GSMA

Digital Nations in Asia Pacific

Preserving digital trust

GSMA

The GSMA is a global organisation unifying the mobile ecosystem to discover, develop and deliver innovation foundational to positive business environments and societal change. Our vision is to unlock the full power of connectivity so that people, industry and society thrive. Representing mobile operators and organisations across the mobile ecosystem and adjacent industries, the GSMA delivers for its members across three broad pillars: Connectivity for Good, Industry Services and Solutions and Outreach. This activity includes advancing policy, tackling today's biggest societal challenges, underpinning the technology and interoperability that make mobile work and providing the world's largest platform to convene the mobile ecosystem at the MWC and M360 series of events.

For more information, please visit the GSMA corporate website at www.gsma.com

Follow the GSMA: @GSMA

GSMA Intelligence

GSMA Intelligence is the definitive source of global mobile operator data, analysis and forecasts, and publisher of authoritative industry reports and research. Our data covers every operator group, network and MVNO in every country worldwide – from Afghanistan to Zimbabwe. It is the most accurate and complete set of industry metrics available, comprising tens of millions of individual data points, updated daily.

GSMA Intelligence is relied on by leading operators, vendors, regulators, financial institutions and third-party industry players, to support strategic decision-making and long-term investment planning. The data is used as an industry reference point and is frequently cited by the media and by the industry itself.

Our team of analysts and experts produce regular thought-leading research reports across a range of industry topics.

www.gsmaintelligence.com

info@gsmaintelligence.com

Authors

Kenechi Okeleke, Senior Director, GSMA Intelligence
James Joiner, Lead Analyst, GSMA Intelligence

Contributors

Jeanette Whyte, Head of Policy & External Affairs, GSMA Asia Pacific
Noriswadi Ismail, Senior Director - Data Privacy, GSMA
Syed Khairulazrin Bin Syed Khairuldin, Policy Director, GSMA Asia Pacific
Gulistan Ladha, Consumer Policy Director, GSMA
Natasha Nayak, Senior Policy Manager, GSMA Asia Pacific
Jessica Mills, Advocacy Coordinator, GSMA

Published September 2024

GSMA

Contents

Preface

In 2023, we published the eighth and final edition of the Digital Societies series, which focused on how countries in Asia Pacific were accelerating progress on their ambitions to become fully fledged digital societies. This was based on five components: connectivity, digital identity, digital citizenship, digital lifestyle and digital commerce.

The reports also chronicled the efforts of governments, the mobile industry and other stakeholders to bring citizens online, deliver life-enhancing services over digital channels and use digital platforms to tackle some of society's biggest challenges, including the Covid-19 pandemic.

In a fast-changing world characterised by growing concerns about the effect of climate change, diminishing supplies of resources relative to demand and political conflicts, resulting in new health and humanitarian emergencies, digitalisation has become the core element of nation building by integrating digital technologies and services into every sector of the economy.

Building on the foundation of the Digital Societies series, this report marks the inaugural edition of the Digital Nations series. It explores the aspirations of governments in Asia Pacific to leverage digital technologies as a means to achieve sustainable, resilient and inclusive economic growth, based on the development of five key components of a digital nation: infrastructure, innovation, data governance, security and people.

Executive summary

The widespread adoption of mobile technology during the last two decades has amplified the impact of digital technologies on economic growth and development, primarily by democratising access to digital services and enabling the creation of new industries while enhancing efficiency and productivity in existing ones. However, there has been a pivotal shift this decade in the role of digital technology from merely a platform to access various services to the foundation upon which economies are built. This scenario will define future digital nations.

Realising digital nations aspirations is a function of the five key components – infrastructure, innovation, data governance, security and people – of a digital nation. To this end, GSMA Intelligence has developed a new index to track the progress of 18 countries across Asia Pacific. The index serves as a tool for countries to assess their performance and identify areas that require improvement. Singapore, Australia and South Korea are the top-three countries in this year's index, while Papua New Guinea, Cambodia and Nepal are the lowest-ranked countries.

Meanwhile, digital trust has risen to the top of the agenda for policymakers and digital technology stakeholders. This is not too surprising, as the more pervasive digitalisation becomes and the more it replaces (or at least offers substitutes for) activities in the physical world, the more concerned citizens and organisations will be about the safety, privacy, security, reliability and ethics of the digital world.

High levels of digital trust build confidence among citizens and businesses, and justifies the investments into developing the components of a digital nation. Conversely, online threats that erode trust often have a significant and adverse impact on victims and wider society. Notably, they can reverse digital inclusion gains in affected communities, cause financial losses and reputational damage for people and businesses and take a mental toll on victims.

GSMA Intelligence has identified five key measures for governments, industry players and other stakeholders to preserve digital trust (see Figure i).

Preserving trust in the digital world is a collective effort, and all stakeholders – including policymakers, industry players, public and private organisations and citizens – have a role to play. In the coming years, governments and other stakeholders will make efforts to develop the five components of a digital nation. But it is also important for these stakeholders to take steps to preserve digital trust, considering the potential various threats to undermine the efforts to achieve their digital nation ambitions.

Figure i

Five key measures to preserve digital trust

Source: GSMA Intelligence

01
Defining a digital nation

Digitalisation has been at the heart of social and economic development in the biggest economies in Asia Pacific. It has also played an increasingly important role in the rapid growth of many emerging economies in the region.

The widespread adoption of mobile technology during the last two decades has amplified the impact of digital technologies on economic growth and development, primarily by democratising access to digital services and enabling the creation of new industries while enhancing efficiency and productivity in existing ones.

However, there has been a pivotal shift this decade in the role of digital technology from merely a platform to access various services to the foundation upon which economies are built. This mirrors the process of digital transformation in the corporate world, whereby an organisation integrates digital technology into all areas of a business, fundamentally changing how it operates and delivers value to customers and other stakeholders. Driving similar digital transformation across the wider economy and realising a digital-first approach to the way society operates will define future digital nations.

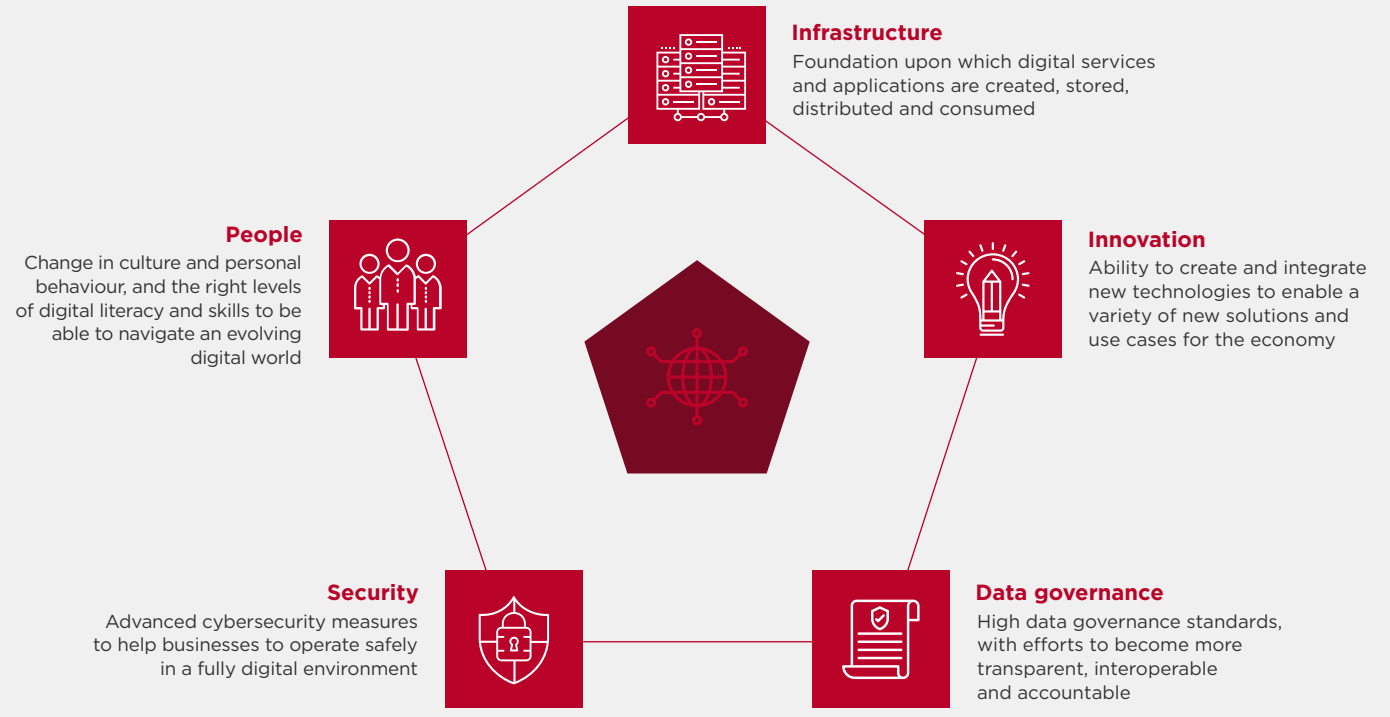
1.1
The components of a digital nation

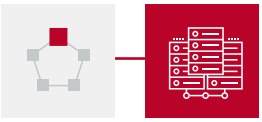
Based on the concept of a digital nation that describes a scenario where digitalisation is at the heart of nation building, with a coordinated effort to fully integrate digital technologies into every sector of the economy, GSMA Intelligence has identified five key components required to build a digital nation. These components (Figure 1) are interconnected and must be developed together to avoid potentially costly gaps and delays in the implementation of digitalisation initiatives.

Figure 1

The five components of a digital nation

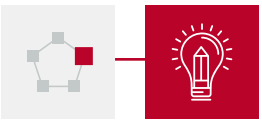
Source: GSMA Intelligence





Infrastructure

Infrastructure is the bedrock of a digital nation and the foundation upon which other components are built. This includes hard digital infrastructure (e.g. mobile networks, fibre and other fixed networks, satellite connectivity, data centres and data exchange systems) and soft digital infrastructure (e.g. digital ID systems and electronic payments and other digital transactions systems). The pace of transition to a digital nation correlates directly with available digital infrastructure, meaning it is imperative for the right policies to be put in place to attract investments into the development of various digital infrastructure.



Innovation

Innovation is required to create relevant digital solutions for different sectors of the economy. The global nature of digital technologies means innovation can be easily imported and applied locally. However, indigenous innovation will be crucial to accelerate progress on digital nation ambitions, given its potential to help build up a domestic skills and knowledge base that is more responsive to unique local challenges. Importantly, innovation in a digital nation needs to be continuous and sustained by a workforce that is capable of using various forms of technology to address new and existing challenges.

Data governance

Data governance describes the management of data based on applicable data protection legislative frameworks' data-processing activities (including access, collection, retention, transfer, copy, disclosure, modification, recording, updating and deletion). As countries progress towards digital nations, the large volume of digitised personal data and business information will exponentially increase. Emerging technologies such as AI rely on countless data sets, which individuals and organisations may consider sensitive. Having an applicable data governance policy and standard by embedding data protection principles is crucial to demonstrate accountability, transparency and trust in a digital ecosystem.

Security

Security in the digital world (referred to as cybersecurity) describes how individuals and organisations protect themselves and their assets from various forms of cyberattacks. The scope and scale of cyberattacks will inevitably increase as countries become digital nations, reflecting an expansion of the attack surface and increasing sophistication of threats that are leveraging technologies, such as AI, to evade detection. The borderless nature of digital technology also exposes potential targets to bad actors in other jurisdictions, making it more challenging for local authorities to deal with certain threats.

People

People's ability to engage effectively with the society around them is an essential part of nationhood. In a scenario where digital technology becomes the primary access point for key services, it is imperative for people to be adequately equipped to participate in society. There are two ways this needs to happen in a digital nation. First, it is essential to ensure that every individual has the right level of digital skills to interact with the society around them in a digital environment. Second, there needs to be a process in place to train the workforce and equip them with the necessary skills to support the workings of a digital nation.

1.2
Rationale for digital nation aspirations

Table 1 summarises the overriding rationale for envisioning digital nations aspirations. These are fairly consistent among governments and have been grouped into four broad categories.

Table 1

The rationale for digital nation aspirations split into four categories

Source: GSMA Intelligence

Resilience

Over the last five years there have been a number of global shocks – from the Covid-19 pandemic to political conflicts – that have disrupted established supply chains and stretched many economies to the limit, resulting in rising inflation, interest rate hikes and job losses. With prevailing uncertainties and the risk of further disruption, governments are increasingly leveraging digital technology to build economies that can better withstand future internal and external shocks.

Resources

Available resources are often limited and, in some cases, dwindling. At the same time, demand for services relying on those resources continues to rise, thereby creating a significant access gap for many social and economic necessities. For example, there is a shortage of skilled healthcare workers and teachers relative to the demand for health and education services. Digital technology offers a lifeline for governments to bridge such gaps and drive overall efficiency and productivity in the economy despite limited resources.

Sustainability

The need to protect the environment and meet decarbonisation goals has risen to the top of the agenda for governments and other stakeholders. Achieving this requires a rethink of conventional processes across many sectors of the economy to reduce waste, minimise energy consumption and cut greenhouse gas emissions. Examples of areas where digital technology is already having a significant impact on sustainability goals include enabling sustainable farming practices, clean mobility solutions and utility usage monitoring and remote control.

Inclusion

In some instances, there is a considerable access gap for certain key services. This is often driven by macro factors, such as income inequality and urban-rural disparities, as well as sociocultural factors, such as gender and age. Digital technology has proven to be a valuable tool for extending essential services to underserved individuals and communities. Digital technology will play an even more important role in a digital nation, ensuring that no one is left behind or excluded from essential services and other economic activities.

Several countries in Asia Pacific have outlined digitalisation plans that demonstrate ambitions to become digital nations. The 2023 edition of the Digital Societies report, the last in that series, assessed some of these plans against the five components of a digital nation. More recent pronouncements and developments also underline the commitment of governments and other stakeholders across the region to become digital nation nations. In subsequent chapters of this report, we highlight some of these developments and their impact on the realisation of the stated digital nations aspirations.

02
Tracking progress with the Digital Nations Index

Realising digital nations aspirations is a function of the five key components – infrastructure, innovation, data governance, security and people – of a digital nation. To this end, GSMA Intelligence has developed a new index to track the progress of 18 countries across Asia Pacific on these components, using a combination of quantitative and qualitative metrics to determine where each country is on their digital nation journey.

The countries in the index are ranked based on the aggregate of their scores on each of the five components of a digital nation (see the appendix for the methodology). However, to get the most out of the Digital Nations Index, countries should focus on their internal performance and identify areas that require improvement, as opposed to viewing the index as a competition with peers.

Based on the aggregate scores, we have categorised the 18 countries in the 2024 index into two groups (see Figure 2). Leading digital nations have an aggregate score of 50–100, while emerging digital nations have an aggregate core of 0–49. Singapore, Australia and South Korea are the top-three countries in this year's Digital Nations Index, all with aggregate scores of more than 70 out of 100. Vietnam tops the list of emerging digital nations, followed by India and Indonesia.

Figure 2

Digital Nations Index: aggregate scores, 2024

Source: GSMA Intelligence

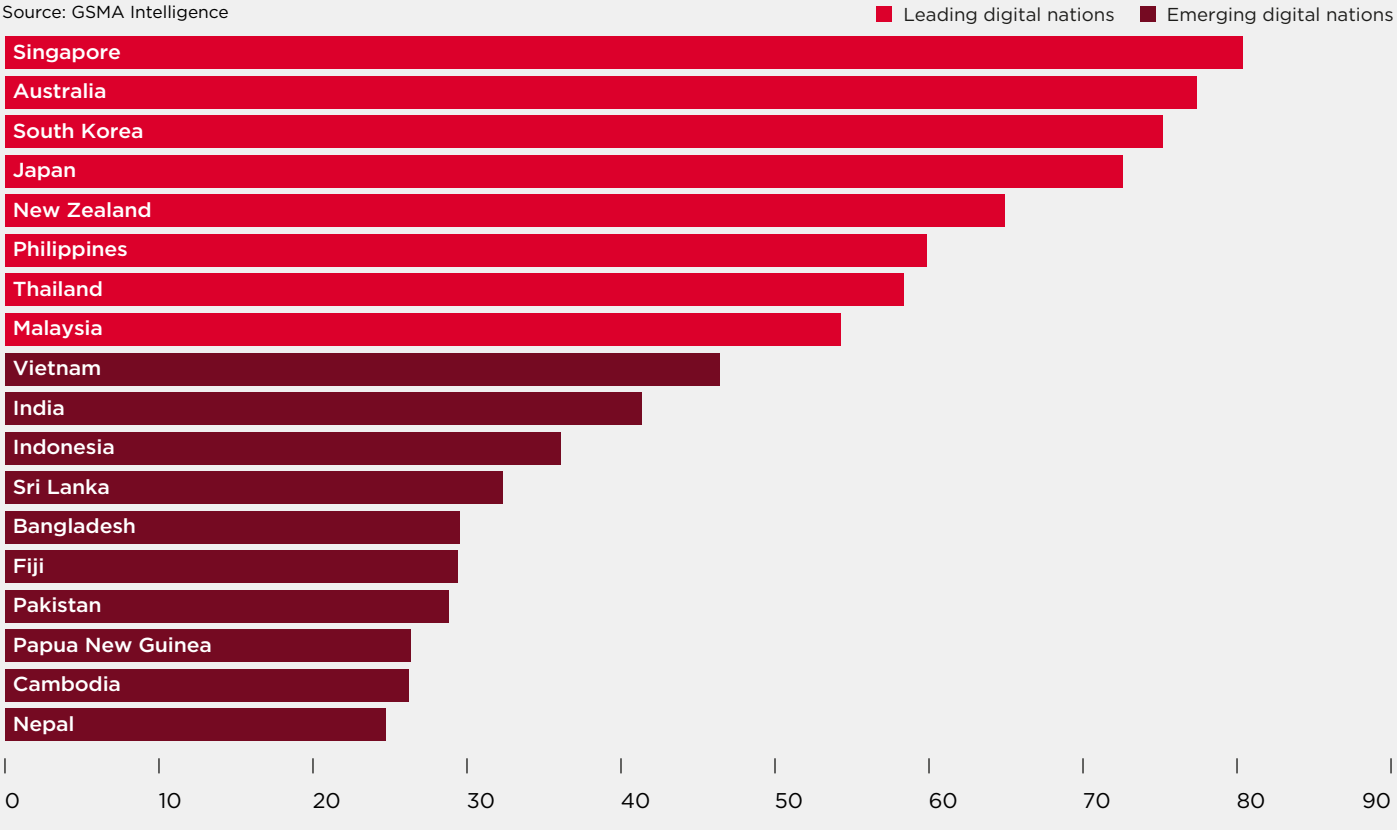


Figure 3 shows the performance of the countries in the index against the five components of a digital nation. It is important to note that for countries that have scored in the highest category for a component, this does not always correspond to the maximum score but rather a score in the top range, which needs to be improved upon to make progress on digital nations ambitions.

Figure 3

Digital Nations Index: component scores, 2024

Source: GSMA Intelligence

	Infrastructure	Innovation	Data governance	Security	People
Singapore	50–75	76–100	76–100	76–100	76–100
Australia	50–75	50–75	76–100	76–100	76–100
South Korea	50–75	50–75	76–100	76–100	76–100
Japan	50–75	50–75	76–100	50–75	76–100
New Zealand	50–75	25–49	76–100	50–75	76–100
Philippines	25–49	0–24	76–100	76–100	50–75
Thailand	25–49	25–49	76–100	76–100	50–75
Malaysia	25–49	25–49	76–100	50–75	76–100
Vietnam	25–49	0–24	50–75	50–75	50–75
India	25–49	25–49	25–49	50–75	50–75
Indonesia	25–49	0–24	25–49	50–75	50–75
Sri Lanka	0–24	0–24	25–49	50–75	50–75
Bangladesh	0–24	0–24	25–49	50–75	25–49
Fiji	0–24	0–24	25–49	50–75	25–49
Pakistan	0–24	0–24	25–49	50–75	25–49
Papua New Guinea	0–24	0–24	25–49	50–75	25–49
Cambodia	0–24	0–24	25–49	25–49	50–75
Nepal	0–24	0–24	25–49	25–49	25–49

Infrastructure

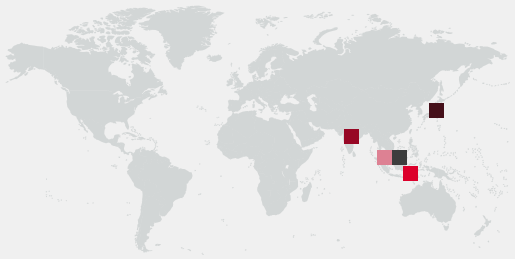
The infrastructure landscape in Asia Pacific varies widely, with countries in various stages of development. Singapore is the highest-ranked country in this component, but its score of 74 indicates there is considerable scope for improvement across the region as a whole. On the other end of the scale, Fiji has the lowest score of 12 for this component.

Mobile networks, particularly 5G, will underpin most digitalisation efforts across key sectors of the economy. 5G is now present in 10 of the 18 countries in the index. To date, operators in seven countries have also introduced 5G standalone (SA), which comes with new capabilities for enterprise use cases, and are exploring more advanced forms of 5G, including 5G-Advanced and 5G RedCap. For example, Reliance Jio has built one of the world's largest 5G SA networks in India, and in August 2024, Maxis and Huawei announced plans to collaborate on a Joint Innovation Centre focused on developing of 5G-Advanced solutions for industry use cases.

Beyond 5G, there are efforts in some countries to improve other connectivity infrastructure where this is lacking. For example, the Philippines' National Fiber Backbone project will increase internet capacity across provinces and serve key sectors, such as education, health, energy, housing, transport and IT. In Vietnam, the government is prioritising the transition to IPv6 by 2025 and the extensive integration of IoT to future-proof its digital infrastructure and accommodate the increasing number of connected devices and applications. As of 25 September 2024, Vietnam has over 50% IPv6 adoption (55.6%), alongside India (71.39%), Malaysia (68.5%), Japan (51.51%) and Sri Lanka (51.16%), according to the Google IPv6 Country Rank.[1]

Growing investments in cloud infrastructure across Asia Pacific

Cloud infrastructure, including hardware, software, storage and networking elements, form part of the necessary infrastructure to unlock the full potential of digital nations. Countries in Asia Pacific have seen a significant increase in data centre investments in recent years, a development that would generate much-needed capacity for future workloads. Below are some examples:



Japan

In Japan, Singtel and Hitachi have announced plans for the co-development of green data centre innovations and GPU cloud capabilities, with the potential to expand across Asia Pacific. Separately, KDDI is teaming up with Supermicro, Sharp and Datasection to build a large AI data centre to collaborate with businesses across various fields and industries. Meanwhile, Microsoft plans to invest $2.9 billion in AI and cloud infrastructure in Japan.

India

In India, Reliance Industries plans to build gigawatt-scale data centres in Jamnagar that will provide affordable access to AI models and services.

Indonesia

In Indonesia, Indosat Ooredoo Hutchison's ICT arm Lintasarta has launched a new GPU-as-a-service (GPUaaS) offering that provides a sovereign AI cloud solution.

Malaysia

In Malaysia, Microsoft and Google have announced plans to invest $2.2 billion and $2 billion, respectively, in data centres and cloud services to support AI initiatives.

Singapore

In Singapore, AWS plans to invest an additional SGD12 billion ($9 billion) into its existing cloud infrastructure from 2024 to 2028 to meet growing customer demand for cloud technology and services in the country.

1 www.aelius.com/njh/google-ipv6/

Innovation

There is a stark contrast in the level of innovation among countries in Asia Pacific. While the region is home to some of the most innovative countries in the world, more than half of the countries in the Digital Nations Index place in the lowest range of scores in the innovation component. Key areas that require attention for these countries include R&D spend and legal protection for innovators. Again, Singapore (78) is the highest-ranked country and Fiji (12) scores the lowest.

Like with infrastructure, investment is an important enabler of innovation. In Japan, KDDI will invest up to JPY100 billion ($649 million) over the next four years to build a large-scale computational platform for generative AI (genAI) R&D, with up to JPY10 billion coming from the government.[2] In India, the Union Budget 2024–25 includes proposals aimed at boosting startups and the startup ecosystem,[3] including an INR1,000 crore ($120 million) venture fund to further strengthen the country's startup ecosystem.

Ecosystem collaboration is another important enabler of innovation, with the pooling of resources by ecosystem players, including operators, tech startups and government agencies, expected to create beneficial synergies. For example, Malaysian operator CelcomDigi and agritech startup BoomGrow Productions have partnered together to launch 5G and AI-powered smart farm solutions to enhance sustainable farming practices and food production. Meanwhile, in Indonesia, Telkomsel Ventures has partnered with startup community AppWorks to develop innovative startups that will create inclusive and sustainable solutions for Indonesia's digital economy.

Data governance

In the last few years, a number of countries in Asia Pacific have taken steps to improve data governance, in recognition of the important role it plays in a digital nation. However, several countries still lag behind their peers in the establishment of a fully independent and resourced supervisory authority to enhance enforcement activities. Japan and the Philippines top the ranking in this category, with maximum scores.

Beyond laws and enforcement, some countries' supervisory authorities are advancing data governance through capacity building, joint consultations and awareness campaigns. For example, Thailand's newly established Personal Data Protection Commission (PDPC) serves as an advisory and complaints hub. In January 2024, PDPC organised a training course on the Personal Data Protection Act for government officials and employees responsible for data-processing activities. Supervisory authorities in Australia, Japan, New Zealand, Singapore, South Korea, the Philippines and other ASEAN member states have been collaborating with their counterparts in Asia Pacific and beyond on regional interoperability frameworks, such as the APEC Cross Border Privacy Rules, ASEAN Digital Data Governance Framework and ASEAN Model Contractual Clauses.

Meanwhile, cross-border data flows (CBDF) are currently regulated by a number of international, regional and national instruments and laws, though sometimes there is no regulatory guidance at all. There are also regional frameworks, such as the ASEAN Framework on Personal Data Protection, and regional initiatives, such as the APEC Privacy Framework and APEC Cross Border Privacy Rules. CBDF is pivotal to enabling the global digital economy and facilitating digital trade. This is especially true in the context of borderless nations, where many digital services, such as mobile applications services, may have been deployed abroad but accessed locally and regionally. The challenge for policymakers is to contextually implement an interoperable framework that allows individuals and organisations to access a wide range of digital services and platforms while acknowledging and observing data protection, security and CBDF requirements.

2 "Performance Highlights and Q&A for the First Quarter of the Fiscal Year Ending March 2025", KDDI, August 2024

3 "'Budget 2024–25 will boost StartUps and the StartUp ecosystem through bold and innovative proposals like ending "Angel Tax" and introducing paid internships,' says Union Minister Dr. Jitendra Singh", Ministry of Science and Technology, July 2024

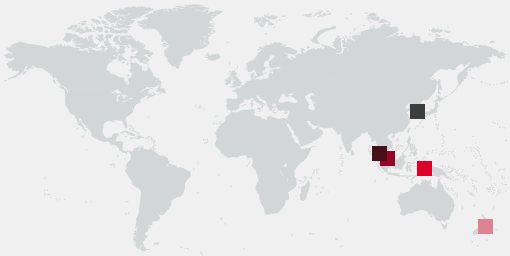
Security

Like in the physical world, security in the digital world is a top priority for all stakeholders. Countries in Asia Pacific generally perform well in this component, owing to the existence of cybersecurity laws and enforcement mechanisms. Australia (100) tops the rankings in this component, with Nepal (25) and Cambodia (25) having the lowest scores.

Industry players are continuing in their efforts to enhance cybersecurity. In Singapore, Singtel has launched the National Quantum-Safe Network Plus, which employs modern quantum-security solutions to protect enterprises against quantum threats, as well as a customised programme for enterprises to trial the technology before adoption. In Thailand, AIS has developed a personalised cyber-immunity assessment tool, the Digital Health Check, which allows individuals to assess their ability to cope with cyber threats and gain knowledge to enhance their digital skills.

Efforts to enhance cyber resilience in Asia Pacific

Despite existing laws, cybersecurity is an ongoing process, considering the ever-increasing scope and scale of online threats. As a result, countries in Asia Pacific are implementing various measures to enhance cyber resilience as part of their digital nation ambitions. Some examples are highlighted below:



Malaysia

Malaysia's Cyber Security Act 2024, which came into effect in August 2024, aims to enhance the cybersecurity of national critical information infrastructure. This includes government, banking and finance, transport, defence and national security, ICT, healthcare, water supply and waste management, energy and agriculture.

Singapore

In August 2024, Singapore unveiled the updated Operational Technology Cybersecurity Masterplan 2024, which aims to enhance the technical cybersecurity capabilities and competencies within the country's operational technology sector.

Indonesia

The government of Indonesia has highlighted the important role of cybersecurity in achieving the Vision of Digital Indonesia 2045. The government aims to draw lessons from Singapore's digital defence approach that makes cybersecurity the responsibility of all through a whole-of-nation approach.

New Zealand

In March 2024, the New Zealand government introduced a new cybersecurity strategy with four main goals: cyber resilience, cyber capability, addressing cybercrime and international cooperation. The strategy also includes a commitment to enhancing national security across various industries, including healthcare, finance, government and education.

South Korea

In February 2024, South Korea launched its new National Cybersecurity Strategy, with five strategic tasks: offensive posture, infrastructure resilience, emerging technologies, industry-government coordination and global collaboration.

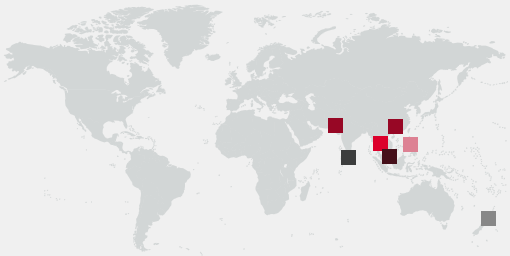
People

A fully fledged digital nation requires people with the right levels of digital skills to safely and effectively engage with online services, and a workforce capable of supporting the continuous digitalisation of different sectors of the economy. In the Digital Nations Index, Singapore (87) topped this ranking, just ahead of South Korea (86), while Papua New Guinea (30) registered the lowest score.

Some countries face various age-related challenges in the people component of a digital nation. For example, Japan and South Korea are particularly affected by an ageing population, with the rising average age of the workforce suggesting a slowing supply of younger workers into the labour market. Some other countries face the challenge of lower rates of digital skills among older people, making it difficult for them to fully adopt digital-first solutions. Malaysia and Singapore are among the countries that have introduced various initiatives to improve the digital skills of older people.

Initiatives to develop a skilled workforce in Asia Pacific

The development of a workforce with relevant skills for the digital age has become a priority across Asia Pacific. In recent years, several governments and private-sector players have introduced initiatives to develop a skilled workforce, such as the following:



Singapore

In July 2024, Singapore opened the CyberSG Talent, Innovation, and Growth Collaboration Centre, a partnership between the National University of Singapore and the Cyber Security Agency of Singapore, to bolster the country's cybersecurity ecosystem and workforce.

Pakistan and China

In June 2024, Pakistan and China formed the China-Pakistan Digital Education Alliance to collaborate on equipping students in Pakistan with digital skills.

Cambodia

In April 2024, the government of Cambodia launched the Digital Skills Development Guide for Cambodia 2024–2035, a roadmap for building digital human capital that can respond to the needs of the government and support the digital transformation process.

The Philippines

In March 2024, Microsoft announced plans to train 100,000 women in the Philippines on AI and cybersecurity, using online platforms, including ones powered by OpenAI's large language model.

Sri Lanka

In March 2024, Microsoft teamed up with the government of Sri Lanka to introduce AI education to students in grade 8 and above. The project, supported by the country's leadership, seeks to equip teachers and students with skills for the digital age.

New Zealand

In March 2024, Kiwibank partnered with AWS to offer AWS CloudUp for Her, an eight-week professional development programme on cloud technology for women in New Zealand.

03
Assessing the impact of digital trust on the components of a digital nation

Digital trust has risen to the top of the agenda for policymakers and digital technology stakeholders. This is not too surprising, as the more pervasive digitalisation becomes and the more it replaces (or at least offers substitutes for) activities in the physical world, the more concerned citizens and organisations will be about the safety, privacy, security, reliability and ethics of the digital world. In this context, the task of building a digital nation goes beyond developing the five components previously highlighted, but also includes collaborative efforts to build and preserve digital trust.

3.1 Digital trust: what and why?

Although specific definitions of digital trust vary, the underlying principle is similar and the basic concept is generally understood. Some notable definitions are highlighted below:

> "Digital trust is individuals' expectation that digital technologies and services – and the organisations providing them – will protect all stakeholders' interests and uphold societal expectations and values"
> **World Economic Forum (WEF)[4]**

> "Digital trust is what enables individuals and businesses to engage online with confidence that their footprint in a digital world is secure."
> **DigiCert[5]**

> "Digital trust is the confidence in the integrity of the relationship, interactions and transactions among providers and consumers within an associated digital ecosystem. This includes the ability of people, organisations, processes, information and technology to create and maintain a trustworthy digital world."
> **ISACA[6]**

These definitions show clearly that digital trust is an essential requirement for a digital nation. High levels of digital trust build confidence among citizens and businesses and justify the investments into developing the components of a digital nation. Conversely, online threats that erode trust often have a significant and adverse impact on victims and wider society. Notably, they can reverse digital inclusion gains in affected communities, cause financial losses and reputational damage for people and businesses and take a mental toll on victims.

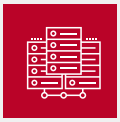
4 https://initiatives.weforum.org/digital-trust/home
5 https://www.digicert.com/faq/trust-and-pki/what-is-digital-trust#
6 https://www.isaca.org/resources/isaca-journal/issues/2023/volume-1/defining-establishing-and-measuring-digital-trust

3.2
Mapping online threats to the components of a digital nation

The nature and source of online threats are diverse. Some are created and/or weaponised maliciously by bad actors, while others may result from negligence or be an unintended consequence of an otherwise innocuous action by individuals and groups. Irrespective of the source, the outcome is the same: the erosion of digital trust and, by extension, the risk of undermining efforts to build a digital nation. Additionally, some online threats appear to be more widespread, while others are more prevalent in certain communities due to the socioeconomic and cultural factors at play.

All five components of a digital nation are susceptible to online threats, as evidenced by reported incidents across Asia Pacific and the rest of the world. The scope and scale of these threats are further exacerbated by the borderless nature of digital technologies, which means that bad actors can operate from anywhere in the world. The use of genAI and other AI tools also makes it harder to identify and prevent malicious attacks.

The examples highlighted in this section show that online threats are varied and widespread, and if unaddressed could significantly erode trust in digital systems and ultimately undermine efforts to advance digital nations ambitions. They also reveal that preserving trust in the digital world is a collective effort, and all stakeholders – including policymakers, industry players, public and private organisations and citizens – have a role to play.



ONLINE THREAT EXAMPLE

Network outages

Infrastructure

Individuals and organisations rely on telecoms networks and other digital infrastructure, including data centres, to access digital services. This means that during a network outage – where the usual flow of data and communication between connected devices, servers and applications is interrupted or halted altogether – users are suddenly prevented from accessing online services and resources when and how they need them.

Cases of network outage have always existed; however, their impact has risen in prominence recently, mostly due to increased levels of digitisation. As access to many essential services, including emergency, financial, healthcare and public services, move online, with few or no alternatives in the physical world, disruptions from network outages can leave users vulnerable, with potentially dire consequences.

Several factors can cause a network outage, but the most notable ones include power-supply failure, cybercrime, human error and natural disasters. In some countries, service restriction orders are used to suspend network services for a variety of reasons, including for political, social, economic or security concerns. Regardless of the cause or reason, the implications for digital trust can be severe.

In recent years, Asia Pacific has had its fair share of network-outage incidents, some of which are highlighted below:

- In July 2024, a cybersecurity update from CrowdStrike caused a global IT outage that affected thousands of organisations, including airlines, banks and the media.
- In July 2024, Papua New Guinea–based operator DataCo reported a major network outage that affected its transmission network and equipment.
- In June 2024, three out of five of Vietnam's undersea cables experienced a partial or full outage, causing significant internet-speed issues across the country.
- In December 2023, KDDI reported a network outage that affected users in western Japan. Emergency calls, including those for police and fire services, were also impacted.
- In November 2023, South Korea's government blamed a 'glitch in the network' for a 56-hour service disruption in a computer network for civil servants, resulting in 240,000 complaints.
- In November 2023, more than 10 million people and thousands of businesses were affected by a mobile and internet network failure at telecoms operator Optus.
- It has been reported that internet shutdowns in 2023 resulted in the loss of $237.6 million to Pakistan's economy and affected almost 83 million citizens. Along with Pakistan, India also features on the list of the top 25 countries in terms of the longest duration of internet shutdowns in 2023.[7]

7 "Internet shutdown caused Rs65bn loss to Pakistan in 2023", The News International, August 2024

ONLINE THREAT EXAMPLE

Deepfakes

Innovation

The democratisation of genAI and other new AI tools has created opportunities for individuals and businesses to generate innovative digital assets quickly and efficiently. However, they can also have an adverse impact on digital trust. For example, bad actors can use the same tools to create convincing fake content in text, image, video, audio and other formats to incite, misinform, impersonate and manipulate victims.

The use of such hyper-realistic fake videos, images and audio, also referred to as deepfakes, has increased recently across Asia Pacific, enabling perpetrators to create false narratives and blur the lines between fact and fiction. According to The Global Initiative, Asia Pacific saw a 1,530% increase in deepfake cases between 2022 and 2023, the second highest in the world after North America. The Philippines saw the highest growth in deepfake cases (4,500%), while Vietnam had the highest increase in deepfake fraud in the region (25.3%), followed by Japan (23.4%).[8]

Deepfakes and other unethical uses of innovative technologies have the potential to erode trust in digital content. This has significant implications for several sector areas, including in media, the arts, academia, security and justice. Below are recent examples of this threat in Asia Pacific:

- Local reports in several countries in Asia Pacific suggest that deepfakes were used to varying degrees in major elections in 2024, including in Bangladesh, India, Indonesia, Pakistan and South Korea. In South Korea, for example, at least 129 deepfake videos and images were reported to have been detected, violating the country's election laws.[9]
- In May 2024, Thailand's Central Investigation Bureau warned that some call-centre gangs were using genAI to produce fake TV news and articles to extract money from victims.
- In December 2023, Singapore's government warned citizens of deepfake videos and audio of the prime minister and deputy prime minister purporting to promote crypto scams.

ONLINE THREAT EXAMPLE

Personal data breaches

Data governance

A personal data breach describes an incident where sensitive or confidential information about individuals is accessed by an unauthorised party. Sensitive data can include bank account details, ID credentials, home addresses and medical records. Data breaches can occur inadvertently, through negligence or from malicious attacks.

Some common examples include sending personal data to the wrong person, accidental or deliberate exposure of sensitive data, weak security protocols on digital platforms and malicious hacking or stealing of databases or devices that contain confidential information. These can lead to identity theft, discrimination, reputational damage and other negative consequences for victims, potentially eroding digital trust.

Data breaches are a growing concern in Asia Pacific, with a number of high-profile cases in recent years. According to a study by PwC in 2023, 35% of organisations surveyed claimed to have experienced data breaches that cost between $1 million and $20 million over the previous three years.[10] Below are some examples of reported cases:

- Australia has recorded several data breaches in recent years, including a ransomware attack that compromised a MediSecure database and exposed personal information, a data breach on Telstra that compromised customer information and a data breach on Optus that resulted in the theft of personal information.
- In August 2024, a security researcher discovered that the website of intimacy-products manufacturer Durex India was leaking sensitive customer information, including names, phone numbers, email addresses, shipping addresses, product orders and payment details.
- In 2023, 1.5 terabytes of data was stolen from state-owned Bank Syariah Indonesia, including customer and employee contact details, financial documents and passwords.
- In 2023, Japanese electronics company Casio blamed human error for a data breach that resulted in an external party gaining unauthorised access to the records of over 125,000 customers in nearly 150 countries around the world.
- In 2023, a Bangladeshi government website data leak exposed the personal information of around 50 million eGovernment portal users. A cybersecurity researcher reportedly discovered the leaked database while researching an SQL error online.

8 "Rogue replicants: Criminal exploitation of deepfakes in South East Asia", Global Initiative, February 2024
9 https://incidentdatabase.ai/cite/673/
10 Digital Trust Insights 2024: Asia Pacific, PwC, 2024

ONLINE THREAT EXAMPLE

Cyberattacks

Security

IBM defines cyberattacks as unwelcome attempts to steal, expose, alter, disable or destroy information through unauthorised access to computer systems. Where this occurs, it is usually deliberate and with malicious intent to cause damage in various forms, including data theft, system downtime, phishing, social engineering, denial-of-service attacks and various forms of malware. These often have a severe impact on victims, including financial losses and reputational damage.

The scale and scope of cyberattacks have increased dramatically in recent years. Key drivers range from geopolitical competition to the use of AI tools to enhance the sophistication of attacks. Meanwhile, more assets are becoming accessible on digital platforms due to increasing digitalisation; there is the likelihood of this attracting more bad actors to perpetrate their activities through online channels.

Due to its rapid digitalisation, the Asia Pacific region has become a major hotspot for cyberattacks. According to the International Institute for Strategic Studies, the region experienced the highest year-on-year increase in cyberattacks in 2023, at 1,835 attacks per organisation per week, in contrast to the global average of 1,248.[11]

Below are examples of recent cyberattacks in the region:

- A report by Viettel revealed that the amount of personal information stolen in cyberspace in Vietnam increased by 50% in the first six months of 2024 compared to the same period in 2023. Specifically, 46 data leaks of businesses and organisations in Vietnam were recorded in the reviewed period.[12]
- In June 2024, several Indonesian government offices were hit by a series of cyberattacks, including a ransomware attack on the country's Temporary National Data Centre. The resulting data loss disrupted services for nearly 300 central and local state agencies, including immigration services and major airports.
- In September 2023, Sri Lanka's government email network was hit by a ransomware attack that wiped out months of data from nearly 5,000 email addresses using the gov.lk email domain, including ones belonging to top government officials.

11 "Contested connectivity: cyber threats in the Asia-Pacific", The International Institute for Strategic Studies, May 2024

12 "Cyber attacks targeting personal information increase by 50% in H1: Viettel report", Vietnam+, August 2024

ONLINE THREAT EXAMPLE

Online abuse and harassment

People

The internet brings many social and economic benefits for users, but also exposes them to potentially harmful content, such as abuse, harassment and discrimination. In many instances, these have been directed at individuals and communities based on certain social and physiological factors that make them particularly vulnerable to such abuse and harassment. These include gender, age, physical or mental disability, ethnicity, income, political ideology and religion.

Online abuse is especially challenging for victims, considering the viral nature of internet platforms and the opportunity for perpetrators to act in anonymity. These can limit the ability of victims to stop these attacks and to get justice. Common attacks include offensive (e.g derogatory or sexist) comments, trolling, spreading rumours, impersonation and digitally facilitated sexual exploitation and abuse.

Measuring online abuse and harassment can be challenging, considering that a significant proportion of victims do not report attacks for various reasons. However, the consequences are potentially dire for many victims. They can also take a mental toll on victims, resulting in loss of trust in digital platforms, which can in turn alienate individuals and communities from beneficial online services.

Below are some example cases of online abuse:

- Digitally facilitated child sexual exploitation and abuse is a concern for many governments in Asia Pacific, where available data shows the prevalence of predatory activities against children. For example, Unicef has classified 80% of Filipino children as vulnerable to digitally facilitated sexual abuse, and a study by ChildFund International found high levels of online bullying among high-school and college students in Indonesia.[13]
- Fiji's Online Safety Commission disclosed that 61.4% of women and 38.6% of men experience online abuse. Incidents were also reported on various social media platforms, including Facebook, TikTok, WhatsApp, Viber, Email, Messenger and Instagram.[14]
- A report by Pakistan-based NGO the Digital Rights Foundation revealed that the use of AI to attack and harass women online was growing, along with apps that steal data from devices of targeted women who are then subjected to financial fraud and blackmail. Women accounted for 58.5% of complainants received in 2023.[15]
- The Malaysian Communications and Multimedia Commission revealed that between 2020 and July 2024, there were 6,598 complaints related to online bullying and sexual harassment. Also, a study by the Malaysian Mental Health Association found that at least 20% of youth suicides in recent years were linked to cyberbullying.[16]

13 "Asia's families must be empowered to combat online abuse", ChildFund Alliance, May 2023
14 "Pacific women and online abuse", Islands Business, February 2024
15 "AI Among Technologies Increasingly Used To Harass Women Online In Pakistan", The Friday Times, April 2024
16 "MP SPEAKS | Deadly cyberbullying trend demands urgent action", Malaysiakini, July 2024

04
Measures to preserve digital trust in Asia Pacific

As demonstrated in the GSMA Intelligence Digital Nations Index, the journey to becoming fully fledged digital nations has begun in countries across Asia Pacific.

In the coming years, stakeholders will make efforts to develop the five components of a digital nation to make progress on their ambitions. In parallel to this, it is important for these stakeholders to take steps to preserve digital trust, considering the potential various threats that can undermine the efforts to achieve their digital nation ambitions.

Figure 4 identifies five key measures for governments, industry players and other stakeholders to preserve digital trust. Encouragingly, some of these measures are currently being implemented, as demonstrated by examples from across the region.

Figure 4

Five key measures to preserve digital trust

Source: GSMA Intelligence

A policy environment that drives investments

Investment is an important underlying factor for the five components of a digital nation. While public-sector investment plays a role in the development of the components, private-sector investment is necessary to improve overall outcomes. As a result, governments have a responsibility to create an enabling environment to attract private-sector investments. This is particularly crucial for the infrastructure component; in the context of threats to digital trust, such as network outages, significant investments will be required to build resilient networks with sufficient redundancy to mitigate the most challenging causes of network outages.

Across Asia Pacific, the rollout of 5G is driving an increase in data traffic (~4% on average over the next six years). However, operators' ability to expand network capacity and coverage is often hindered by regulatory constraints, market structures and excessive tax burdens. This has created an 'investment gap', whereby market conditions for private investment in telecoms networks are not favourable enough to meet ambitious national and regional digital policy targets. Three policy levers can help to close the investment gap: sector-specific taxation, universal service funds and 'fair share' regulation. European authorities are currently gauging the 'fair share' proposal. Meanwhile, in South Korea, regulatory pressure has led to commercial agreements on contributions to network costs between a large traffic generator and a telecoms operator.

The reliance of a growing number of life-saving services and economic output on always-on connectivity underscores the urgency of this measure. While several governments, such as those of Australia and Singapore, have designated telecoms networks as critical infrastructure, an essential step to ensuring network resilience is to safeguard the financial sustainability of the telecoms industry and, consequently, the ability of industry players to continue investing in secure, high-performance networks.

A whole-of-government approach to streamline efforts

The need for a whole-of-government approach[17] to preserving digital trust cannot be overstated. The interconnected nature of digital technologies and services means that a threat in a particular sector could have a knock-on effect on several others sectors and vice versa. Similarly, an attempt to tackle a particular threat could have implications for multiple stakeholders across the digital ecosystem.

For example, attempts to tackle online scams could have implications for multiple sectors, including telecoms, financial services and law enforcement. In many instances, telecoms operators face multiple requirements arising from laws and regulations on a wide range of issues, including sector-specific regulations, such as telecoms licence and spectrum regulations, and regulations from adjacent services, such as cybersecurity, data privacy and financial services. In this context, a whole-of-government approach helps to ensure that all stakeholders are engaged and different viewpoints are reflected in efforts to tackle online threats.

In Singapore, this concept has been adopted to better drive the country's whole-of-nation digital transformation, with leadership at the highest public service level coordinating the efforts of other public service agencies, the private sector and different segments of society. An example of where this is happening is in the area of cybersecurity, where collaboration between the government, industry and academia has yielded a thriving cybersecurity ecosystem in Singapore. Today, the country hosts over 500 cybersecurity providers, driven by constant innovation to counter emerging threats and explore new business avenues.

Private sector commitment and collaboration to tackle threats

As custodians of much of the digital infrastructure and the driving force behind many innovative services that shape the digital world, the private sector has an interest in the preservation of digital trust. As such, private-sector players have a responsibility to commit to tackle threats within their purview. For example, some major social media companies have recently committed to tackling various threats on their platforms, including misinformation and disinformation, online abuse and harassment, and online child sexual exploitation and abuse material. While this is a commendable first step, backing it up with effective action to actually deal with the problem will be crucial to preserving digital trust.

Besides commitments, industry-wide collaboration is also important, given the opportunity to create synergies. One such collaboration is the GSMA Open Gateway initiative, which leverages the power of mobile networks globally by opening up access to network capabilities through common application programming interfaces (APIs). There are 17 APIs in the Open Gateway library,[18] spread across different categories. Much of the early activity has focused on security and fraud prevention. To date, operators in nine countries in Asia Pacific have committed to this initiative: Australia, Indonesia, Japan, Malaysia, the Philippines, Singapore, Sri Lanka, Thailand and Vietnam.

For example, Maxis, AIS and Singtel have signed a memorandum of understanding to federate their APIs and develop solutions that will help mitigate the incidence of illegal account takeovers and unauthorised transactions that result from phishing and malware app scams. Meanwhile, Bridge Alliance, a mobile alliance of 34 member operators worldwide, and Singtel have launched the Bridge Alliance API Exchange, which leverages Singtel's Paragon (an all-in-on orchestration platform for telecoms networks) to aggregate its member operators' network authentication, user verification and network quality APIs.

17 See Advancing digital societies in Asia Pacific: a whole-of-government approach, GSMA, 2020 and Digital societies in Asia Pacific: Accelerating progress through collaboration, GSMA, 2021

18 There are 17 APIs in use with a further 11 defined in CAMARA for a total of 28 associated with the GSMA Open Gateway.

International cooperation to tackle cross-border threats

Many threats to digital trust are perpetrated by bad actors operating across national borders. Therefore, international cooperation will be vital to tackling such threats through intelligence sharing while also giving countries the opportunity to enhance their internal capabilities through technical knowledge sharing.

Over 100 organisations have joined the Global Anti-Scam Alliance (GASA), which aims to mitigate the online threats primarily targeting consumers by creating and leading a cross-sector network that actively monitors fraudsters' activity. These organisations include governments, law enforcement, consumer protection and financial authorities and services, in addition to social media platforms, cybersecurity professionals and internet service providers. In June 2024, GASA launched its first Asia chapter in Singapore, led by Mastercard (Chair) and Amazon (Vice-Chair). Members include TikTok, Feedzai, Google, Grab, HSBC, Mediacorp, Meta, NTU, NUS, OCBC, Rajah & Tann Technologies, Standard Chartered, ST Engineering and Trend Micro.

On a regional level, ASEAN is leading efforts to improve collective defence by bridging the gap between more and less cyber-capable countries. Meanwhile, Singapore, through the Cyber Security Agency of Singapore, is working with ASEAN member states to establish the ASEAN Regional Computer Emergency Response Team (CERT) to promote and facilitate information sharing related to cyber-incident response, and to complement the operational efforts by individual national CERTs in each member state. The ASEAN Regional CERT is expected to enable stronger regional cybersecurity incident response coordination and critical information infrastructure protection cooperation, including for cross-border critical information infrastructure, such as banking and finance, communications, aviation and maritime.

Several countries have also opted for the bilateral route, signing various cooperation agreements with counterparts in the region and beyond. For example, in August 2024, Japan and the US completed a tabletop exercise to bolster maritime cybersecurity and incident-response capabilities as part of efforts to strengthen cybersecurity collaboration around the maritime sector.

Response mechanisms to reassure and support victims

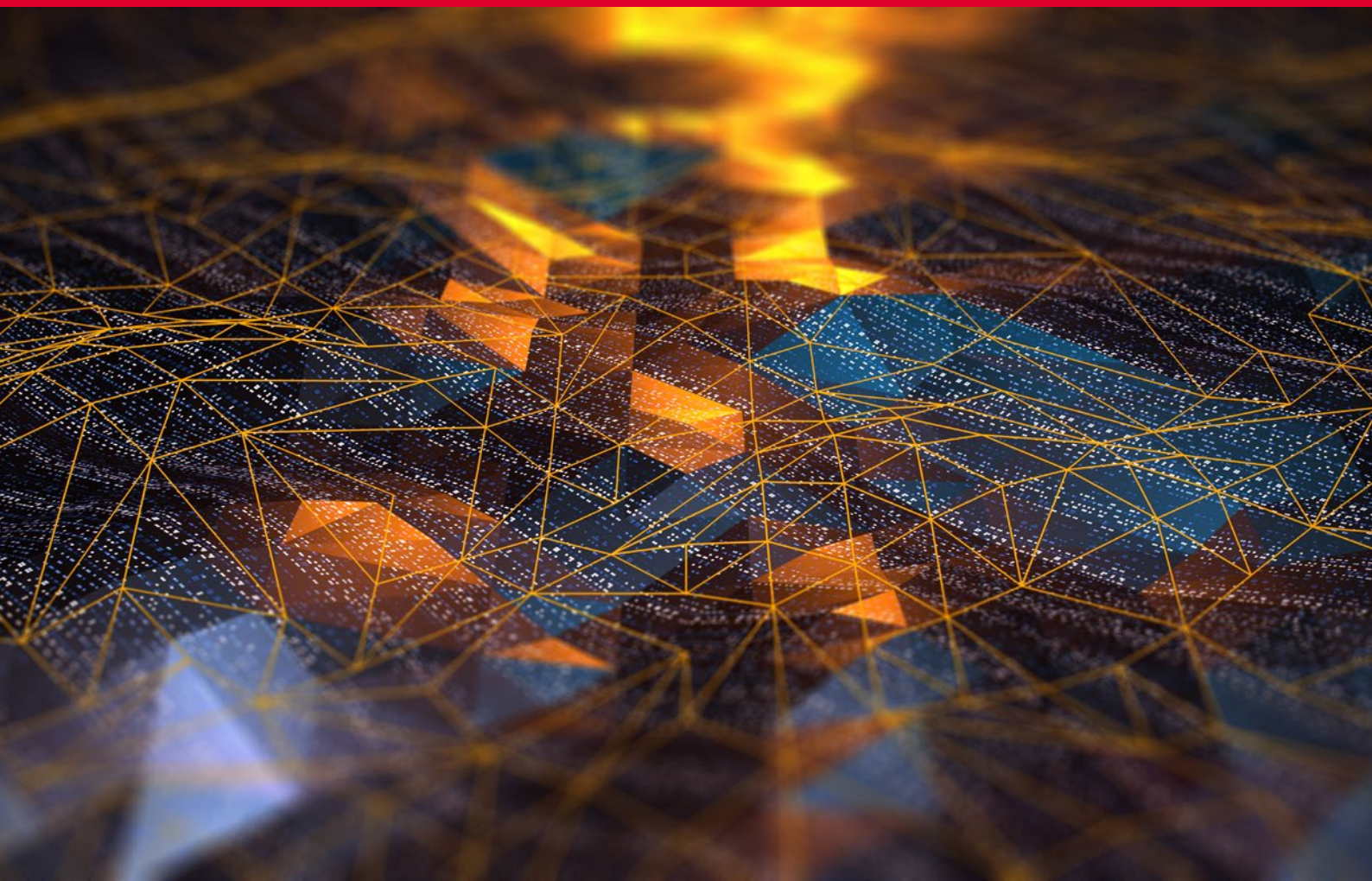
Despite the best efforts of governments, industry players and other stakeholders, various threat incidents are bound to occur. For many victims, the inability to get timely recourse, rather than the threat incident itself, may be the factor that ultimately erodes their confidence in digital technologies. This could arise from several scenarios, including a lack of awareness of where or how to get help, non-existence of response and support mechanisms, or slow/inadequate support from existing mechanisms.

In this context, establishing and creating adequate awareness about a response mechanism for online threats will serve to reassure individuals and organisations and provide support if they fall victim. In August 2024, Australia's government advised the communications regulator to introduce enforceable industry standards to improve telecoms operators' communications with customers during network outages, with the aim of easing the impact of future outages on users. In March 2024, the Sri Lankan government launched a reporting portal for child sexual abuse material, to support vulnerable children.

Outlook for the GSMA Intelligence Digital Nations Index

Countries in Asia Pacific are keen to achieve the objectives outlined in various digitalisation plans and pronouncements. However, it will require significant efforts to develop the five components of a digital nation simultaneously, considering their interdependence and the need to avoid costly gaps in the digitalisation process. The GSMA Intelligence Digital Nations Index serves as a useful guide to identify areas that require the most attention, as well as the necessary policy levers to unlock much-needed investments and the crucial measures to preserve digital trust. The GSMA is committed to working with governments, industry players and other stakeholders in the respective countries through various forums, such as the Digital Nations Summit series, to critically examine their individual performance on the index and identify opportunities to make swift progress on the various indicators.

Appendix: index methodology



Digital Nations Index metrics

The GSMA Intelligence Digital Nations Index examines the five key components of a digital nation: infrastructure, innovation, data governance, security and people. It maps the aspirations of governments in the region to these components.

The metrics of the Digital Nations Index rely on 21 indicators across the five main components. Each component consists of the following dimensions, number of indicators and corresponding weighting of indicators:

1. **Infrastructure:**
   - a. Networks – 5 indicators (40% weighting)
   - b. Spectrum – 1 indicator (30% weighting)
   - c. Cloud – 1 indicators (15% weighting)
   - d. Emerging technology – 2 indicators (15% weighting)
2. **Innovation:**
   - a. Global Innovation Index – 1 indicator (25% weighting)
   - b. R&D expenditure – 1 indicator (25% weighting)
   - c. Legal protection – 1 indicator (25% weighting)
   - d. Startup ecosystem – 1 indicator (25% weighting)
3. **Data governance:**
   - a. Data protection – 1 indicator (50% weighting)
   - b. Cross-border data flows – 1 indicator (50% weighting)
4. **Security:**
   - a. Cybersecurity laws – 1 indicator (100% weighting)
5. **People:**
   - a. Digital inclusion and online participation – 2 indicators (40% weighting)
   - b. Future skills – 1 indicator (20% weighting)
   - c. Digital literacy – 1 indicator (20% weighting)
   - d. Online safety – 1 indicator (20% weighting)

Infrastructure is measured across four dimensions:

1. **Networks:** Adoption of technologies, including 5G, FTTP, NB-IoT, RedCap and non-terrestrial networks.
2. **Spectrum:** The amount of sub-1 GHz, 1–3 GHz, 3-6 GHz and mmWave spectrum used for mobile services per operator.
3. **Cloud:** Expenditure on public cloud infrastructure.
4. **Emerging technology:** Assessment of relevant industry developments across emerging technologies, including AI, drones, robotics and quantum computing.

Innovation is measured across four dimensions:

1. **Global Innovation Index:** The Global Innovation Index is an annual ranking of countries by their capacity for, and success in, innovation.
2. **R&D expenditure:** Gross domestic expenditures on R&D.
3. **Legal protection:** Evaluates national intellectual property laws.
4. **Startup ecosystem:** Measures the maturity of a country's startup ecosystem.

Data governance is measured across two dimensions:

1. **Data protection:** Considers the extent to which there is an independent and/or resourced supervisory authority for data privacy enhancing enforcement activities and whether this authority coordinates with other supervisory and relevant authorities both within and outside the region.
2. **Cross-border data flows:** Considers policy and regulatory guidance on CBDFs, assessing the range of data-transfer mechanisms on CBDFs and/or adequacy requirements.

Security is measured across one dimension:

1. **Cybersecurity laws:** Assesses the extent to which countries have fit-for-purpose cybersecurity laws and regulations.

People is measured across four dimensions:

1. **Digital inclusion and online participation:** Analyses the percentage of mobile internet users as a share of the total population and the availability of online content and services that are relevant to local populations.
2. **Future skills:** Examines the percentage of science, technology, engineering and mathematics degrees as a share of all tertiary-education degree recipients.
3. **Digital literacy:** Measures adult literacy rates and school-life expectancy to determine whether individuals have the basic skills needed to use mobile internet.
4. **Online safety:** Evaluates the level of online safety for children across different countries.

Building the index

The process for building the index consisted of determining the relevant data for the five components, identifying the 21 indicators, normalising the data, addressing missing data and calculating the composite of the measures. For all the indicators, the index used the latest data available at the time of research and took the values for each indicator from the same year.

The creation of the index required a complete data set, so the imputing of variables used a 'hot-deck' method of imputation to imply a value for a country by taking the value of a similar country.

The indicators had different units and scales, so the index normalised any indicator that did not use a 100-point scale to make the indicator values comparable and to construct aggregate scores for each country. For indicator values that required normalisation, the process set minimum and maximum values to transform the indicators into indices between 0 and 100 using the following formula:

Normalised value = ((actual value – minimum value) / (maximum value – minimum value)) × 100

After normalisation of the necessary values, the index became a composite of the five components on a 100-point scale, according to the weights in the indicator table above, with 1 representing the worst situation and 100 the best. This normalisation allows comparison of the countries' scores for each category. To calculate the overall score, the index used the sum of the indicators within each component while taking into consideration each indicator's weighting.

The data for the index came from a variety of sources, including GSMA Intelligence, DQ Institute, FTTH Council, Startup Blink, Statista Market Insights, Tortoise Media, the US Chamber of Commerce, the World Intellectual Property Organization and the World Bank.

GSMA
1 Angel Lane
London EC4R 3AB
United Kingdom

+44 (0)20 7356 0600