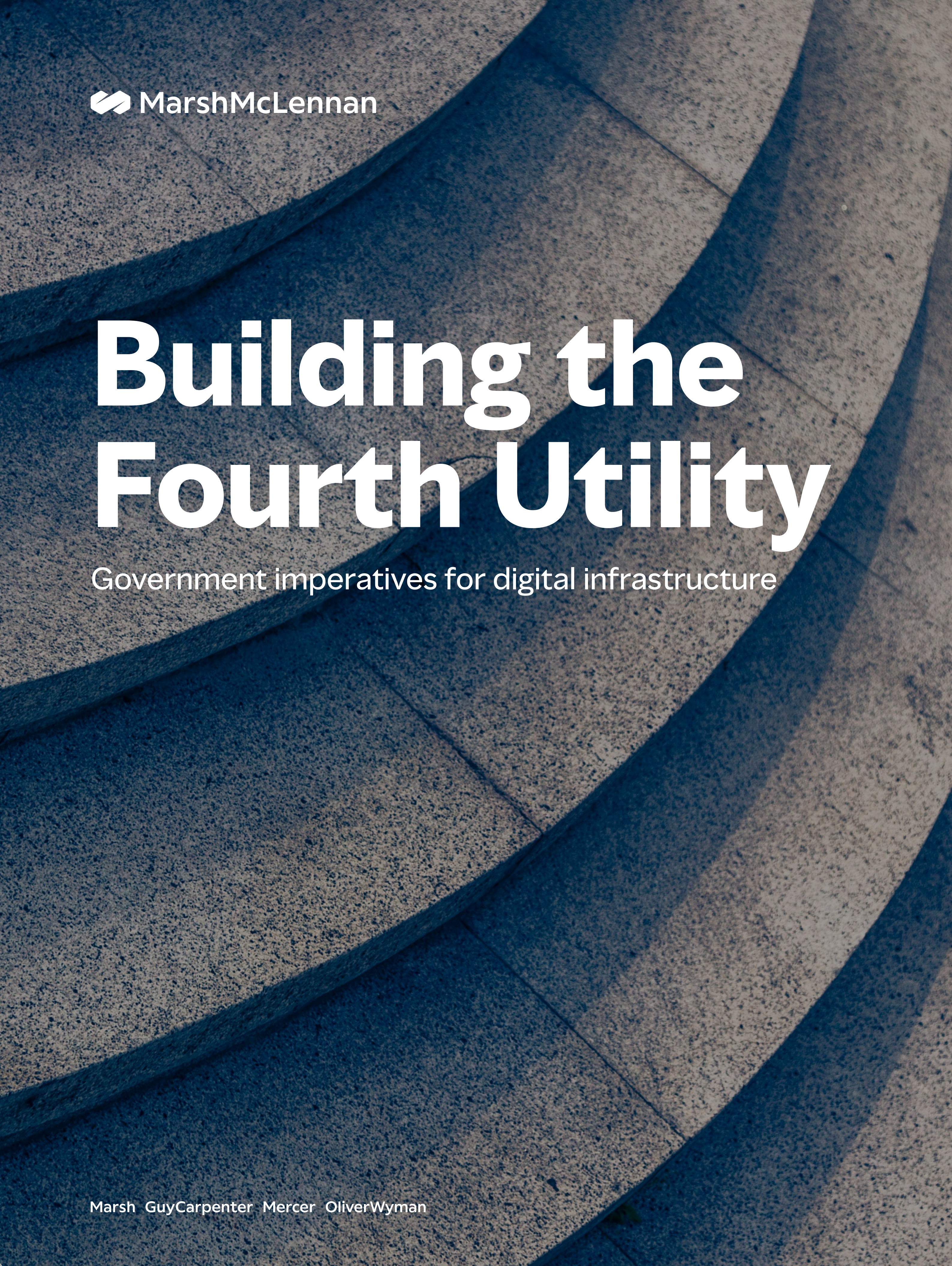


MarshMcLennan

Building the Fourth Utility

Government imperatives for digital infrastructure

Marsh GuyCarpenter Mercer OliverWyman

Contents

KEY TAKEAWAYS

1 The benefits that can be gained from high-quality digital infrastructure are numerous and varied. From GDP and innovation gains, to increased employment, productivity levels and housing values, the benefits arising from investments in this sector are meaningful and long-lasting

2 Governments have understandably planned significant investment in digital networks. However, truly maximizing the benefits of these investments and protecting national interests requires that governments meet three imperatives addressing the sovereignty, sustainability, and resilience of networks

3 Digital infrastructure has become nation-critical infrastructure and the **sovereignty** of digital networks is of paramount concern to governments. Controlling how data is processed and stored, ensuring network-wide integrity, and controlling the level of foreign influence in a network have become essential tasks. Nevertheless, each of these decisions have spillover impacts on industry, geopolitics, and access to innovation — making it difficult to predict potential contingencies and ramifications

4 Digital assets like data centers have a significant carbon footprint, but also have the potential to help other industries realize significant savings in terms of their carbon footprints and broader emissions goals. Governments can incentivize the private sector to act in support of national **sustainability targets** through a mix of 'carrot and stick' measures

5 With industry and society increasingly dependent on digital networks to support how we work, learn, communicate, and relax, the costs of network failures have never been so high. At the same time, the risks to networks have never been so significant, with cyber and supply-chain risks rising quickly and constantly evolving in nature. Governments can play a nuanced role in working with a wide range of stakeholders to ensure **the resilience of operations** over time

Introduction

Digital infrastructure networks underpin how societies and industries function. They are built on assets and capabilities provided by different types of players, such as energy utilities and the innovation sector. However, only governments have the mandate and ability to shape the direction of the sector at a national level in the face of a fast-evolving competitive, technological and risk landscape.

This report defines "digital infrastructure" as the collective term for the physical and digital assets that comprise communication and data transfer networks. High quality digital networks drive important economic and societal benefits; at the same time, perceived failures can have significant political consequences.

Around the world, networks are undergoing a significant evolution to bring service to those who are currently unconnected and as well as to meet growing demands of existing individual and corporate users for faster and more reliable services. During the COVID-19 pandemic, networks mostly held up in the face of significant changes to the way populations came to work, learn, travel, communicate, and consume.

Government stakeholders have a broad view of the sector; in some countries, they are responsible not only for setting national targets, but also for funding, operating, using, and regulating some services. Nonetheless, greater private-sector participation in digital infrastructure is essential to ensure that the sector benefits from a continued focus on innovation, which can increase service quality while also reducing costs and emissions.

Appreciating the speed of technological change, governments should continually manage the tensions between attracting foreign investment in the space, ensuring that citizens and businesses benefit from the many and varied gains and protecting the same users from potential unintended consequences.

Against that backdrop, this report explores three areas (sovereignty, sustainability, and resilience) where governments can play a unique role in safeguarding services from threats and challenges that private-sector participants are rarely empowered, structured, and incentivized to address alone. Each chapter highlights two primary issues within each as well as proposing possible avenues — informed by selected policy examples from across the world — for addressing them. Each segment then concludes with a section on government watchpoints that discusses the broader implications of and considerations behind the recommendations.

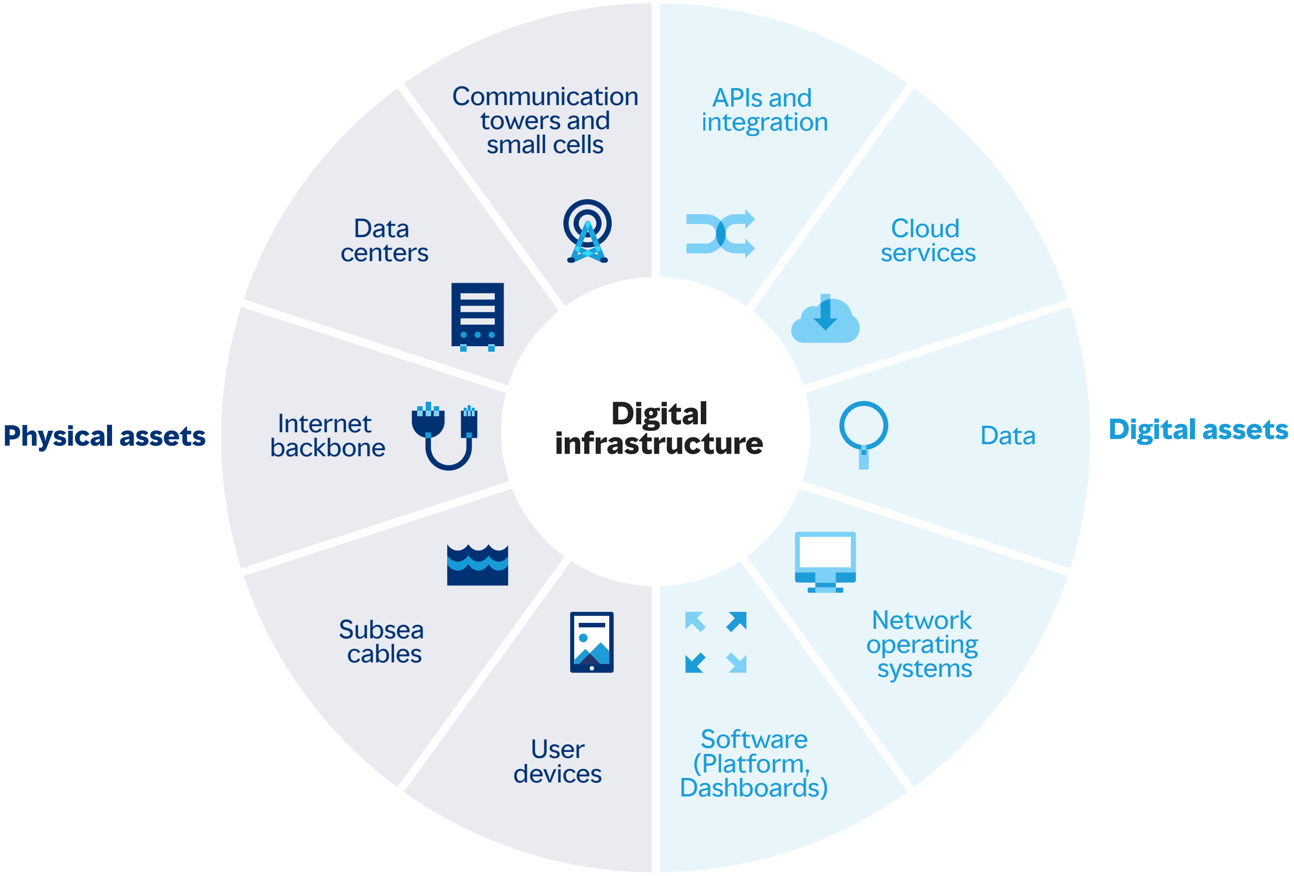
Shaping the future of digital infrastructure

As it has evolved into the fourth utility, societies and industries have become dependent on digital infrastructure. This chapter provides a high-level overview of its components, driving factors for the surge in its demand, and outlines some key roles of governments in regulating the sector

What is Digital Infrastructure?

Digital infrastructure encompasses both physical and digital assets that underpin the digital ecosystem where information is created, traded, and stored. These assets enable services such as broadband communication, 5G, and mobile data transfer that have come to define how we communicate, work, and educate in the digital age (see Exhibit 1).

Exhibit 1: Types of physical and digital assets



Source: Marsh McLennan Advantage analysis

Demand for digital services is skyrocketing

As the reach of digital services continues to expand across the globe, not least due to the COVID-19 pandemic, the demand for the physical assets that underpin these services — such as 5G, data centers, and fiber networks — has likewise skyrocketed in recent years. In fact, the OECD estimates that Internet traffic grew by about 60% just two months after the outbreak of the virus in 2020, with the majority of businesses, schools, and personal communications having to transition to digital platforms to maintain operations.[1] Unsurprisingly, the compound annual growth (CAGR) for global 5G services currently stands at about 50%[2], with the same level of growth year on year in mobile traffic data being transmitted, while the CAGRs for data centers and fiber services stand at 14%[3] and 10%[4] respectively.

Companies have similarly adopted digital assets and services to further business growth, productivity, and worker safety. Advancements in 5G technology have proven to be particularly salient and transformative at the industry level, where higher transmission speeds and lower latency have enabled wider usage of artificial intelligence (AI), machine learning (ML) and deep learning (DL) in complex processes such as detecting online fraud, optimizing manufacturing, and predicting customer needs. It is estimated that the use of these smart processes can improve a business' productivity levels by 54%[5], reduce lost sales by 30%, and increase the quality and safety standards of products.[6] It is therefore unsurprising that the number of businesses using smart processes grew 270% between 2015 and 2019, with more than 9 in 10 high-value businesses in the US currently reporting investments in the space.[7] The possible applications of 5G are boundless across industries and societies (see Exhibit 2).

Exhibit 2: Cross-industry use cases of 5G

These 5G applications are underpinned by physical and digital Infrastructure assets

PHYSICAL ASSETS

TRANSPORT

5G is essential for automated transport systems and autonomous vehicles, which can reduce congestion, collisions and pollution

EDUCATION

Immersive learning opportunities leveraging AR/VR and increased remote learning

AGRICULTURE

Precision farming can assist farmers in managing crop yields, pests and animal health

HEALTHCARE

Telemedicine and remote healthcare monitoring can close rural/urban health gaps

DIGITAL ASSETS

ENERGY

AI/ML analytics can enhance the reliability, efficiency and sustainability of energy grids

MANUFACTURING

Smart factories are 20-30% more productive and have higher quality and safety assurances

ENTERTAINMENT

Low-latency networks enable new forms of entertainment, including holographic calls and AR gaming

SMART CITIES

IOT devices can increase the safety and efficiency of traffic, utilities, first-responder systems, etc.

Source: Marsh McLennan Advantage analysis

The role of government in digital infrastructure

The growing reliance on digital services means that digital infrastructure assets now play a critical role in the basic functioning of societies and therefore require a level of government oversight. Generally speaking, governments tend to examine their digital infrastructure in terms of two main roles:

1. **Setting national targets for coverage, quality, and affordability**
   Recognizing that differences in price, coverage, and service quality are key nationwide concerns, national coverage targets or ambitions are usually set at a high level of government — at times even by the highest legislative body. In large countries in particular, governments have to bridge a growing digital divide as service provision and quality in rural geographies are often significantly worse than in urban areas.
2. **Ensuring that services are fair, competitive, and reliable**
   At a more granular level, these high-level ambitions may be pursued by a national media or communications authority that ensures fair competition between operators and liaises directly with them to determine benchmarks for service pricing, speed, frequencies, and operational boundaries. At times, the realization of high-level goals may also require the injection of government funds to attract private buy-in for less economically viable projects. In such cases, the media authority will often have to collaborate with other relevant government bodies (for example, the trade and commerce departments, municipal governments and the like).

Beyond these two main roles, the sector has also become closely intertwined with other parts of the national government agenda:

- **Sovereignty**
  As digital infrastructure assets have become increasingly indispensable, there is a greater need for robust frameworks to regulate the involvement of foreign actors and minimize threats of sabotage or espionage. Specific focus tends to center around foreign investor involvement in digital assets and foreign firms as vendors for key components within networks. Similarly, data protection laws and standards have evolved quickly in recent years to respond to greater online threats that can harm data center operators and mobile network providers.
- **Sustainability**
  Concerns about climate change have led most countries in the world to set national targets focused on several aspects of the sustainability agenda such as industrial greenhouse gas (GHG) emissions and material use (water, energy, etc.). Operators of digital infrastructure have accordingly come under greater scrutiny in recent years, with the sector contributing significantly to global emissions — data centers alone account for up to 5% of global emissions per year.[8] Nevertheless, digital infrastructure has the potential to be a major enabler of sustainability gains, with one estimate suggesting that improving the energy efficiency of assets could help reduce global power sector emissions by 1.4 gigatons a year by 2030 — a figure larger than the annual emissions of Japan.[9]
- **Resilience**
  Delivering national-level resilience in the face of a broad range of physical and operational threats is also a government priority to ensure the stability and reliability of critical infrastructure. Specific to digital infrastructure, resilience presents as ensuring the reliability of assets and services in light of disruptions such as cyber threats, workforce shortages and supply chain shocks.

The scale and strategic importance of these three areas, even beyond digital infrastructure, mean that a wide range of government stakeholders need to be involved in developing sector-specific strategies. The following chapters explore ways in which the full spectrum of public-sector stakeholders may fulfill these imperatives.

Digital infrastructure & sovereignty

While regulatory bodies will rightly continue to be primarily concerned with maintaining the performance level of critical services, there is also an increasing need for a broader government role in ensuring the legitimacy and security of a nation's digital infrastructure network as the digital realm becomes a more prominent theater for geopolitical tension

Issue

Designing better data sovereignty paradigms

Data sovereignty and governance are especially challenging where the source of the data is hard to establish. Complicated or conflicting regulations in different jurisdictions can obfuscate the application of data sovereignty, thereby increasing the cost and difficulty of operating assets as well as stifling innovation and synergies. For instance, the termination of the EU-US Privacy Shield in 2020 means that American organizations are now subject to the more stringent requirements of the EU's General Data Protection Regulation (GDPR) when transferring data to and from the European Economic Area (EEA). However, the US Stored Communications Act and Patriot Act blurs the same legal lines as they negate GDPR stipulations by legitimizing compelled disclosure and granting American law enforcement the power to retrieve and review data no matter where it is stored.[10] Such challenges around legal ambiguity are further exacerbated by the popular usage of cloud service providers, which can move data between countries without clients' knowledge.

Way ahead

Tailor data localization strategies or pursue trusted cross-border collaborations

Governments can step up efforts to deter businesses from moving sensitive data, align standards across borders so that data can be shared where necessary without sovereignty being compromised, and monitor violations of such regulations and standards. One solution could be for legislators to adopt a tiered approach to data localization measures based on sensitivity (see Policy-in-Action). In theory, data localization policies may result in improved security, simplified local data regulations for law enforcement, and greater demand for local cyber services and data centers. Alternatively, regulators and industry associations could pursue long-term cross-border collaborations that streamline requirements across jurisdictions. These may take the form of regional agreements, bilateral frameworks offering mechanisms to help organizations comply with foreign regulations, or shared platforms with unified standards and protocols. In addition to reducing legal ambiguity, clearly delineated and coherent regulations increase the likelihood of compliance by reducing costs and improving operational efficiency.

Policy-in-action

There are three broad forms of data localization strategies that have been adopted by various countries, usually with distinct, bespoke terms and conditions (see Exhibit 3).

- **Local-only storing, transmission and processing:** Where data is managed or stored locally to prevent international data transfers; typically used to exert control over citizens' activities
- **Local copies required:** Where companies are mandated to keep a copy of data in local servers or data centers, which allows governments jurisdictional access for regulatory purposes
- **Conditional restrictions:** Where transfers of data outside national borders are allowed if certain conditions are met by the transferee and/or by the recipient country. These conditions typically rule that the recipient country has adequate personal data protections or privacy safeguards that prohibit exploitation

Exhibit 3: Examples of data localization strategies

AUSTRALIA Local-only storage	**INDIA** Local copies required	**EUROPEAN UNION** Conditional restrictions
Australia’s Digital Transformation Agency (DTA) established its Hosting Strategy in 2021, which is a framework that assesses the suitability of cloud and data providers for hosting sensitive national data. The variables assessed in the framework include: • Facility ownership; • Ecosystem architectures; • Cloud adoption; and • Pricing Assessed data center providers are either distinguished as *“Certified Sovereign Data Centers”* or *“Certified Assured Data Centers”*.	India’s Personal Data Protection Bill stipulates that sensitive personal data (e.g. identifiers, healthcare or financial information) must be stored in India, although copies of the data can be transferred internationally if certain conditions are met, including: • If the user provides explicit consent and the transfer is made to a scheme approved by the authorities • The data is stripped of all identifiers and sensitive information • The Data Protection Agency (DPA) deems that the recipient country has adequate safeguards or protection; or • The DPA has authorized the transfer, in accordance with public or state policy	The General Data Protection Regulation (GDPR) dictates that the transfer of personal data outside the European Economic Area (EEA) is only permitted where: • The recipient is in a territory considered by the Commission to offer an adequate level of data protection; • Data protection authorities have binding corporate rules and safeguards; • The subject provides explicit consent for a data transfer; or • The data is necessary for public interest in accordance with EU or member state laws

Source: Marsh McLennan Advantage analysis

Cross-border collaboration is an alternative strategy that some governments have used to complement certain data localization laws. For example, the Gaia-X software federation — which was launched by primarily European cloud operators and data owners in conjunction with the EU — aims to ensure that data is securely exchanged within a trusted environment. The federation combines jurisdiction-specific regulatory standards, industry-specific standards, and technical standards to maintain a strict data governance benchmark across all global members. With the establishment of regional standards and data federations, data controllers will be able to easily and freely decide where their data is stored, who can process it, and for what purpose, as well as work with trusted operators in full compliance with both local and regional regulations.

Watchpoints

- Data localization laws are costly for businesses and thus affect competitiveness. One study indicated that firms in countries with forced data localization laws may sometimes pay between 30-60% more for their data needs than if the data could be located in more competitive offshore markets.[11] Notably, PayPal suspended its operations in Turkey following a 2016 ruling that required businesses to locate its information systems within the country, which affected thousands of businesses and customers.[12] Legislators, regulators, and industry associations should ensure that laws, regulations, and corporate practices that preserve data privacy and security are not excessively restrictive.
- Increased prices of local data storage can also stifle innovation — which is particularly key to efficiency and growth in the digital infrastructure ecosystem. According to OECD market-regulation data, a 1-point increase in a nation’s data restrictiveness was linked to a 7% decrease in gross trade output, 2.9% decrease in productivity, and 1.5% increase in downstream prices over five years.[13]
- Data localization laws often also prevent data sharing that helps identify system vulnerabilities and potential cyber threats, and practices such as “sharding,” where data is spread across multiple centers to reduce its exposure to cyberattacks.

Issue

Managing foreign influence

Governments are increasingly concerned about how some digital infrastructure components could be modified for espionage uses or to exacerbate cyber vulnerabilities across telecommunications networks, thereby threatening national security.

The biggest debates in this sphere pertain to the provision of 5G coverage and, more specifically, to the use of foreign equipment in 5G rollout. However, the small number of providers presents a significant challenge. Four companies currently account for about 80% of the global market[14], with China-based Huawei being the leading global 5G network equipment supplier, ahead of key competitors Nokia (Finland), Ericsson (Sweden), and Samsung (South Korea). Most countries in the world will therefore need to accept the presence of foreign-manufactured equipment in their network or find alternatives that will not hinder the rollout of 5G.

Another complication arises from the fact that capital-intensive digital assets often depend on significant support from foreign innovators, investors, and operators. The presence of foreign actors may affect or even disrupt the trajectory of national development, such as when economic interests come into conflict while a country's telecommunications network is heavily dependent upon service by a foreign nation's companies, for instance. Governments therefore need to closely monitor and regulate any elements of foreign influence within their digital infrastructure networks to ensure the security of critical national assets.

Way ahead

Balance foreign involvement in digital infrastructure networks

Governments are increasingly implementing rules and legislation that outline a code of conduct for foreign actors involved in financing and operations, especially through the addition of robust enforcement mechanisms, and aim to proactively update these as the digital landscape evolves. This often involves regulators and supporting agencies (for example, defense or intelligence agencies) working closely with private-sector security firms to assess the potential threat posed by foreign involvement in domestic networks and to develop adequate controls.

Taking this one step further, lawmakers may even consider bolder laws affording regulators special, flexible intervention powers during broadly defined "crises" or "emergencies" where national security threats involving foreign actors emerge. For example, the regulator and the relevant governmental departments could retain the authority to freeze foreign assets and order companies to transfer data and hardware to alternative providers should a partner country suddenly adopt a policy that could undermine national security. Legislators and regulators should strive to maintain balance between welcoming foreign participation and ensuring that strong regulations are in place for when entrants begin their in-country operations.

In the longer term, departments and agencies overseeing economic affairs and innovation can establish industry growth centers for the domestic development of relevant capabilities and technologies by incentivizing collaboration between industry and academia. Countries would then be able to gradually decouple their networks from foreign equipment and assets, thereby achieving a greater degree of self-sufficiency and sovereignty.

Policy-in-action

Lighter-touch measures like **oversight processes** involve the screening of investments and acquisitions involving sensitive digital activities for potential risks. One such example is the UK's 2021 National Security and Investment (NSI) Act, which requires the advance disclosure and auditing of foreign acquisitions in 17 sensitive fields pertaining to national security, including telecommunications, energy and AI. The Act grants authorities the power to block potentially harmful deals. Similarly, **the use of licenses, permits, and foreign equity** allows regulators to choose which operators can do business in the country or cap their equity stake to boost the competitiveness of local firms. One example is China's requirement that all operators possess an Internet Data Center (IDC) license to operate, which foreign-owned companies are not allowed to apply for, thereby severely limiting the participation of foreign operators in the local digital space.

Heavier-handed measures like **bans** involve the blacklisting of specific technologies in the digital space for risk of espionage or sabotage by foreign actors, and are usually only used as "last-resort" options to immediately remove actors that present high risks from the local space. The most prominent example of this is the US' "rip-and-replace" mandate for blacklisted 5G equipment, which saw the federal government offering a $1.9 billion grant to operators to swap out banned technology for alternatives.

Rather than directly intervening in the digital infrastructure space, some regulators have instead pivoted to **supporting the growth of local technology alternatives**, which involves the provision of dedicated platforms and support to foster domestic innovation around digital infrastructure to reduce reliance on foreign actors in the long run. Notably, the world's first Open RAN-based 5G network was launched by Japan's Rakuten in 2020, which allowed for different vendors to supply communications technology, as compared to traditional pathways of 5G rollout involving the use of one vendor. Open RAN technology purportedly also slashed the operator's initial capital investment by 40%, proving to be a cost-efficient method of reducing foreign involvement and ensuring rollout.

Watchpoints

- With respect to potential national security threats, strong emergency intervention powers have to be delicately balanced to avoid overreach as well as garner enough political traction to pass. More fundamentally, regulators have to consider if extreme last-resort measures are actually feasible in their context: The extent and nature of these powers should be contingent upon the regulator's capabilities, the business environment, the domestic and international political climate, and the availability of excess capacity elsewhere to take on additional service loads. To expand, agencies with greater resources and operating in states with a proclivity for centralization may be able to directly take over, or at least supplement, digital infrastructure operations for a short period, whereas others may prefer to steer economic activity by issuing emergency directives.
- While high-level oversight processes are important in giving regulators the power to turn away potentially harmful foreign actors, lower-level surveillance processes are equally important to regulate current players in the field. This includes the use of cybersecurity agencies or defense equivalents being vigilant for backdoor exploits or other cyber vulnerabilities designed for illegal exfiltration among existing providers.
- Blunt instruments such as bans and sanctions may have harmful long-term ripple effects beyond the disruption caused by their introduction. These include shortfalls in investment, competition distortion — if operators in a country are banned from using a specific technology — and retaliatory geoeconomic or geopolitical implications. Countries that have chosen to adopt stricter legislation on foreign ownership or investment in digital infrastructure should explore pathways varying in restrictiveness to design a strategy suited to their network's characteristics, dependencies, and vulnerabilities.
- Equipment bans can be difficult or costly for operators and may give rise to geopolitical tensions between countries. In some situations, blanket bans merely lead to the substitution of one source of foreign influence for another, thus requiring that regulators remain vigilant and delicately weigh the threat of some foreign actors against others. In some cases, government funding may also be needed to support "rip-and-replace" mandates as they can otherwise cost millions of dollars per operator.
- Measures perceived as being antagonistic to foreign involvement could also leave the country at risk of falling behind in technological investment and workforce skillsets. Indeed, according to a World Economic Forum (WEF) report, the ease of receiving licenses, openness to foreign investment, and regional coordination for infrastructure investment were among the top regulatory determinants for companies deciding to invest in digital infrastructure overseas.[15]

Digital infrastructure & sustainability

Digital infrastructure assets can be a significant enabler for governments in realizing their climate ambitions, but they are currently among the largest consumers of energy across the globe. Achieving success in the sustainability space involves making sure that digital asset operators account for all forms of waste and emissions to improve efficiency and stimulate innovation

Issue

Ensuring all emissions are accounted for by operators

Given that electricity accounts for approximately 40% of all data center costs, it is no surprise that 82% of operators track their energy consumption metrics and a further 70% track their power usage effectiveness (PUE) figures.[16] Many operators are presently faced with increased pressures from investors and consumers to green their operations, which has aligned sustainable energy imperatives directly with profitability concerns.

However, energy consumption is only part of the picture when considering the environmental impact of data centers. Data centers consume vast quantities of water directly for cooling — sometimes up to 60% from potable sources — and indirectly through water requirements for carbon-based electricity generation.[17] In one survey, only 51% of operators said they measure direct water use; among those that don't, the majority say there is little motivation to do so given water is a relatively inexpensive commodity.[18] The environmental impact of this can be monumental — in the US, for example, the data center industry remains among the top 10 highest industrial consumers of water in the country, and it so happens that water-scarce areas in the US host a disproportionate number of operations, meaning that without meaningful intervention, the industry will continue to exacerbate water stress as it grows.[19] The collection and reporting of other environmental metrics, such as for carbon emissions and e-waste, also remain critically low in the industry, at 33% and 25% respectively.[20]

Way ahead

Regulate and incentivize broader sustainable behavior

Regulators should work together with their country's data center industry associations (or equivalent) to design and implement measures that ensure operators take a broader view of their environmental footprint. In maximizing compliance, they can leverage various "carrot-and-stick" policy tools ranging in intensity and outcome, from conventions and standards to heavier-handed mandates. Ultimately, the sustainability of any asset or operation will improve most rapidly when it is in the financial interests of an operator to comply. Mandating the reporting of a wider set of sustainability-linked metrics will put the spotlight on operator performance; pressure will then follow from both investors as well as customers for operators to act quickly in areas in which they underperform.

Policy-in-action

In some cases, regulators have adopted **standard-setting** practices to benchmark operators against sustainability best practices. Operators in China have to abide by strict energy usage regulations, such as a minimum PUE rating of 1.3 and an energy utilization rate of 60% by the end of 2023.[21] Operators in the Netherlands, meanwhile, face wider regulations that span a number of areas, including energy efficiency, special use, water consumption, and heat recycling.[22] Both countries also boast differential regulations based on resource constraints and other factors.

Exhibit 4: Overview of a regional data center policy in The Netherlands

2020 guidance policies for Amsterdam and Haarlemmermeer data centers

Energy consumption

Data centers must have a PUE of at least 1.2, and commit to the use of sustainably-generated energy. At present, 85% of Dutch Data Association members use green energy, and is expected to rise to 92% by 2025.

Residual heat

Centers with heat storage facilities must recover heat energy and link it to the Dutch heat network. Currently 24% of all centers are connected to the heat grid, with more expected as a result of these new policies.

Spacial use

Data centers must be built in an "intensively stacked" manner to maximize land use, using circular and future-proof methods. Centers must also be integrated into the landscape, and have minimal impact on nature.

Water consumption

The use of groundwater and drinking water in cooling processes is prohibited. Waternet, the Dutch water utility, will look to capping water consumption figures, which will encourage the adoption of alternative cooling measures.

Source: Marsh McLennan Advantage analysis

In other cases, regulators have also looked to adopting **mandatory reporting practices** where operators are obliged to disclose various inputs and/or outputs relevant to sustainability. All industrial facilities in Singapore, including data centers, that emit more than 2,000 tons of GHGs are subject to the Carbon Pricing Act (CPA), which requires operators to submit annual emissions reports. Those emitting more than 25,000 tons of GHGs are required to submit emissions reports, participate in a monitoring plan and be subject to prevailing carbon taxes.[23] Similarly, the US Securities and Exchange Commission (SEC) has proposed mandating registrants to include climate-related disclosures in their registration statements and periodic reports, such as data on GHG emissions and certain climate-related financial statement metrics.[24]

In some cases where regulators have determined the sole use of standard-setting or mandatory reporting practices to be too heavy-handed, they have instead opted for **a mix of policy levers or adjusted the intensity of policies**. The EU, for example, launched a Data Center Code of Conduct in 2008, which combines voluntary reporting with standard-setting exercises to improve energy efficiency among private operators. Voluntary participants are subject to energy measurements, energy audits and frequent monitoring. In turn, participants successful in reaching the benchmarks are offered incentives (for example, public recognition, advertisements, and invitations to stakeholder forums) to increase their visibility.[25]

Watchpoints

Governments need to critically consider their role in the sustainability space: Is the goal to promote greater transparency for investors and consumers or to proactively set benchmarks to which operators must conform? Ultimately, the answer to this question will lead to greater clarity on what actions will be appropriate for a country's digital infrastructure ecosystem.

Metric reporting is inherently tricky. Metrics are often calculated inconsistently, meaning that data across individual operators cannot always be directly compared. Regulators leveraging mandatory reporting should devise suitable guidelines to address this issue by laying out specific methodologies for calculation, a process that will require significant industry expertise and robust stakeholder communication. They, and any supporting agencies (for example, environmental and energy departments), will then have to receive and review these reports and set out incentives or disincentives for operators, depending on their performance.

It can be difficult to set realistic standards as different operators can have drastically different needs (for example, the scale of operations, equipment age, or location). Regulators can attempt to acknowledge these by applying a tiered regulatory approach where there may be different requirements for different operations (for example, hyperscale versus networks of small cell data centers) or by crafting flexible, progressive regulations to afford operators space to innovate and adjust their operations accordingly.

Lastly, progressive approaches also afford governments time to consider more lasting and impactful policies for sustainability. As it stands, many legislators and regulators have encouraged operators to reduce GHG emissions by using renewable energy (RE) in their energy mix. Where RE is not available near operations or cost-efficient to adopt, however, operators have used Renewable Energy Certificates (RECs) as substitutes — where clean energy generated in one place is purchased to offset the energy used in another, effectively rendering the original energy input "carbon-neutral". Without RECs, for example, Google's direct utilization of RE would only cover 39% of its asset emissions.[26] However, while RECs may be a cheaper stop-gap measure to offset emissions, they do not diminish the current demand for carbon-based energy. Thus, governments still need to balance the use of these measures with more permanent, long-term solutions on their path toward net-zero.

Issue

Harnessing private-sector innovation efforts

Truly embracing sustainability requires different operators to collaborate with governments to harness their synergies for mutual benefit. However, cross-sectoral collaboration on digital infrastructure has not always been as effective or widespread as it should be: In the months between February 2020 and August 2021, G20 governments announced over $480 billion worth of telecommunications infrastructure projects, whereas global private investment only totaled $8.5 billion.[27, 28] As it stands, operators are largely motivated by profitability when assessing the viability of additional operating costs, rendering it difficult to garner buy-in for capital-intensive solutions like heat waste recycling or further technological innovation. While these endeavors may initially present themselves purely as costs to operators, they have the potential to unleash broader economic benefits, rendering them indispensable in the path towards net-zero.

Way ahead

Incentivize tailored private-sector innovation in aid of sustainability

Some governments have carried out a series of strategic and targeted efforts that focus on stimulating and supporting private-sector efforts to green digital networks in line with their national sustainability commitments. As a first step, regulators and other relevant industry-facing agencies must know about emerging technologies in the sector, understand the potential gains to efficiency and sustainability that each brings, and discern any potential barriers to their implementation. Next, these agencies must work together to decide what strategies are most appropriate for the country's climate goals and identify pathways for these solutions to be developed at scale.

Effective strategies may include new or renewed regulations aimed at recalibrating the business environment and facilitating the implementation of particular technologies. Additionally, relevant departments could take care of setup costs involved in locating digital assets near symbiotic industries (for example, those that require significant heat inputs), engaging experts on the design and development of cutting-edge technologies, organizing pilot programs to test new solutions, establishing partnership grants, or more. Working toward a self-sustaining, open research and development ecosystem where businesses are empowered and motivated to cooperate will benefit legislators, regulators, agencies, and industry associations in the long run. Ultimately, by sharing risks and providing incentives and support for businesses to work more closely with the public sector, governments will be better able to shape their digital ecosystem in a manner that best matches the nation's climate ambitions.

Policy-in-action

Many governments across the world have been responsive to technological breakthroughs in the digital infrastructure ecosystem. For example, following Microsoft's successful experiment with an underwater data center that found that servers operating in a static, dry nitrogen environment were more energy-efficient and eight times more reliable than those running in land-based data centers[29], China announced plans to build a series of undersea data center projects by 2026.[30]

Some governments have also made changes to regulatory frameworks to facilitate the adoption of new innovations, as is the case of battery energy storage system (BESS) projects in Finland. The Finnish regulatory framework in particular, incentivizes and enables BESS-as-a-service by permitting stacked revenues for BESS owners and supporting technological interoperability.[31] Consequently, data center operators can generate revenue as well as help to stabilize the grid by connecting their BESS assets to the energy market, earning over $177,000 per year per MW according to 2020 figures.[32] Nordic telco Telia, for example, has connected its Helsinki data center to Fortum Spring, a "virtual battery" program run by a local utility, and contributed several MW of capacity to the power grid since spring 2021.[33]

For other countries, the pursuit of breakthroughs in environmental technology has involved more direct fiscal support. Where Ireland's Climate Action Plan details the country's key strategies for attaining a 70-percent RE-powered grid by 2030, it has also included fiscal incentives to increase private participation in the transition. One key initiative is the proposed Rhode Green Energy Park in Offaly County, a government-funded eco-industrial park where energy-intensive operations — like data centers — are offered grants to strategically locate their operations where other industries stand to benefit from a sharing of material resources. The Park is situated close to a hydrogen energy pipeline, and will include other complementary industrial players like greenhouses, fertilizer producers, and anaerobic waste digestion facilities, which will utilize waste heat from data centers to lower the overall ecologicalfootprint of these processes.[34]

The Singapore government has been active in efforts to partner with the private sector to make its digital infrastructure more sustainable. Initiatives include building a high-tech, green industrial park, offering grants linked to the adoption of more efficient technology, and the funding of the expansion of renewable energy capacity in the country (see Exhibit 5).

Exhibit 5: Examples of strategic interventions by the Singapore government to support greener digital services

BUILDING OUT A HIGH-TECH GREEN INDUSTRIAL PARK	SINGAPORE GOVERNMENT	PROVIDING OPERATORS WITH ENABLING TECHNOLOGY	ROLLOUT OF RENEWABLE ENERGY
The Infocomm and Media Development Authority of Singapore (IMDA) has unveiled plans to build out a green industrial park, Tanjong Kling, which will include a ready-made 170,000 square meter vertical data center complete with direct access to solar energy, water-efficient cooling systems and ventilation technology. The 20-storey data center will also be built in a manner that maximizes the limited land in Singapore to accommodate the country's long-term data needs.	The Singapore government has brought together key national universities as well as large operators like Meta and Keppel to launch a US$17 million research project on novel cooling techniques for tropical data centers. In 2020, the country's Energy Market Authority (EMA) and Ministry for Trade and Industry (MTI) also announced a US$36 million research fund for low-carbon energy solutions, including the piloting of a floating energy storage system (ESS).	The National Environment Agency (NEA) of Singapore has launched the Energy Efficiency Fund (EEF) to support the evolving energy needs of the country's data centers. This includes a grant for operators of up to 50% for investing in energy efficient equipment and technologies, up to 50% for implementing an energy management information system (EMIS), up to S$200,000 for energy audits, and up to S$600,000 for subsidized facility design consulting.	A joint programme between the Housing Development Board (HDB), the nation's leading energy utility (Sembcorp) and the Economic Development Board (EDB) of Singapore will see that solar farm capacities are quadrupled through to 2030. Further investments in building the country's hydrogen-harvesting and utilization capacities are also expected, given the country's limited access to harvesting other forms of renewable energy.

Source: Marsh McLennan Advantage analysis[35, 36, 37]

Watchpoints

- Commercial sensitivities, insufficient incentivization, and inequitable distributions of risks and costs often hinder the cultivation of active, healthy research and development ecosystems. Thus, in addition to footing the "first-dollar" bill, legislators and regulators will need to be bold in designing information-sharing arrangements and intellectual-property rights with a view to protecting commercial value while encouraging openness and collaboration.

  They will also have to consider the full spectrum of potential ramifications with regulatory changes that aim to support a given technology or solution, including ripple effects for other forms of innovation or broader structural vulnerabilities associated with a particular course of action: For instance, if incentives to introduce more effective sustainability measures are supported by standards and regulations, smaller operators without access to the latest technologies and techniques may be left behind, precipitating a less competitive market and all of the associated risks and disadvantages. Valuable lessons may be derived from how other countries have approached similar challenges to implementation and stakeholder management.

- The selection of partners, technologies, and strategies may also create long-term complexities, if not issues, if not handled with forethought and tact. Fairness and transparency in both procedure and subsequent communication can be particularly pertinent with higher-profile partnership opportunities that promise to be lucrative for selected participants. The relevant departments and agencies should therefore take care in the identification of companies to partner with on pilot schemes in order to maintain strong relationships with other private-sector actors in general. Similarly, the broader national sustainability strategy should be coherent and consistent with identified national goals. Constant evaluation, perhaps with the aid of appropriate metrics, will also be important to ensure that all actions taken remain on the right track in the face of contingencies or new macro developments in the world of digital infrastructure.

Digital infrastructure & resilience

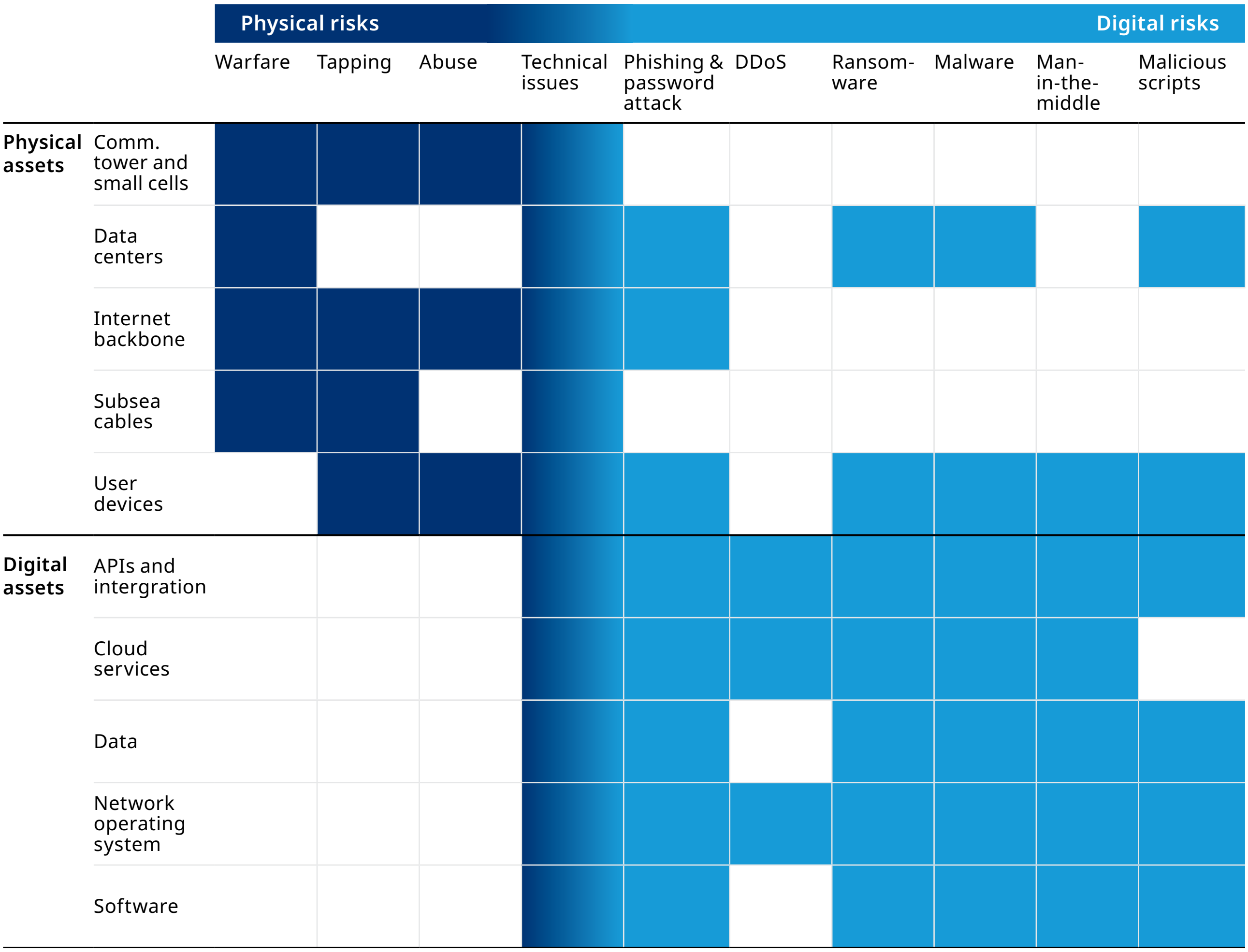
Digital networks have become critical infrastructure for countries, exacerbating the threat networks and operations face from a plethora of cyber and supply-chain risks. Despite high levels of private-ownership in digital networks, governments should have a strong presence in mitigating national cyber, supply and labor-related risks

Issue

Holistic cyber-physical security strategies

Achieving a high level of resilience requires a comprehensive national strategy that encompasses both cybersecurity and physical integrity, and moreover both vulnerabilities inherent to digital technology and risks perpetuated by malicious agents. Operators and end users of digital infrastructure remain exposed to technical faults, whether as a result of traffic surges, software complexities, human error, or other points of failure (see Exhibit 6).

Exhibit 6: Digital infrastructure security risk exposures



		Physical risks									Digital risks
		Warfare	Tapping	Abuse	Technical issues	Phishing & password attack	DDoS	Ransom-ware	Malware	Man-in-the-middle	Malicious scripts
Physical assets	Comm. tower and small cells	■	■	■	■						
	Data centers	■			■	■		■	■		■
	Internet backbone	■	■	■	■	■					
	Subsea cables	■	■		■						
	User devices		■	■	■	■		■	■	■	■
Digital assets	APIs and intergration				■	■	■	■	■	■	■
	Cloud services				■	■	■	■	■	■	
	Data				■	■		■	■	■	■
	Network operating system				■	■	■	■	■	■	■
	Software				■	■		■	■	■	■

Source: Marsh McLennan Advantage analysis

In 2021, numerous outages to cloud services, particularly those run by Big Tech market leaders, severely disrupted online services and communications worldwide. These resulted from more incidental causes such as overwhelmed networking devices and router configuration changes.[38, 39] Malicious activity is on the rise simultaneously — the communications industry experienced over 1,000 attacks weekly per organization in 2021, a 51% increase from 2020.[40] From a geopolitical standpoint, nation-state hacking incidents have been on the rise too, rendering it more important than ever to keep data safe and networks functioning.[41] Subsea fiber cables have also come under increasing scrutiny as concerns grow around the possibility of antagonistic states damaging cable networks amidst tension or conflict.[42]

However, the protection of critical national assets often proves to be a complex affair as digital infrastructure networks across the globe tend to be primarily funded, owned, and operated by the private sector.[43] Critical gaps potentially exist between private- and public-sector defense capabilities as well as remits — while an individual private-sector entity may have its own cybersecurity measures, its systems and protocols are rarely designed with ecosystem-wide interdependencies in mind, and furthermore do not always account for physical threats. The crux of the security challenge is thus to align public- and private-sector interests such that skillsets and resources complement well to produce system-wide synergies for resilience.

Way ahead

Mobilize across all phases of the crisis cycle

Governments can contribute in numerous ways to building preparedness and mitigating shocks in the rollout of digital assets. In the short term, this might involve government departments and agencies engaging in cross-sector and cross-border intelligence sharing, participating in regional surveillance networks, undertaking national risk assessments, adopting strong cybersecurity mandates, and developing contingency plans with full buy-in from stakeholders.

In the long run, agencies and state-owned institutions could invest in regional security or the digital networks of other countries to create a bulwark abroad for their domestic ecosystems, amongst other options. Agencies across a range of domains can also work together with regulators to support existing or encourage new private-sector initiatives to facilitate more effective post-crisis response and recovery. This may include encouraging industry associations to develop crisis codes of conduct that help establish expectations and guide behavior for enhancing private-sector capabilities that the public sector cannot match, for instance. As digital assets are typically owned by private firms differing in size and capabilities, government support through awarding loans, grants, or subsidies or providing human capital and security expertise will also be critical for protecting assets and the broader environment in which they operate.

Policy-in-action

Direct examples include **investments in regional security and overseas digital networks** to improve geopolitical stability, create a buffer against state-sponsored cyberattacks, and more. US and EU cross-sectoral investments in Ukrainian cyber defenses have helped improve the country's resilience as well as allowed participating countries and companies to gain valuable experience in deconstructing and countering different types of cyberattacks than those typically encountered domestically.[44] Similarly, AUKUS, the trilateral security pact between Australia, the UK, and the US, aims to develop cyber capabilities, AI, quantum technologies, and additional undersea capabilities through collaboration and information sharing. One area of particular focus is the protection of undersea fiber optic cables against tapping by antagonistic state actors.[45]

In other instances, government efforts focus on **coordinated crisis response and recovery efforts** in the event of an attack. The US Cable Security Fleet program, which aims to maintain a fleet of government-licensed but privately owned vessels that can quickly repair damaged subsea cables, is one example of a new cross-sectoral initiative for enhancing resilience.[46] An indirect example for digital infrastructure is Australia's Data Availability and Transparency Bill, which imposes mandatory vulnerability assessments and regular reporting while affording enhanced powers for direct intervention by a National Data Commissioner.[47] While this bill concerns public-sector data, its central tenets of boosting transparency and regulatory force can be applied to the governance of digital networks, especially given the public-facing nature of many such services.

A key role for governments in ensuring cyber resilience comes in the form of **conducting simulation and stress-testing activities**. In 2018, the Bank of England, in partnership with the UK's most systemically important financial firms and other financial authorities, required participants to respond to a cyberattack scenario in a joint exercise between the public and private sectors.[48] Digital infrastructure operators could be required to partake in similar cybersecurity exercises to improve their crisis preparedness and response capabilities. Similarly, InfraStress was an EU-led project aimed at improving the cyber and physical security of Sensitive Industrial Plants and Sites (SIPS) infrastructure through stress-testing, modeling, and solution-development workshops.[49] A digital infrastructure-focused version of such an initiative could bolster risk understanding and spur innovation around asset resilience.

Watchpoints

- Stronger regulation, which is often at least initially necessary for greater security and resilience, may not always be congruent with firms' interests and risk management strategies. Consequently, to compose a truly "whole-of-society" approach to asset integrity, lawmakers and regulators will have to communicate clearly and openly to secure political traction for more aggressive measures, particularly those involving greater centralization. They may have to explore creative framing and incentivization strategies to generate buy-in where businesses fail to subscribe to wider or longer-term goals. Moreover, regulators need to consider whether smaller players can meet heightened expectations on this front — and, indeed, how best to remedy any potential constraints, shortfalls, or pitfalls in engagement and implementation.
- For strategies where private-sector leadership is a prerequisite, regulators risk appearing paternalistic if they attempt to dictate substantive details, terms, and conditions. At the same time, however, they should be careful not to afford too much discretion to industry associations lest the end result neglect wider strategic considerations and impact other national goals: Firms may prefer to cut costs and avoid large-scale, cross-sectoral exercises that yield greater benefits for the wider ecosystem than individual actors, for instance. In navigating this dilemma, it is essential that regulators and other agencies actively contribute by helping to identify desired outcomes, guide design, and highlight systemic interdependencies. For instance, with crisis codes of conduct, the national regulator could be better placed to advise if it would be more effective to pursue an overarching sector- or nation-wide code with built-in contingency and flexibility mechanisms, or merely high-level principles or guidelines that subsequently inform sector-specific or even crisis-specific codes.

Issue

Managing potential supply and labor bottlenecks

A truly resilient digital ecosystem is not only capable of managing and recovering from critical outages, but is also forward-looking and well-equipped to counter shocks that will affect rollout and operations. Pandemic-related transportation woes, coupled with drops in production capabilities, led to a severe shortage of semiconductor chips in 2021. As a result, US operators saw material supplies fall from an average of 40 days' worth in 2019 to just five days' worth in December 2021, resulting in major disruptions across reliant industries[50], and a full percent age point drop in the country's GDP.[51] A telecommunications provider in the Philippines was also unable to meet its original target of 1,600 5G towers, only building 300 due to these shortages.[52]

Supply chain issues remain pervasive in 2022, taking the form of pandemic-related port congestion in key Chinese ports and geopolitical conflict between Russia and Ukraine. Combined, both Russia and Ukraine account for a significant portion of global noble gas and rare earth production (including palladium, manganese, xenon, neon, and krypton), which are crucial components of semiconductors and chips. Further, the conflict has caused disruptions along key trade routes — both sea and land — around Eastern Europe and Asia, leading to six-fold increases in shipping costs and significant delays in the delivery of component parts.[53]

Additionally, there is a worldwide shortage of the skilled labor necessary to install and maintain digital infrastructure assets — largely owing to the high private costs of training laborers (that is, an estimated $12,000 per worker in the US)[54] — which has led to delays in projected rollouts of fiber networks and 5G towers as well as growing operator frustration. More than 20,000 tower climbers are required in the US to meet current 5G demand, while the expansion of both 5G and fiber networks will create 850,000 new jobs by 2025, although it remains to be seen how operators will fill these vacancies.[55]

Way ahead

Anticipate operational interdependencies and mitigate disruptions

Governments can adopt systems and protocols to anticipate and counter shocks with a mix of approaches befitting the country's economic landscape, which may include supply-chain management strategies, bilateral trade agreements, and various workforce policies. The intrinsic challenge with building resilience in this space is that these shocks are often unpredictable, and regulators may only have access to a limited number of policy levers to mitigate them. Nevertheless, private sector-led initiatives often lack the reach and strategic purview of government-backed programs, rendering high-level oversight necessary in the case of critical digital networks.

Departments, agencies, and industry associations should help facilitate the flow of information between critical stakeholders — both public and private — to identify and tackle potential operational mismatches as they arise. This may involve comprehensive risk-mapping efforts, which will require that government entities maintain strong alliances with industrial players, build expertise on identifying system vulnerabilities to various political currents, and tap on the knowledge of inter-ministry capabilities to understand the intricacies of how any given disruption could affect the economy. Prior to launching a response, legislators may also want to critically evaluate their country's existing capacities — understanding production capabilities, relationships with key trade partners, and current workforce landscapes — to determine what responses will be realistic and appropriate.

Policy-in-action

In response to the shortage of semiconductor parts in the US, the Biden administration established a dedicated Supply Chain Disruptions Task Force in 2021, which tapped on public and private stakeholders, to **monitor supply chain risks and to address supply/demand mismatches** as they arose.[56] The Administration later made a $17 billion commitment to work with local companies to boost the manufacture of semiconductor parts. The UK faced similar shortages of semiconductors in 2021. With limited semiconductor manufacturing capabilities themselves, the UK instead announced a bilateral agreement with South Korea to reduce trade barriers specific to the semiconductor supply chain to reduce the risk and intensity of future shortages.[57]

The shortage of laborers in the telecommunications sector has been widespread and pervasive across markets and has led numerous governments to respond by **launching workforce recruitment and training programs**. In Singapore, this has taken the form of the 5G & Telecoms Academy, a government-funded program that has (re)trained over 3,000 telecom workers in 5G mobile technology skills, with another intake of 5,000 workers over the next two years.[58] Elsewhere, the US Federal Communications Commission's 5G Jobs Initiative has expanded in-school programs to recruit and train prospective telecom workers, with increased community outreach efforts to low-income, high-unemployment areas.

Watchpoints

- Operational disruptions can severely stunt the rollout of digital networks that are vital to national and economic security, and while it may be natural for legislators to want to intervene across all anticipated disruptions, it is not always prudent to do so. Regulators should take care to ensure that all policy responses are proportionate to the magnitude of a disruption, allowing catastrophic disruptions to be averted without overreacting to natural market fluctuations, to incentivize businesses to innovate and become more efficient over time.
- Beyond merely facilitating information exchange and supporting the risk management efforts of public- and private-sector stakeholders, regulators could consider setting explicit standards on implementing adequate controls against supply-chain risks, with robust enforcement mechanisms, such as contracting requirements, to secure at least a baseline level of resilience. They could also mandate the reporting of said risks and existing and planned measures to reduce exposure and mitigate potential impacts.
- Given the dynamism of the digital landscape, the skill set of the average worker has and will likely evolve rapidly over the next decade. Conducting frequent pulse checks on the industry, such as communicating with industry associations and relevant academics, will be fundamental to understanding the future needs of the workforce, and how relevant government departments may be in supporting the industry's expansion over time.
- At the same time, cross-sector responses are expensive, meaning that budgetary constraints should always be taken into account before action and allocated against the most pressing threats. Instead of rolling out public initiatives, departments and agencies with limited financial resources could look toward building strategic public-private partnerships (PPPs) with operators to share the costs of potential ventures, such as the buildout of co-funded training programs.

Closing thoughts

The sovereignty, sustainability, and resilience of a nation's digital infrastructure network directly impacts the stability and security of broader institutions, structures, and systems critical to regular functioning. Effective governance therefore requires governments to embrace their unique position as a powerful yet non-absolute entity within national digital infrastructure ecosystems. They must work with private-sector stakeholders that directly operate sensitive assets, commit to crafting and enforcing appropriate legislation and regulation, and offer assistance, encouragement, and incentives to direct the private sector toward desired ends. Departments, agencies, and other public-sector stakeholders may in turn find themselves applying their capabilities and resources in different capacities vis-à-vis the private sector depending on the prevailing context around a given issue. Given that different entities will naturally have discrete agendas and remits, cross-government alignment and coordination are key to any successful endeavor.

The cross-cutting nature of the various imperatives outlined in this report introduces another layer of complexity to governance efforts. Accounting for contingencies and designing for synergy in conjunction with a wide range of stakeholders can therefore improve the reliability and sustainability of solutions. Ultimately, the greatest challenges for legislators and regulators may well be to strike the right balance between "carrots" and "sticks" to maximize private-sector participation, if not leadership, and to navigate the fine line between structure and overreach. To that end, clarifying roles and responsibilities by identifying optimal working dynamics for each relationship may help enhance the efficacy of cross-sectoral collaboration.

In the broader picture, keeping an open ear and ensuring clear and consistent communication across sectors can help precipitate ideas that can generate greater traction among all involved, including citizens and consumers, to achieve the "whole-of-society" effort needed for holistic, long-term governance. While it is not within the scope of this initial discussion, it may also be important for public-sector decision-makers to embrace the third sector within national planning arrangements. Integrating their unique capabilities and perspectives into ongoing dialogue and innovation could facilitate more expansive discussions around expectations for digital services or even out-of-the-box strategies beyond the typical reach of the public and private sectors.

Acknowledgements

Authors

Blair Chalmers

Managing Director, Marsh McLennan Advantage
blair.chalmers@mmc.com

Rachel Juay

Research Analyst, Marsh McLennan Advantage
rachel.juay@oliverwyman.com

Darrel Chang

Research Analyst, Marsh McLennan Advantage
darrel.chang@oliverwyman.com

Contributors

Richard Smith-Bingham, Ben Hoster, Swati Khurana, Martin Bennett, Richard Owen Phillips, Zia Bhadiar and Boris Tawakkoli

Designed by Tezel Lim

References

1 OECD. (2020). *Digital Transformation in the Age of COVID-19*. OECD.

2 Bloomberg, & PR Newswire. (2021, July 28). *5G Infrastructure Market Size Worth $80.5 Billion By 2028 | CAGR: 49.8%: Grand View Research, Inc.* — Bloomberg.

3 PR Newswire. (2021, September 3). *Global Internet Data Centers Market Report 2021: U.S Market is Estimated at $16 Billion, While China is Forecast to Grow at 17.5% CAGR by 2027.*

4 Businesswire. (2021, June 30). *Global Fiber to the X Market Report 2021: U.S Accounts for Over 19.5% of Global Market Size in 2020, While China is Forecast to Grow at a 11.1% CAGR for the Period of 2020-2027*. ResearchAndMarkets.

5 Oberlo. (2022, February 12). *10 Artificial Intelligence Statistics You Need to Know in 2022 [Infographic].*

6 Columbus, L. (2020, May 18). *10 Ways AI Is Improving Manufacturing In 2020*. Forbes.

7 Oberlo. (2022, February 12). *10 Artificial Intelligence Statistics You Need to Know in 2022 [Infographic].*

8 Wee, K. (2021, May 21). *The curious case of green data centers*.

9 Actis. (2022, March 7). *Global Digital Infrastructure: Enabling a Just Transition*. Actis.

10 Maincubes. (2021). *Solving the Data Soveregnty Conundrum*. Maincubes.

11 Leviathan Security Group. (2015). Quantifying the Cost of Forced Localization. 16.

12 Lunden, I. (2016, May). *PayPal to halt operations in Turkey after losing license, impacts 'hundreds of thousands'*. TechCrunch.

13 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 and Innovation Foundation.

14 Davies, J. (2020, August 4). *Nokia, Ericsson and Huawei dominance beginning to fade — analyst*. Telecoms.com.

15 World Economic Forum. (2021). *Delivering Digital Infrastructure — Advancing the Internet Economy*. World Economic Forum.

16 Bizo, D. (2021). *Uptime Institute Global Data Center Survey 2021 — Growth stretches an evolving sector.* 26.

17 Mytton, D. (2021). *Data centre water consumption*. Npj Clean Water, 4(1), 1-6.

18 Bizo, D. (2021). Uptime Institute Global Data Center Survey 2021 — Growth stretches an evolving sector. 26.

19 Siddik, M. A. B., Shehabi, A., & Marston, L. (2021). *The environmental footprint of data centers in the United States*. Environmental Research Letters, 16(6), 064017.

20 Bizo, D. (2021). *Uptime Institute Global Data Center Survey 2021 — Growth stretches an evolving sector.* 26.

21 Kang, S. C., Liu, P., & Thompson, D. (2021). *Beijing steps up power and renewable energy regulations on datacenters*. 5.

22 Dutch Data Center Association. (2020). *The State of Dutch Data Centers*. Dutch Data Center Association.

23 National Environment Agency. (2019). *Carbon Tax*.

24 U.S Securities and Exchange Commission. (2022, March 21). *SEC Proposes Rules to Enhance and Standardize Climate-Related Disclosures for Investors*. Retrieved April 5, 2022.

25 European Commission. (2022). *Code of Conduct for Energy Efficiency in Data Centres*.

26 Miller, R. (2020, September 14). *Google: Our Data Centers Will be Carbon-Free, Round-the-Clock by 2030*. Data Center Frontier.

27 Global Infrastructure Hub. (2021, October 14). *Infrastructure as a stimulus is $3.2 trillion — What outcomes can we expect for people and planet?.* Retrieved April 5, 2022.

28 Global Infrastructure Hub. (2021, December). *Infrastructure Monitor 2021*.

29 Roach, John. (2020, September 14). *Microsoft finds underwater datacenters are reliable, practical and use energy sustainably*. Microsoft. Retrieved March 24, 2022.

30 Judge, Peter. (2021, January 13). *China launches underwater data center.* Data Center Dynamics. Retrieved March 24, 2022.

31 Ramos, Ariana, Markku Tuovinen, and Mia Ala-Juusela. "Battery Energy Storage System (BESS) as a service in Finland: Business model and regulatory challenges." *Journal of Energy Storage* 40 (2021): 102720.

32 Leto, Giuseppe. (2021, August 31). *Going Green: Decarbonizing the Data Center Industry*. Mission Critical. Retrieved March 24, 2022.

33 Judge, Peter. (2022, January 25). *UPSs at Telia's Helsinki data center to put power into the grid*. Data Center Dynamics. Retrieved March 24, 2022.

34 RPS Group. (2020). *Rhode Green Energy Park: Opportunity Assessment Report*. RPS Group.

35 Clay, L. (2019, January 14). *Rethinking data center design for Singapore*. Engineering at Meta.

36 Chitakasem, P., Rao, A., Neo, C. C., Yeo, J., & Cheam, J. (2020). *The future of data centres in the face of climate change*. Eco-Business.

37 Mah, P. (2021, October 14). *Singapore's sustainability drive*.

38 Gregg, A., & Harwell, D. (2021, December 22). *Amazon Web Services' third outage in a month exposes a weak point in the Internet's backbone*. The Washington Post. Retrieved April 13, 2022.

39 Isaac, M., & Frenkel, S. (2021, October 8). *Gone in Minutes, Out for Hours: Outage Shakes Facebook*. The New York Times. Retrieved April 13, 2022.

40 Check Point Research. (2022, January 10). *Check Point Research: Cyber Attacks Increased 50% Year over Year*. Check Point Blog. Retrieved April 13, 2022.

41 Harding, Luke. 2022, March 1. *Ukraine says Russia targeting civilians as missiles hit Kyiv TV tower*. The Guardian. Retrieved March 14, 2022.

42 Brzozowski, Alexandra. 2020, October 23. *NATO seeks ways of protecting undersea cables from Russian attacks*. Retrieved March 14, 2022.

43 Asian Infrastructure Investment Bank. 2020, January 10. *Digital Infrastructure Sector Analysis*.

44 Kagubare, I. (2022, March 13). *US, EU cyber investments in Ukraine pay off amid war*. The Hill. Retrieved March 15, 2022.

45 Unal, B. et al. (2021, September 16). *Is the AUKUS alliance meaningful or merely provocation?*. Chatham House. Retrieved March 30, 2022.

46 US Maritime Administration. 2021, January 5. *Request for Applications to Be Considered for Enrollment in the Cable Security Fleet*.

47 *Australian Data Availability and Transparency Bill 2020* (Cth) pt 4.2 div 1.

48 Bank of England. (2019, September 27). *Sector Simulation Exercise: SIMEX 2018 report*. Retrieved March 30, 2022.

49 *InfraStress* (n.d.). Retrieved March 30, 2022.

50 BBC News. (2022, January 26). *Global chip shortage: US says firms' stocks have plunged*. BBC News.

51 Business Times. (2022, April 6). *Biden aide Deese says semiconductor shortage cost 1% of US GDP*, Technology — THE BUSINESS TIMES.

52 S&P Global Market Intelligence. *Asia-Pacific Tower and Small Cell Projections through 2031*. March 31, 2021.

53 Tan, W. (2022, March 11). *How the Russia-Ukraine war is worsening shipping snarls and pushing up freight rates*. CNBC.

54 Egan, Casey. 2020. *US Policymakers Tackle 5G Workforce Shortage*. January 22, 2020.

55 Maurer, Roy. 2020. *The 5G Workforce Needs a Big Boost*. SHRM. January 28, 2020.

56 The White House. (2021, June 8). *FACT SHEET: Biden-Harris Administration Announces Supply Chain Disruptions Task Force to Address Short-Term Supply Chain Discontinuities*. The White House.

57 James, W. (2022, February 7). *UK and South Korea to sign deal to strengthen supply chains*. Reuters.

58 Chee, K. (2021, November 17). *"Rapid progress" made with 3,000 S'poreans trained in 5G skills in national drive*. The Straits Times.

This report and any recommendations, analysis or advice provided herein (i) are based on our experience as insurance and reinsurance brokers or as consultants, as applicable, (ii) are not intended to be taken as advice or recommendations regarding any individual situation, (iii) should not be relied upon as investment, tax, accounting, actuarial, regulatory or legal advice regarding any individual situation or as a substitute for consultation with professional consultants or accountants or with professional tax, legal, actuarial or financial advisors, and (iv) do not provide an opinion regarding the fairness of any transaction to any party. The opinions expressed herein are valid only for the purpose stated herein and as of the date hereof. We are not responsible for the consequences of any unauthorized use of this report. Its content may not be modified or incorporated into or used in other material, or sold or otherwise provided, in whole or in part, to any other person or entity, without our written permission. No obligation is assumed to revise this report to reflect changes, events or conditions, which occur subsequent to the date hereof. Information furnished by others, as well as public information and industry and statistical data, upon which all or portions of this report may be based, are believed to be reliable but have not been verified. Any modeling, analytics or projections are subject to inherent uncertainty, and any opinions, recommendations, analysis or advice provided herein could be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. We have used what we believe are reliable, up-to-date and comprehensive information and analysis, but all information is provided without warranty of any kind, express or implied, and we disclaim any responsibility for such information or analysis or to update the information or analysis in this report.

We accept no liability for any loss arising from any action taken or refrained from, or any decision made, as a result of or reliance upon anything contained in this report or any reports or sources of information referred to herein, or for actual results or future events or any damages of any kind, including without limitation direct, indirect, consequential, exemplary, special or other damages, even if advised of the possibility of such damages. This report is not an offer to buy or sell securities or a solicitation of an offer to buy or sell securities. No responsibility is taken for changes in market conditions or laws or regulations which occur subsequent to the date hereof.

Marsh McLennan www.mmc.com