2022 — ASEAN and the future of innovation-driven growth. [https://www.wipo.int/about-wipo/en/offices/singapore/news/2023/news\\_0002.html](https://www.wipo.int/about-wipo/en/offices/singapore/news/2023/news_0002.html)
- Wu, E. (2021, July). *Sovereignty and data localization*. Belfer Center for Science and International Affairs.
- Wu, T. (1997). Cyberspace sovereignty? The internet and the international system. *Harvard Journal of Law & Technology*, 10, 647. [https://scholarship.law.columbia.edu/cgi/viewcontent.cgi?article=3239&context=faculty\\_scholarship](https://scholarship.law.columbia.edu/cgi/viewcontent.cgi?article=3239&context=faculty_scholarship)
- Yeo, S. (2021, June 30). Behind Singapore’s role as a regional tech hub. *Tech in Asia*. <https://www.techinasia.com/singapores-growth-regional-tech-hub>

Yeong, Z. K. (2021, September 9). *Speech by Deputy Commissioner, Mr Yeong Zee Kin, at 10th Asia Privacy Bridge Forum 2021, on 9 September 2021.*  
<https://www.pdpc.gov.sg/news-and-events/press-room/2021/09/speech-by-deputy-commr-mr-yeong-zee-kin-at-10th-asia-privacy-bridge-forum-2021-on-9-september-2021>

Zakhour, Z., & Gomes, V. (n.d.). *What is sovereignty and why it does matter?* Atos.  
<https://atos.net/en/lp/digital-sovereignty-cybersecurity-magazine/what-is-sovereignty-and-why-it-does-matter>

Zeng, J., Stevens, T., & Chen, Y. (2017). China's solution to global cyber governance: Unpacking the domestic discourse of "internet sovereignty." *Politics and Policy*, 45(3), 432–464. <https://doi.org/10.1111/polp.12202>

Zhu, J. (2022, December 14). Exclusive: China readying \$143 billion package for its chip firms in face of U.S. curbs. *Reuters*. <https://www.reuters.com/technology/china-plans-over-143-blb-push-boost-domestic-chips-compete-with-us-sources-2022-12-13/>