

**Infrastructure**

**Digital  
Resilience**

**Economy**

**Policy**

# DCO

## Policy Watch

Navigating Disruption:  
Policy Perspectives on  
Digital Resilience

**Edition 5** | July 2025



# Table of contents

	<b>Executive Summary</b>	1
<b>1</b>	<b>Defining Digital Resilience</b>	4
	Three Dimensions of Digital Resilience	7
<b>2</b>	<b>From Reaction to Resilience: Policy Shifts in Response to Global Disruptions</b>	9
	Disruption #1: Geopolitical Dynamics	10
	Disruption #2: Economic Dependencies and Supply Chain Disruptions	11
	Disruption #3: Infrastructure Failure and Cyber Incidents	11
	Disruption #4: Regulatory and Market Shifts	13
<b>3</b>	<b>The Evolving Digital Policy Responses</b>	14
	Policy Responses and Strategies Across Regions	14
	Cloud and Data Sovereignty: Local Data Localization Mandates and National Cloud Initiatives	19
	Labor Market Resilience and Workforce Development Policies	20
<b>4</b>	<b>Multilateralism Under Pressure: New Alignments and Alliances</b>	24
	1. Traditional Multilateral Institutions Adapting to Digital Realities	24
	2. Emergence of Alternative Multilateral Frameworks for Digital Resilience	25
	3. Multilateral Digital Cooperation and Diplomatic Integration	26
	4. Cybersecurity, Data Standards, AI: Multilateral Tools to Build Resilience	27
<b>5</b>	<b>Conclusion: The Future of Digital Resilience</b>	29

---

# Executive Summary

---

Welcome to the fifth edition of the DCO Policy Watch, a special issue focused on the urgent and multidimensional concept of digital resilience. As global disruptions increasingly test the strength of digital infrastructure, regulatory frameworks, and cross-border cooperation, this edition investigates how national and regional strategies are evolving to respond. Rather than viewing digital resilience as solely a technical or cybersecurity issue, the DCO Policy Watch 5 emphasizes its broader significance as a strategic policy imperative. This includes sovereignty over data, technology, and regulation, the enforceability of domestic policies in a transnational environment, and strategic control over critical digital infrastructure. At its core, this issue emphasizes how evolving governance frameworks and policy responses are becoming vital levers for ensuring resilience during disruptions.

Building on prior editions, which examined foundational elements of the digital economy, from digital public infrastructure (DPI) to responsible ecosystems and sustainable societies, this special issue introduces digital resilience as a critical lens through which governments plan for national stability, economic continuity, and more cohesive digital cooperation.

This edition presents a working definition of digital resilience that captures the capacity of governments, businesses, and digital systems to anticipate, absorb, adapt or respond to, and recover from disruption while sustaining essential functions and preserving long-term strategic objectives. It articulates three dimensions of digital resilience:

- **Infrastructure Dimension** – ensuring continuity of services through redundancy, autonomy, and security in cloud, network, power, and data infrastructure.

- **Economic Dimension** – reducing dependence on single points of failure by diversifying sources of digital goods and services (e.g., semiconductors, cloud providers, code libraries).
- **Policy Dimension** – increasing the agility of policy and regulatory frameworks, and multilateral coordination mechanisms to respond to evolving risks and shifting geopolitical dynamics. This will also include crisis response and governance resilience, focusing on developing adaptive legal and institutional mechanisms capable of addressing emerging threats such as misinformation, systemic platform failures, or malicious technology misuse. Equally important, policy resilience involves forward-looking national strategies and regulatory foresight that anticipate future disruptions and embed resilience into long-term digital planning.

In recent years, recurring disruptions have exposed vulnerabilities across the broader digitally-driven systems that underpin modern economies, governance, and daily life. From infrastructure outages and cyber incidents to protectionist trade policies and AI-related risks, the frequency and scale of these developments reveal structural vulnerabilities across the digital economy. In response, governments are accelerating efforts to enhance localized infrastructure, diversify supply chains, and reform digital policy frameworks to ensure continuity, adaptability, and strategic autonomy.

As this transformation unfolds, digital policy is increasingly shaped by diverging geopolitical priorities. Governments are navigating competing priorities, balancing the need for cross-border collaboration with domestic imperatives for sovereignty over data, infrastructure,

and regulation. As a result, some nations and regions are pushing for harmonized governance models, while some are adopting protectionist or self-sufficient approaches in response to emerging risks.

At the international level, traditional institutions are under pressure to keep pace with rapid digital transformation and shifting power dynamics. In parallel, new regional and international coalitions are emerging, focusing on specific domains such as cybersecurity, AI, and digital trade. These new alignments offer alternative pathways for digital cooperation, but also raise important questions about coherence, inclusivity, and interoperability.

The fifth edition of the DCO Policy Watch concludes by examining practical implications of recent disruptions on the digital economy. As digital trade,

digital finance, data flows, and emerging technologies continue to evolve at pace, the imperative for resilience becomes increasingly urgent, particularly in the face of rising cyber threats, systemic platform dependencies, and increasing geopolitical and regulatory fragmentation.

The most resilient digital economies and ecosystems will be those capable of maintaining openness while managing risks, fostering innovation while ensuring security, and driving prosperity while advancing sustainability. By exploring these dynamics through a policy lens, this edition aims to support DCO stakeholders - and the broader international community - in shaping resilient and inclusive digital futures.

---

# 1 Defining Digital Resilience

---

According to a recent academic research, digital resilience [refers](#) to the ability of digital systems, assets, and activities to continue operating under stress and to recover swiftly from shocks. Importantly, achieving that stable state implies that after a crisis, a [system](#) is more prepared for future challenges, not simply reverting to a pre-crisis state.

As various organizations and policy bodies have sought to define digital resilience, each emphasize different dimensions in line with their distinct mandates and priorities. For example, the Organisation for Economic Co-operation and Development (OECD) frames digital resilience within the broader context of economic transformation and [digital security](#), emphasizing the need for trust and continuity in digitally dependent economies. Meanwhile, the European Union (EU) Agency for Cybersecurity [focuses](#) on the resilience of systems and services against cyber threats and disruptions. These variations reflect the multifaceted nature of digital resilience, which encompasses both systemic and operational dimensions.

Recognizing the various approaches, we offer the following working definition of Digital Resilience:

**“Digital resilience is the capacity of governments, businesses, and digital systems to anticipate, adapt or respond to, and recover from disruptions while maintaining continuity of core functions and preserving the strategic objectives.”**

In practical terms, digital resilience at the national, regional, and global levels involves the ability of governments and interconnected systems, including public institutions, private sector partners, and critical infrastructure providers, to withstand adverse events and leverage them as opportunities to strengthen digital governance, infrastructure, and interagency coordination. This perspective highlights that resilience is not only about survival, but about transformation and leapfrogging using disruption as the key catalyst for long-term improvement.



To understand how digital resilience is achieved, it is useful to examine it as a process. This process can be conceptualized through four interlinked phases: anticipation, absorption, adaptation, and recovery.



#### **Anticipation:**

Involves proactive risk identification and scenario planning. This includes investing in early warning systems, digital infrastructure audits, and cross-border coordination to boost resilience.



#### **Absorption:**

Refers to the capacity to endure shocks without systemic collapse. This includes maintaining continuity of critical digital services through redundancy, decentralization, and flexible operational models. For example, during infrastructure outages or cyber incidents, resilient systems can reroute traffic, activate backup protocols, or shift workloads across jurisdictions to preserve essential functions. During infrastructure outages or cyber incidents, resilient systems can reroute traffic, activate backup protocols, or shift workloads across jurisdictions to preserve essential functions.

#### **Case Study: OVHcloud Data Centre Fire (2021) – A Test in Digital Resilience**

In 2021, a major fire broke out at OVHcloud's (one of Europe's largest cloud service providers) data center in Strasbourg, France. The incident led to the destruction of the SBG2 data centre and partial damage to others on site, affecting millions of websites and critical digital services, including those of government agencies, banks, and universities across Europe. Despite the sudden infrastructure loss, OVHcloud

promptly initiated disaster recovery protocols, rerouted services to other data centers across France and Germany and communicated transparently with clients about service restoration timelines. Within days, most services were back online, and full infrastructure restoration followed through a combination of cloud redundancy and rapid operational response.



#### **Adaptation:**

Is the process of recalibrating systems and policies in response to disruption. This may involve updating cybersecurity frameworks or protocols after cyberattacks, reconfiguring digital supply chains, or reallocating public investments to digital priorities. Adaptation is not merely reactive as it reflects institutional learning and policy agility in the face of evolving risks.



#### **Recovery:**

Captures long-term strategic shifts that follow disruption. Crises can serve as inflection points, prompting governments to fast-track reforms that had previously stalled. A notable [example](#) is found in the accelerated digital transformation that followed the onset of the COVID-19 pandemic.

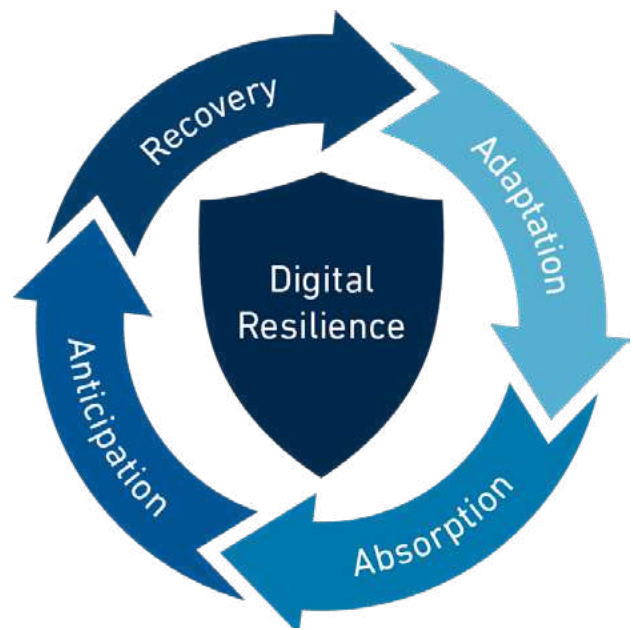


---

Together, these phases form a dynamic cycle that enables economies to not only withstand disruption but emerge stronger and more strategically aligned. This framework sets the stage for the next section, which explores the three core dimensions of digital resilience: infrastructure, economic, and policy resilience.

Recent events have exposed the fragility of the interconnected digital and traditional systems, each increasingly reliant on the other, when faced with disruption. For example, in April 2025, a major power outage affected nearly 60 million people in Portugal and Spain. Within seconds, Spain [lost](#) approximately 15 gigawatts of power – around 60% of its supply causing significant [impact](#) on businesses and the broader [economy](#) as digital communications and services halted.

In this context, digital resilience has emerged as a policy imperative—extending beyond technical concerns to serve as a strategic foundation of national resilience.



## Three Dimensions of Digital Resilience

To gain a comprehensive understanding of digital resilience, it is useful to consider three interrelated dimensions: **infrastructure, economic, and policy (governance) dimensions**. This lens offers a structured approach to analyzing how economies can strengthen their digital foundations against disruption:



### 1. Infrastructure Dimension

The infrastructure dimension of digital resilience refers to the robustness and continuity of the physical and digital systems that deliver digital services. This includes data centers, broadband networks, cloud platforms, and energy systems. For instance, **redundancy** ensures that if one system fails, another can take over. Estonia's e-government infrastructure exemplifies this: its use of a Data Embassy in Luxembourg, [ensures continuity](#) of digital services even in the event of a domestic crisis.

#### Case Study: Estonia's Data Embassy

Estonia has taken a proactive approach to infrastructure resilience through the establishment of its "Data Embassy". In 2017, Estonia launched its first Data Embassy in Luxembourg, hosted in a high-security data center under full Estonian jurisdiction, enabled through a bilateral agreement. This facility mirrors essential databases and systems, including national registries and e-governance platforms, ensuring that the state can continue operating even in the face of unforeseen disruptions or crises.

**Autonomy** is equally critical. This refers to the [ability](#) of digital infrastructure to function independently, without relying on external control, foreign platforms, or centralized systems that may fail or become inaccessible during emergencies. Autonomous systems include sovereign cloud platforms, localized data centers, and decentralized emergency networks that can maintain operations even if international links are severed. During the 2025 blackout in Portugal and Spain, the lack of autonomous local systems meant that digital payment, communications, and emergency services were severely disrupted. Countries investing in sovereign cloud infrastructure and localized data centers, such as France's "[Cloud de Confiance](#)" initiative, might be better positioned to maintain operations when global networks are compromised.

Finally, **cybersecurity** is foundational. Without robust protection, even the most redundant systems are vulnerable. The OECD [emphasizes](#) that digital public infrastructure (DPI) must be secure and interoperable to support inclusive and resilient service delivery. A recent reminder of this surfaced during the [CrowdStrike incident in 2024](#), when a faulty update from the cybersecurity firm triggered a global IT outage. Though not the result of a malicious cyberattack, the misconfiguration caused widespread failures in Windows-based systems across governments, airports, hospitals, and enterprises, from the UK and US to Australia and India. Airlines grounded flights, emergency call centers experienced delays, and critical hospital equipment malfunctioned. The disruption exposed how even a single weak link, in this case, a security provider's update pipeline, can undermine the stability of supposedly resilient infrastructures.



## 2. Economic Dimension

The economic dimension of digital resilience addresses the ability of economies to withstand digital disruptions, such as supply chain shocks or dependency on a single vendor or nation for critical technologies. The COVID-19 pandemic revealed how fragile global digital supply chains can be, particularly in areas like semiconductors, routers, cloud hosting, and device manufacturing.

Diversification is key. The global semiconductor shortage between 2020 and 2022 exposed the risk of non-diversification, prompting the EU to launch [the European Chips Act](#), which aims to double Europe's share of global chip production by 2030. Similarly, [India's DPI](#) strategy promotes open-source, interoperable platforms, such as [Aadhaar](#) or [UPI](#), reducing reliance on foreign technology providers and fostering domestic innovation. By encouraging domestic developers to build and scale services through shared public platforms, India reduces lock-in to foreign vendors, retains data sovereignty, and cultivates a local digital ecosystem that can grow independently. These efforts reflect a growing recognition that digital resilience from an economic perspective requires strategic diversification, domestic capacity building, and coordinated industrial policy.



## 3. Policy Dimension

The policy dimension of digital resilience refers to the **agility of governance systems** to respond to fast-moving digital risks while maintaining trust, oversight, and coherence. This includes creating flexible regulatory frameworks, coordinating across borders, and deploying emergency measures where necessary. The [EU's Digital Markets Act](#) (DMA) and [Digital Services Act](#) (DSA) exemplify proactive governance, aiming to regulate dominant platforms and ensure accountability in digital markets. Furthermore, during the COVID-19 pandemic, countries like

South Korea and Singapore rapidly adapted [data governance rules](#) to enable digital contact tracing while balancing privacy concerns.

In addition to regulatory responsiveness, policy resilience also involves the proactive development of national strategies that **anticipate future risks** and shape policy landscapes before crises emerge. This strategic dimension involves high-level planning, including setting national priorities, risk frameworks, and investment pathways that ensure digital systems can withstand, adapt to, and recover from disruptions.

Governments are increasingly developing national digital resilience frameworks that go beyond regulation to guide **whole-of-government responses**. For instance, the UK's [Government Resilience Framework](#) (2022) outlines systemic approaches to anticipate future threats; Singapore's [Safer Cyberspace Masterplan](#) (2020) emphasizes pre-emptive digital safety measures; Estonia's [Digital Agenda 2030](#) positions resilience as a pillar of digital innovation; and the UAE's [Digital Government Strategy 2025](#) emphasizes embedding resilience into core operations and capabilities. These examples highlight how resilience is being institutionalized through national planning, not just regulatory reform.

Policy resilience also entails investing in **institutional capacity**, such as skilled human capital, future-looking policymaking, capacity to fast-track cybersecurity protocols during an attack, and international coordination to manage transnational risks. As digital networks transcend national borders, countries engage in multilateral dialogue and regulatory harmonization to ensure that their domestic policies remain effective and enforceable in a fragmented global landscape.

These three dimensions of digital resilience – infrastructure, economic, and policy – are closely connected.

- A country's infrastructure resilience, for instance, cannot be fully achieved without considering its economic dependencies, such as reliance on foreign-manufactured digital equipment, cloud service providers, and undersea cable operators. These dependencies expose critical systems to geopolitical risks and supply chain disruptions, underscoring the need for diversified sourcing and domestic capacity building.
- But economic diversification alone is insufficient without the right policy frameworks. Building redundant networks or sovereign cloud infrastructure often requires regulatory mandates, public investment incentives, and regional agreements that enable cross-border interoperability and crisis coordination.
- This is where policy adaptability and regional cooperation become essential. For example, the EU's coordinated approach to cybersecurity, through mechanisms like the Network and Information Systems Directive 2 ([NIS2 Directive](#)), demonstrates how regional governance can enhance national resilience by setting common standards, facilitating information sharing, and enabling joint responses to cross-border threats.

Hence, digital resilience is best achieved through a holistic approach that strengthens physical networks, secures supply chains, and updates governance frameworks to respond to an increasingly volatile world. In this context, the growing frequency and impact of real-world disruptions make it essential to examine how countries are shifting from reactive responses to proactive policies that strengthen digital resilience.





---

# 2 From Reaction to Resilience: Policy Shifts in Response to Global Disruptions

---

The need for digital resilience has become increasingly evident in the face of ongoing and intersecting global disruptions. Events such as geopolitical conflicts, economic shocks, natural disasters, technological failures, and regulatory shifts have revealed vulnerabilities in both national digital systems and the broader global digital ecosystem. This section reviews how these disruptions have affected each of the three resilience dimensions, reinforcing the case for stronger safeguards and cooperation at national, regional, and international levels.

## **Disruption #1: Geopolitical Dynamics**

Geopolitical dynamics are increasingly shaping the digital landscape, with technological interdependence and competition introducing new dimensions of [vulnerability](#). Strategic measures such as export controls, investment restrictions, and resource limitations—particularly in areas like semiconductors and critical minerals—are influencing global supply chains and access to emerging technologies. For example, the US has introduced export controls on advanced chips and manufacturing equipment, while China has restricted exports of key minerals used in chip production.

These dynamics also extend to emerging technologies like AI, which are now at the center of geopolitical tensions. Control over AI capabilities - including access to high-performance compute power, foundational AI models, and critical data assets has become a strategic priority for many nations. Countries

without sovereign AI capabilities risk becoming passive consumers of AI technologies developed elsewhere, with limited influence over their design, governance, or ethical parameters. This imbalance threatens to widen the digital divide and reduce national capacity to ensure resilient and context-appropriate AI integration.

These dynamics are prompting countries to reassess their digital strategies, alliances, and risk exposures. The result is a more fragmented technology environment, where regulatory divergence, cross-border trade constraints, and shifts in digital partnerships are affecting the resilience and openness of digital ecosystems.



---

## Disruption #2: Economic Dependencies and Supply Chain Disruptions

The COVID-19 pandemic further highlighted the fragility of digital and technology supply chains, revealing how quickly disruptors can cascade across interconnected systems. Lockdowns increased demand for digital services and electronics, but [factory shutdowns](#) and logistics issues led to shortages of critical components like semiconductors. Stay-at-home orders led to a surge in [demand](#) for computers and other electronic devices due to the shift to remote work and schooling, while simultaneously restricting production at chip manufacturing facilities, many of which were either shut down or operating with reduced staff. The global chip shortage, which caused significant production delays and economic losses, highlighted the vulnerabilities of concentrated manufacturing in specific regions and the limitations of just-in-time supply models. These incidents revealed a lack of economic resilience in many countries. Consequently, policy measures such as chip subsidies and diversification strategies [were introduced](#) in the US.

Concentration of compute infrastructure is another concern, as the development and deployment of large-language models (LLMs) are highly dependent on advanced computing infrastructure, primarily high-performance GPUs and cloud-based data centers, which are predominantly operated by a limited number of global technology providers concentrated in a handful of advanced economies. This centralization creates a structural dependency for other nations, limiting their strategic autonomy and exposing them to potential supply chain disruptions, export controls, and access inequalities.



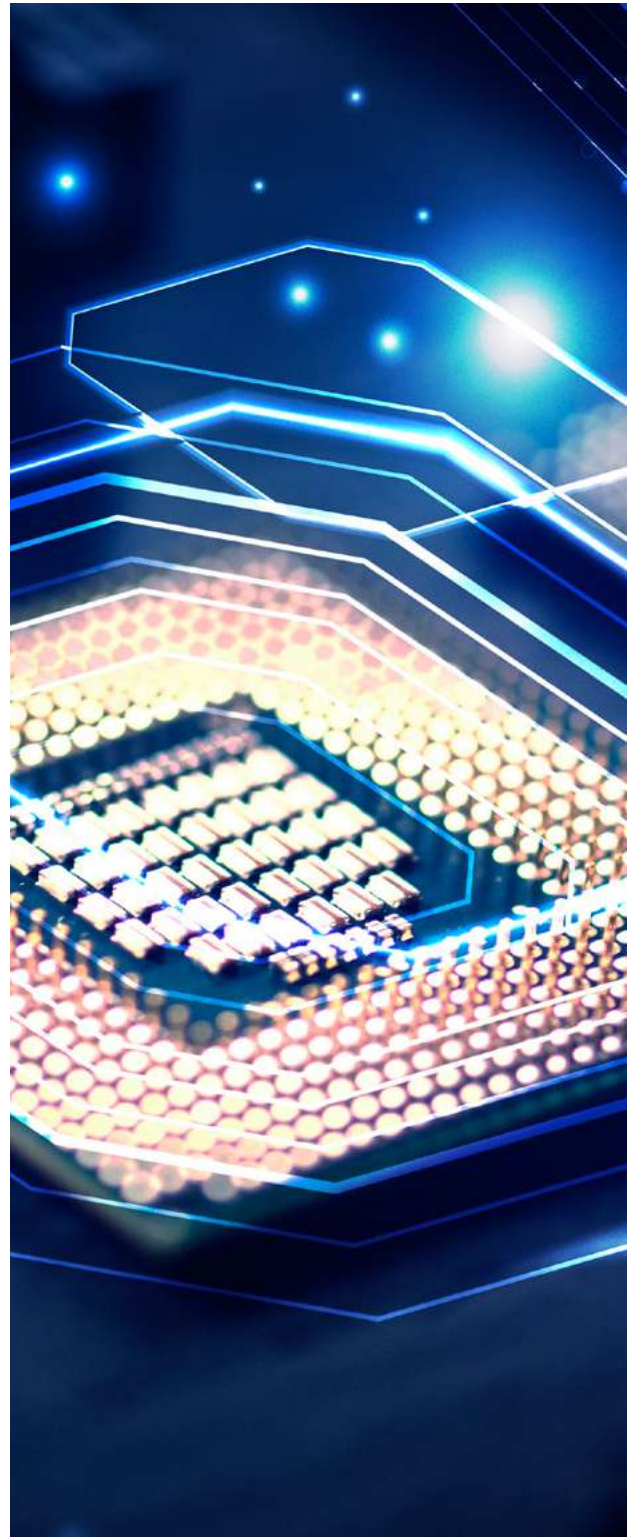
## Disruption #3: Infrastructure Failure and Cyber Incidents

High-profile incidents have also highlighted the fragility of digital infrastructure. In October 2021, a six-hour [Facebook outage](#) disrupted global communications and commerce and highlighted the need for alternatives and the risks associated with reliance on a small number of service providers. The disruption affected billions of users worldwide, halting key communication channels and interrupting business operations dependent on digital platforms. More recently, in March 2024, widespread service disruptions again revealed vulnerabilities in the global digital services ecosystem, with hundreds of thousands of users reporting access issues at the height of the outage.

In March 2024, seismic activity off the coast of the West African coast severed four major undersea cables, temporarily cutting off internet access to 13 countries. While submarine cable outages are not uncommon, averaging around 100 fiber cuts globally each year, they typically involve single cables and are resolved with [minimal disruption](#). What made this incident particularly significant was the simultaneous failure of multiple cables in the same geographic corridor, exposing a critical vulnerability in the region's connectivity infrastructure. The widespread impact underscored the lack of redundancy in international routing and over-reliance on a single submarine pathway.

In response, regional and international organizations began calling for more resilient infrastructure planning. The Carnegie Endowment for International Peace recommended a [dual strategy](#): investing in redundant cable routes and establishing harmonized governance frameworks at both national and regional levels to coordinate maintenance, risk monitoring, and emergency response.

Cyberattacks have been equally disruptive: ransomware and malware incidents have shut oil pipelines, hospitals, and government services. For example, the 2021 [ransomware attack](#) on Colonial Pipeline forced a shutdown of fuel distribution on the US East Coast, becoming a national security issue. In response, the Biden Administration issued Executive Order 14028, titled "Improving the Nation's Cybersecurity," just days later. The [Order mandated](#) stronger cybersecurity standards across federal agencies and contractors, including the adoption of zero-trust architecture, enhanced software supply chain security, and mandatory incident reporting for those doing business with the US government.





## Disruption #4: Regulatory and Market Shifts

Not all digital ecosystem disruptions are externally driven. Policy changes and evolving market dynamics can also create significant impacts, particularly when coordination is limited. For instance, the EU's DMA, designed to promote fairness, contestability, and safety in the digital economy, introduced notable regulatory changes affecting large digital platforms. The [legislation](#) requires designated "gatekeepers" to modify certain business practices. While intended to reduce concentration risks and enhance long-term digital resilience, such reforms have also introduced transitional uncertainty, and increased compliance demands for technology firms adapting to the new requirements.

These measures may also be viewed as efforts to address systemic risks—such as market dominance or algorithmic opacity—through regulatory means. At the same time, concerns have been raised by industry stakeholders, including some US-based companies, regarding the scale and cost of [compliance, claiming that the EU is targeting US firms](#). The Computer & Communications Industry Association [estimates](#) that large firms may face annual compliance costs of up to USD 430 million. This case underscores the importance of policy resilience: ensuring that regulatory interventions are well-calibrated, transparent, and supported by international dialogue to minimize unintended disruptions, reduce friction in digital trade, and maintain global interoperability.

In sum, turbulent events of the past few years, from conflict and pandemic to blackouts and differing perspectives on regulatory approaches such as those of the EU towards major technology companies, have laid

bare numerous digital vulnerabilities. These challenges have fostered a growing recognition among governments and industries that digital resilience is not a luxury, but a necessity. As the statement does not provide numerical data, it is challenging to represent it in a graph.



The below section examines how nations and regions have begun responding to these warnings by shifting policies and strategies to shore up their digital resilience.

# 3 The Evolving Digital Policy Responses

## Policy Responses and Strategies Across Regions

Governments worldwide are recalibrating their digital policies to enhance resilience in the face of geopolitical tensions, cyber threats, supply chain disruptions, and tariffs. Increasingly, these shifts are shaped by economic nationalism and digital sovereignty, as countries seek to assert greater control over their digital ecosystems. This is especially evident in sectors like semiconductors, where states are investing in domestic fabrication capacity; in cloud services, where national cloud initiatives and data localization policies are gaining traction; and in AI, where governments are balancing innovation with sovereign oversight.

These responses vary widely across regions, shaped by political priorities, technological capabilities, and existing regulatory ecosystems. This section highlights selected national responses that illustrate how states are pursuing efforts to secure their critical infrastructure, enhance their sovereignty, reduce dependencies, and modernize regulatory frameworks to better manage digital risks.



### Europe: Pursuing “Open Strategic Autonomy” and Digital Sovereignty

EU Member States have taken a comprehensive and proactive stance towards digital resilience, with an accelerated push after a series of

disruptions. The 2022 Russia-Ukraine conflict underlined Europe’s reliance on external parties for critical needs, such as energy and critical technologies. EU leaders, in the [2022 Versailles Declaration](#), stressed the need to reduce strategic dependencies in areas like semiconductors and digital technologies.

The risk of dependency became evident when energy supplies were disrupted, leading to broader discussions about technology supply chain resilience. Simultaneously, EU stakeholders recognized growing foreign influence over data governance, which led to the “[Digital Sovereignty for Europe](#)” initiative – the idea that the EU should have control over its digital destiny, including home-grown alternatives in cloud, data infrastructure, and platforms. The EU response has thus been multi-levelled, by focusing on the three aspects of digital resilience:

- **For infrastructure and cyber resilience,** the EU updated [NIS2 Directive](#) (2022), broadened the scope of mandatory cyber safeguards to more sectors (from energy grids to social media platforms) and set higher security standards to ensure continuity of essential services. Additionally, the EU has invested heavily in connectivity redundancy: through the [Connecting Europe Facility](#), it co-finances new cross-border fiber links and data center infrastructure in partnership with the public and private sectors. Spurred by the risk of undersea cable sabotage, some European countries are [investing in satellite](#)

broadband constellations and alternative routing. These efforts aim to ensure that, even if a major global service fails or is cut off, European users and companies have robust fallback options.

- **To boost supply chain resilience**, the EU aims to reduce reliance on foreign suppliers. [The European Chips Act](#) (2022–2023) was introduced to address supply chain risks exposed by the pandemic and global tensions, allocating billions to boost domestic chip production. Additionally, the EU is diversifying supply chains by partnering with countries like Japan and India to source critical materials and technology. This strategy, known as [“open strategic autonomy”](#), balances trade openness with the capacity for self-sustainability in case of global supply disruptions.
- **On the regulatory side**, the EU has been at the forefront of regulatory innovation in the digital space. The DMA, DSA, and the EU [AI](#) acts represent a new approach to governing large platforms. The DMA designates major online platforms as “gatekeepers” and imposes ex ante obligations – for example, requiring interoperability, fair access for business users, and limits on self-preferencing. The DSA implements responsibilities for digital services and requires mandatory risk assessments and content moderation accountability. The EU AI Act governs large platforms, particularly when developing high-risk AI systems or general-purpose of AI models that are widely deployed across sectors.

### **USA: Securing Supply Chains and Protecting Critical Technologies**

The US approach to digital resilience is shaped by its market-oriented philosophy, tempered by growing recognition of national security risks. As home to many of the world’s tech giants and advanced research, the US has historically enjoyed a position of digital dominance.

However, a series of developments have challenged this position, as countries like China have emerged as competitors. Additionally, the supply chain shocks of the pandemic and high-profile cyber incidents necessitated more action on the resilience front. Thus, US strategy has focused on economic and supply chain robustness, often framed as maintaining technological leadership and safeguarding security, which in turn ensures economic stability.

The US share of global semiconductor production fell from 36% in 1990 to 10% in 2020, causing economic and security worries. The [CHIPS and Science Act of 2022](#) was passed as a response to pandemic-era supply shocks, with funding aimed at strengthening the domestic chip supply. The Act allocated USD 39 billion in subsidies and tax incentives to semiconductor manufacturers, catalyzing over USD 500 billion in private investment. Alongside internal investments, the US has employed export controls and sanctions to address potential risks to its digital infrastructure and infrastructure integrity. The [export control campaign](#) peaked in October 2022 when the US imposed restrictions on advanced semiconductor technology exports to China, covering high-end chips and chip equipment.

In April 2025, US President Trump issued [Executive Order under Section 232](#) of the Trade Expansion Act to investigate the national security implications of US reliance on imported processed critical minerals and their derivatives. The investigation aims to evaluate supply chain vulnerabilities, economic impacts, and potential trade remedies to support domestic production. This action is part of a broader strategy to enhance US digital resilience by reducing dependence on foreign sources, particularly for materials essential to defense, infrastructure, and advanced technologies, and to ensure long-term economic and national security.

Compared to the EU, US digital policy has been perceived as being less restrictive. In AI governance, the US has favored voluntarily guidelines (such as the [NIST AI Risk Management Framework](#)) over binding regulations, aiming to address emerging risks without hindering innovation. This flexible approach reflects a form of policy resilience, allowing rapid adaptation as technologies evolve – illustrating how economic resilience can be shaped through industrial policy and strategic investment.



### **China: Strategic Self-Reliance and State-Steered Resilience**

China's approach to digital resilience is rooted in its drive for technological self-sufficiency and domestic capacity-building. Chinese policy documents, from the ["Made in China 2025"](#) plan to the current 14th [Five-Year Plan](#), have emphasized indigenization of high-tech industries. The latter emphasizes domestic investment, boosting internal demand across sectors such as energy, transportation, R&D, and the environment. China is accelerating [domestic technology manufacturing](#), maintaining an annual growth rate of over 9%, while its software industry continues to expand at a rate of 13%. Some measures that showcase China's resilience strategy include:

- The Broadband China initiative, which expanded fibre and broadband access across urban and rural areas. Chinese cities demonstrated greater economic resilience during the COVID-19 pandemic thanks to more robust digital infrastructure.
- The Digital Silk Road, part of the broader Belt-and-Road Initiative, which has delivered over \$79 billion in digital infrastructure (terrestrial and subsea cables) across Asia, Africa, and Europe, strengthening network redundancy.



### **GCC Countries and the Middle East: Sovereign Strategies**

In Gulf countries, digital resilience is being operationalized through targeted investments, regulatory reforms, and sovereign digital strategies. In Saudi Arabia, digital infrastructure is a pillar of [Vision 2030](#) and a strategic asset for national security and economic diversification. This year, the Kingdom [launched](#) HUMAIN, a state-owned AI company, as part of its broader strategy to become a global AI leader. The company [plans](#) to build a data center with a capacity of 1.9 gigawatts by 2030, expanding to 6.6 gigawatts by 2034, aiming to capture 7% of global AI data processing. These efforts align with Crown Prince Mohammed bin Salman's vision to position Saudi Arabia at the forefront of AI innovation.

The Kingdom has invested billions in telecommunications ([deploying nationwide 5G, investing in fiber](#)), established large-scale data centers, and is implementing data localization for certain sensitive data. These efforts are coordinated through the Ministry of Communications and Information Technology and the National Cybersecurity Authority, which also oversees the Haseen platform, a [national portal](#) for cybersecurity services. Similarly, [Qatar invested](#) USD 1.1 billion in cybersecurity infrastructure around the 2022 FIFA World Cup, building capabilities that remained as a legacy for national resilience. Moreover, Qatar's [National Cybersecurity Strategy 2024-2030](#) was designed to incorporate innovation to protect the country's digital and sovereign assets.

In a similar manner, the United Arab Emirates (UAE) has put cybersecurity and AI development as a digital priority. The country has implemented a National Cybersecurity Strategy promoting [public-private partnerships](#) to counter AI-

enabled threats and build cyber-awareness across sectors, and launched major AI initiatives. This includes a USD 1.5 billion Microsoft investment in Emirati AI firm G42 and plans to massively scale up AI data center capacity, with ambitions to build 10 to 100 times more infrastructure. These efforts are supported by strong government backing, energy resources, and strategic geographic positioning. Together, these measures strengthen the UAE's digital infrastructure resilience by boosting secure computing capacity, reducing dependence on external providers, and ensuring the country can maintain digital operations during times of global disruption.



### **Africa: Bridging the Digital Divide and Building Redundancy**

Across Africa, digital resilience is closely tied to the challenge of bridging the digital divide. While basic access and affordability are often prioritized, recent disruptions highlight the need for built-in resilience. The 2024 internet outage in Africa, caused by damaged underwater fiber optic cables, severely [affecting West African](#) countries like the Ivory Coast, Liberia, Nigeria, and Ghana. The incident's damage extended to banking systems, business operations, public services, and everyday communication, highlighting the fragility of dependence on a small number of international submarine cables and limited domestic redundancy. However, the region is taking steps to address these vulnerabilities through continental frameworks, such as Agenda 2063 and the Digital Transformation Strategy for Africa (2020-2030), which promote infrastructure diversification, improved connectivity, and long-term [digital resilience](#).

Investments in additional submarine cables and inland fiber routes are also underway to improve connectivity and reduce reliance on limited international gateways. For example, the

2Africa cable, expected to become the largest subsea cable system in the world at 45,500km in length. Once operational, it will connect 33 countries across Africa, Europe, and Asia, and is projected to serve over 3 billion people. Beyond its size, a key feature of the project is its focus on landing in underserved coastal and island nations, helping to close the digital divide and improve access in hard-to-reach areas. Led by a consortium of major tech firms and telecom providers, [2Africa](#) is designed to enhance network resilience, reduce latency, and significantly expand internet capacity and affordability across the continent.



### **Latin America: Regulatory Innovation and Supply Diversification**

The Latin American region has experienced various disruptions, from massive data breaches and cyberattacks, such as in Mexico, to [physical outages](#) due to hurricanes in the Caribbean. With that said, the region is gradually advancing digital resilience through regulatory reform and infrastructure diversification. Several countries are strengthening cybersecurity, fostering domestic digital capacity, and reducing foreign technology dependencies. Mexico's [National Cybersecurity Strategy](#) establishes a governance model for cyber threat response and cross-sector coordination. The country also created [CERT-MX](#) (Computer Emergency Response Team), enhancing institutional capacity to prevent and respond to cyberattacks.

Brazil has focused on strengthening its digital resilience through governance and security of its digital ecosystem. To support data localization and sovereignty, Brazil's government has prioritized using national cloud services for public institutions through its ["GovCloud"](#) strategy. The COVID-19 pandemic emphasized Brazil's need for secure and inclusive digital services. The Digital Transformation Strategy ([E-Digital 2022-2026](#))

outlines the need for public policies for digital inclusion such as expanding broadband access, promoting digital inclusion, and strengthening institutional cybersecurity. These measures collectively aim to ensure that Brazil's digital ecosystem can withstand and recover from disruptions. Similarly, Chile's [Digital Transformation Law](#) (2019) mandates public services to be digital by default and includes provisions for digital infrastructure redundancy and system interoperability, thereby embedding resilience in e-government operations.



### **Asia-Pacific: Diverse Paths to Resilience**

The Asia-Pacific region, outside China, is highly diverse, including advanced digital nations (e.g., Japan, South Korea, Singapore), large emerging economies (e.g., India, Indonesia, Vietnam), and small island states (Pacific Islands), each with distinct resilience concerns.

Asia has long been the epicenter of global semiconductor manufacturing. However, growing geopolitical pressures, such as the disruptions in global supply chain following the COVID-19 pandemic and tariffs-driven pressures have led key Asian governments to pursue fabrication diversification strategies to enhance both resilience and competitiveness. TSMC, the world's largest contract chipmaker, has begun building fabrication plants abroad. These moves are not only about geographic diversification but also about mitigating tariff exposure and aligning with host-country industrial policies. Japan has launched an initiative to support domestic production. The Japanese government has provided USD 13 billion for production as well as partnerships with TSMC and the creation of [Rapidus](#), a national foundry aiming at producing domestic advanced chips.

South Korea continues to expand its [K-Semiconductor Belt strategy](#), offering tax incentives and infrastructure support for local production hubs, while India and Singapore are positioning themselves as emerging players with generous subsidies and policy frameworks to attract foreign chipmakers. This regional diversification reflects a broader trend where semiconductor manufacturing is no longer viewed purely through an economic lens, but as a core pillar of national security and technological sovereignty.

A common thread is that many countries have deep integration with global supply chains (either as manufacturers like Vietnam, or consumers like Japan and Australia), and are therefore especially vulnerable to global disruptions.

At the same time, several countries in the Asia-Pacific region are positioned at the intersection of US–China technological competition. Thus, their strategies often aim for resilience through flexibility and balancing multiple partnerships.

Furthermore, natural disasters such as typhoons and earthquakes are also a significant threat in this region, regularly testing the sturdiness of digital and power networks in countries like Japan, the Philippines, and Pacific islands, nations particularly vulnerable to climate change due to their geographic location along the Pacific Ring of Fire and typhoon-prone zones.

These events result in widespread power outages, damage to undersea cables, and disruptions to connectivity and emergency communication systems. In this context, enhancing digital resilience is critical and a tool that is being developed by countries. For instance, Japan has pioneered [disaster technologies](#) that integrate AI and



---

real-time data. Similarly, the Philippines is a key participant of the UN Digital Cooperation and the Government of Japan [DX4Resilience](#) program that focuses on digitizing disaster data and integrating early warning systems. These initiatives ensure digital functionality during and after disasters. As digital technologies become more embedded in disaster response, strengthening digital resilience has become not just a technical priority, but a national and regional security imperative.

## New Framework for Digital Resilience

Governments and international bodies are embedding resilience into trade frameworks. Modern trade agreements now include provisions to enhance supply chain resilience. The Office of the US Trade Representative (USTR) advocates for [trade policies](#) that promote diversified and secure supply chains, encouraging partnerships with allied nations and incorporating resilience clauses.

The Trade and Technology Council (TTC), a collaborative initiative between the EU and the US, serves as a platform to coordinate technology and trade policies. The TTC [focuses](#) on aligning standards, addressing supply chain challenges, and fostering innovation, thereby strengthening transatlantic ties and promoting a resilient digital economy. Nevertheless, the Council's long-term trajectory remains uncertain, as differing views on issues such as regulatory approaches continue to generate tensions between stakeholders on both sides of the Atlantic. This underscores the challenges of sustaining international cooperation in a shifting political environment and highlights the importance of institutional frameworks that can maintain continuity and resilience amid evolving policy priorities.

## Cloud and Data Sovereignty: Local Data Localization Mandates and National Cloud Initiatives

Strategic priorities are being recalibrated to enhance the focus on digital infrastructure, which is increasingly being recognized as essential to national security, economic competitiveness, and societal resilience. As a result, governments around the world are prioritizing data sovereignty and investing in domestic cloud initiatives aimed at reducing dependence on foreign technology providers. By implementing greater control over where and how data is stored and processed, states are not only seeking to protect sensitive information from external threats but also to stimulate local innovation, ensure regulatory autonomy, and bolster digital sovereignty amid evolving geopolitical dynamics.


One of the first jurisdictions that started developing [data localization policies](#) was Russia. The Federal Law on Personal Data, issued in 2006 and [modified](#) in 2014, came into force in 2015. According to this law, companies operating in Russia must collect personal data from individuals residing in the country and Russian citizens. They are also required to store and process that data on servers located within Russia. This law is enforced through a combination of administrative penalties, service bans, and blocking of non-compliant websites. China, meanwhile, has mirrored and expanded upon these strategies with a set of cybersecurity and data governance laws that elevate data sovereignty as a national security imperative.

China has built one of the most comprehensive legal frameworks for digital and data sovereignty. The Cybersecurity Law of 2017 introduced the requirement that [“critical information infrastructure”](#) operators store personal and important data within the country's jurisdiction. This was expanded



through the Data Security Law of 2021 and the [Personal Information Protection Law](#) of 2021 (PIPL, 2021), which requires security assessments for any cross-border data transfers and defines strict compliance obligations for data handlers. These laws collectively assert the state's authority over all forms of digital information deemed relevant to national security or economic stability. While China and Russia have pursued sovereignty through localization and state control, the EU has opted for a values-based approach that emphasizes jurisdictional autonomy and data trustworthiness.

While the [GDPR](#), implemented in 2018, does not impose direct data localization requirements, it has shaped global norms around data governance and privacy. Under GDPR, personal data can only be transferred outside the EU if the receiving country ensures "adequate" levels of data protection. The European Data Strategy (2020) emphasizes the development of "European data spaces" across sectors like health, energy, and finance. These spaces are intended to ensure EU control over critical data infrastructure and promote trusted, interoperable cloud services that align with values of transparency, accountability, and privacy. Initiatives like [GAIA-X](#), led by France and Germany, reflect the EU's ambition to establish a sovereign digital ecosystem that supports innovation while reducing dependency on non-EU cloud providers. The GDPR has inspired several countries to enact policies that encourage data governance and privacy.

 In 2023, India's push for data sovereignty gained momentum with the enactment of the [Digital Personal Data Protection Act](#), which introduces a rights-based framework for data protection and places guardrails on cross-border data flows. The Act allows data transfer to select jurisdictions deemed "trusted," and encourages localization of sensitive personal data, especially data classified as critical by

the government. This shift is supported by broader policy efforts under the [Digital India initiative](#), which seeks to build sovereign digital infrastructure, including cloud platforms like [MeghRaj](#) and a growing network of government data centers. Together, these measures aim to enhance state control over digital assets, reduce reliance on foreign tech companies, and foster local capacity in India's rapidly expanding digital economy.



Saudi Arabia's approach to digital sovereignty is closely aligned with its broader economic transformation goals outlined in [Vision 2030](#), announced in 2016. Recognizing the strategic importance of cloud infrastructure, the government has heavily invested in the development of a domestic cloud ecosystem through the [Saudi Cloud Computing Company](#), a venture from national entities and international tech partners. The cloud computing market in the country is projected to grow by [USD 111.3 billion](#) by 2033. Saudi policies require that government and certain private sector data be hosted locally, reflecting a clear emphasis on self-sufficiency and cybersecurity. These efforts directly strengthen Saudi Arabia's infrastructure and policy resilience by ensuring greater control over critical data flows, reducing reliance on external providers, and enhancing the country's ability to withstand and recover from digital disruptions.

## Labor Market Resilience and Workforce Development Policies

As the digital economy and disruptive emerging technologies continue to reshape labor markets, governments are adopting proactive policies to enhance workforce resilience. The accelerated technological change, driven by AI, automation, and platform-based business models, has led many governments to reassess conventional employment strategies. A World Bank [study](#) indicated that productivity in Latin America and the Caribbean could increase by 8% to 12% by

utilizing generative AI across various sectors. In the same manner, the Anthropic [Economic Index](#) highlights that AI is used more for augmentation (57%) rather than for full automation (43%) of work. These findings underscore a shift in workforce trends, highlighting the need for more technologically-skilled employees.

A central component of these efforts is upskilling and reskilling. Countries like Singapore and Germany have become global leaders in lifelong learning models (see Singapore case study below). Germany, has expanded its [dual vocational training system](#) to include digital competencies, partnering with tech firms and community colleges to deliver short-term certifications in data analysis, AI literacy, and cybersecurity. These programs are not only addressing current skill gaps but also fostering a culture of adaptability in the face of rapid technological change.

#### **Case Study: Singapore's Latest AI-Driven Upskilling and Workforce Resilience Programs**

Singapore's comprehensive upskilling and workforce transformation strategy has been expanded significantly to include AI and emerging technologies. The government has launched several targeted initiatives, which, together, enhance **economic resilience** by equipping the workforce with critical digital and AI competencies, supporting national competitiveness and adaptability in the face of disruption. These include:

- **SkillsFuture Level-Up Programme (2024–2026):** Offers Singaporeans aged 40+ a SGD 4,000 SkillsFuture

Credit. From March 2024, selected full-time course participants are eligible for a training allowance of up to SGD 3,000/month, capped at SGD 72,000 over 24 months.

- **SkillsFuture Workforce Development Grant (2025):** Supports employers by covering up to 70% of job-redesign costs for AI and automation.
- **AI Skilling via IMDA and Partners:** Aims to reskill 18,000 professionals in AI, cloud, analytics, and software engineering.

In parallel, governments are navigating the impacts of widespread technology sector workforce reductions, which have surged since late 2022, particularly across the US and Europe. In response, some states have introduced targeted interventions. For example, the US Department of Labor has expanded the [Trade Adjustment Assistance program](#) to support displaced tech workers, while local governments in states like California [have launched rapid response](#) units to connect laid-off employees with training, mental health support, and In parallel, governments are contending with the aftershocks of large-scale tech layoffs, which have surged since late 2022, particularly in the US and Europe. In response, some states have introduced targeted interventions. For example, the US Department of Labor has expanded the [Trade Adjustment Assistance program](#) to support displaced tech workers, while local governments in states like California [have launched rapid response](#) units to connect laid-off employees with training, mental health support, and reemployment services. In Europe, countries like Ireland and Finland have [deployed public-private transition](#) funds to help high-skilled workers find pathways into growing sectors like clean tech and digital health.

---

Beyond short-term support and training, there is also a growing push to modernize labor regulations to reflect the realities of hybrid work, algorithmic management, and platform-based employment. The EU's [Platform Work Directive](#), first proposed in 2021, aims to clarify employment status for gig workers and ensure algorithmic transparency in work assignments and evaluations. California's [AB5 law](#) (2019) was an early attempt to classify platform workers as employees rather than independent contractors, offering them greater access to benefits and protections. These regulatory frameworks signal a broader trend toward aligning labor law with digital-era realities, balancing innovation with worker security.

Taken together, these policies reflect a growing consensus: future-proofing the workforce requires more than just reacting to economic shocks. It demands long-term investment in human capital, adaptive institutions, and governance mechanisms capable of responding to structural shifts in the way work is organized and rewarded.

## Measuring Digital Resilience: Existing Frameworks and Gaps

As governments implement policies to enhance digital resilience, there is an important question: how to effectively measure progress and identify persistent vulnerabilities? The measurement of digital resilience is still developing, and there is currently no single global index that comprehensively captures infrastructure, economic, and policy resilience in the digital domain. However, several existing indices and frameworks provide partial insights, and organizations are developing tools to assess various components of digital resilience. Some examples are provided below.

- **Digital Economy Navigator (DEN):** The DCO evaluates 50 countries' digital economy maturity, identifies opportunities for growth and benchmark progress. This tool serves to support policymakers to promote economic growth, social inclusion, and a sustainable human-centric approach to digital transformation.
- **Internet Resilience Indices:** The Internet Society's "Internet Resilience Index" (IRI) tracks the robustness of countries' internet ecosystems. The IRI compiles around 30 indicators across four key areas – infrastructure (availability of multiple international links, domestic IXPs, etc.), performance (speed and latency), security (uptake of standards like DNSSEC, route security), and market readiness (competition levels).
- **Cybersecurity and Readiness Indices:** The Global Cybersecurity Index by the International Telecommunication Union (ITU) evaluates countries' cyber capacity across legal, technical, organizational, capacity building, and cooperation measures. It serves as a proxy for readiness to prevent and respond to cyber incidents, a key aspect of resilience.
- **Digital Economy and Society Index (DESI):** The EU's DESI tracks digital development and now integrates into the "Digital Decade" targets, which include goals like 75% of enterprises using cloud/AI by 2030 and all households having gigabit connectivity. Progress toward these goals can be interpreted as reducing dependencies and raising baseline capabilities, thus improving resilience.

---

Despite these efforts, comprehensive measurement of digital resilience remains nascent. Current indices often concentrate on isolated dimensions, such as, technical infrastructure, cybersecurity policy, or over digital adoption without capturing the full spectrum of resilience. Integrated frameworks that evaluate infrastructure robustness, economic interdependencies, and policy effectiveness in tandem are still lacking. For example, a country may rank highly on cybersecurity preparedness due to strong legal and strategic frameworks, yet remain vulnerable due to a physically centralized network architecture, such as reliance on a limited number of cables or providers – a risk not reflected in most cybersecurity indices.

Additionally, there is no standard metric for assessing “digital supply chain diversity” or “level of digital autonomy” within an economy. Some proxies such as the percentage of technology imports or the use of local versus foreign technologies offer some insight, but these are not commonly compiled into an index.

Moreover, there is virtually no index that measures international resilience mechanisms, such as whether a country has agreements with neighbors for mutual support, diversity of routing through multiple countries, and membership in international Computer Emergency Response Team (CERT) collaborations. Considering that digital networks transcend borders, a country-by-country view misses the collective preparedness angle.

While various indicators exist to assess internet robustness and cyber readiness, there is no comprehensive dashboard that offers policymakers an integrated view of overall digital resilience.

---

# 4 Multilateralism Under Pressure: New Alignments and Alliances

---

As national strategies for digital resilience take shape, another critical dimension emerges: the role of regional and global cooperation in enabling sustainable, cross-border resilience. Recent disruptors have [exposed](#) how localized failures can have cascading global effects, interrupting communications, transport, and digital services. These developments underscore the importance of digital resilience as a foundation for national stability and economic well-being. Building this resilience requires coordinated action through common norms, shared standards, and collaborative capabilities, rather than isolated national efforts. In this section, we explore global forums and new alliances shaping digital policy; assess regional digital cooperation and the rising role of digital diplomacy; and analyze multilateral approaches to cybersecurity, data, and AI. Together, these developments shape the frameworks and collective capacities needed to enhance digital resilience across borders.



## 1. Traditional Multilateral Institutions Adapting to Digital Realities

Global policy-shaping entities such as the WTO, OECD, and UN agencies remain key players in shaping digital norms, that underpin global digital resilience. However, they are under mounting pressure to adapt their frameworks to keep pace with technological disruption and emerging risks—even as reform efforts are underway.

The World Trade Organization (WTO)'s journey toward establishing global digital trade rules exemplifies the potential of traditional multilateral institutions in addressing digital disruptions. In July 2024, 91 countries, including the UK and several DCO Member States, signed the first-ever global [WTO E-Commerce Agreement](#). The agreement's provisions for strengthening consumer protection online, facilitating international cybersecurity collaboration, and providing technical support to developing countries demonstrate how traditional multilateral institutions are evolving to address the multifaceted nature of digital disruptions.

As noted by the [UN Economic and Social Commission for Asia and the Pacific \(ESCAP\)](#), while 90 members have drafted some e-commerce provisions, achieving more comprehensive and far-reaching outcomes remains a challenge for the time being. The protracted nature of these negotiations reflects the complex interplay between national interests, technological advancement, and evolving business models that have transformed the global economy. In practice, most digital-trade rulemaking has migrated to smaller forums. [Preferential/regional trade pacts \(RTAs\)](#) now routinely include digital chapters, and ESCAP observes that these RTAs provide “wider, deeper and more comprehensive rules” than

WTO negotiations. In short, multilateral trade institutions are seeking a baseline, but countries are increasingly turning to plurilateral deals to govern areas such as data flows and cross-border e-commerce.

Global digital policy coordination is further supported by other international institutions. The UN has strengthened global digital policy coordination through the Global Digital Compact (GDC), adopted by all 193 Member States in 2025. The GDC [sets shared principles](#) for an open, secure, and human rights-based digital future, emphasizing the need to build digital resilience, especially in developing countries, by scaling connectivity, skills, and inclusive governance.

Likewise, the OECD has published a [Going Digital](#) series emphasizing data as a strategic asset and advocating a holistic, cross-border data governance approach. [OECD](#) notes that data flows underpin economic activity and well-being, but many governments still operate in silos.

Organizations such as the WTO, UN, and OECD continue to lay the foundation for global digital governance, though progress remains gradual. Their role is to convene stakeholders, set guidelines, and help less-advanced countries catch-up even as many concrete rules emerge via smaller coalitions.

### **Case Study: Digital Trade and Resilience: How Standardization Fuels Economic Security and Growth**

The economic implications of multilateral [digital trade initiatives](#) are substantial, with UK government analysis suggesting that adoption of digital trading systems through the WTO E-Commerce Agreement could increase GDP by GBP 2.7 billion to GBP 24.2 billion. This economic

potential underscores why the stakes for multilateral digital governance continue to escalate, as businesses increasingly depend on cross-border digital transactions that require standardized rules and procedures. Inconsistent digital standards not only hinder efficiency but also increase systemic vulnerabilities such as fragmented cybersecurity practices, data incompatibility, and regulatory mismatches that threaten the stability of global trade. By contrast, harmonized frameworks contribute to digital resilience by supporting secure, reliable, and interoperable systems across borders. As such, recognition that digital trade, [estimated by the OECD](#) to be worth approximately USD 5 trillion globally, requires coordinated international frameworks rather than fragmented national approaches.



## **2. Emergence of Alternative Multilateral Frameworks for Digital Resilience**

Beyond traditional institutions, new multilateral alliances are emerging to address digital governance challenges through different approaches and priorities. The BRICS [Digital Economy Partnership Framework](#) represents a key alternative model that acknowledges varying levels of digital development among member nations while focusing on overcoming digital divides and ensuring shared benefits from digitalization. This framework emphasizes the need to leverage digital opportunities for sustainable development while addressing the specific challenges faced by emerging economies in their digital transformation journeys.

The BRICS approach takes a distinct perspective by emphasizing the role of digitalization in advancing industrialization and promoting inclusive economic growth tailored to the



developmental needs of member countries. For instance, at the 2024 Kazan summit, China and Russia presented proposals for a decentralized “[BRICS Pay](#)” platform that would let members trade directly in local or digital currencies, thereby reducing reliance on the US dollar.

Similarly, the Indo-Pacific Economic Framework (IPEF) – launched by the US with 13 partners in 2022 – includes a trade pillar with a digital economy component. US analysts note that IPEF’s digital agenda is “[one of IPEF’s most consequential facets](#).” With the Indo-Pacific region seeing the fastest growth in connectivity and e-commerce globally, IPEF aims to lock in high-standard rules –covering data flows, e-commerce protections, and governance of AI and automation– before alternative models take hold. Negotiations on IPEF’s digital provisions continue, reflecting competing domestic interests; but even without tariff cuts, the framework signals a US-led push for open data and technological co-development in Asia.

Other multilateral forums are rising as well. The G7 and EU have launched [tech councils](#) (e.g. US–EU Trade and Tech Council) to harmonize approaches on AI, semiconductors, and data. The G20 has created the [Digital Economy Task Force](#) to propose policies on data governance and digital inclusion. Meanwhile, the [Quadrilateral Security Dialogue \(QUAD\)](#) comprising the US, Japan, India and Australia, has a Cybersecurity Partnership to align regulations and capacity-building. China’s Belt and Road Initiative (BRI), through its Digital Silk Road, is also shaping digital infrastructure and cybersecurity norms, promoting a model of cyber sovereignty, with at [least 16 countries](#) receiving digital infrastructural investment. These forums allow like-minded states to coordinate standards outside universal bodies. While none of these groups matches the universality of the UN or WTO, their coordination is shaping de facto global digital governance.

In all these club arrangements, however, a tension persists: advanced economies push for free data flows and innovation-friendly rules, whereas developing countries emphasize regulatory sovereignty and equity. The emerging challenge is balancing those priorities across different multilateral tracks. Such multilateral breakthroughs highlight that while slow-moving, global cooperation remains vital for resilience, especially in areas where unilateral or bilateral actions may lead to fragmentation.



### 3. Multilateral Digital Cooperation and Diplomatic Integration

Beyond global alliances, multilateral integration is becoming a key resilience tool, enabling countries to collectively strengthen their defenses against cyber risks and economic fragmentation.

For example, Southeast Asia is negotiating the ASEAN [Digital Economy Framework Agreement \(DEFA\)](#) – the first-ever region-wide, binding agreement devoted exclusively to the digital economy. DEFA is tailored to ASEAN’s mix of mature and emerging digital markets, aiming to harmonize e-commerce rules, ease data transfers, and build trust across borders. The APAC ecosystem further benefits from the [Digital Economy Partnership Agreement \(DEPA\)](#), pioneered by Singapore, Chile, and New Zealand. It sets a new benchmark for cross-border digital trade, digital identities, and interoperability standards, further reinforcing the region’s digital resilience through innovative regulatory cooperation.

In Africa, the African Union’s Continental Free Trade Area (AfCFTA) has similarly adopted a [Digital Trade Protocol](#). This protocol – covering data governance, e-signatures, digital payments, fintech, and inclusion – seeks to create a transparent, trusted digital ecosystem continent-



wide. It mandates electronic document validity, e-invoicing and other measures to facilitate pan-African e-commerce and includes capacity-building provisions.

Regional pacts like ASEAN DEFA, DEPA and AfCFTA's Digital Protocol are concrete examples of countries working together to shore up supply chains and markets against fragmentation.

Moreover, regional coordination can significantly shape global digital standards by influencing outcomes in multilateral forums. The development of the [Global Digital Compact](#) (GDC) through the UN framework exemplifies this dynamic. While the GDC is a multistakeholder and member state-driven process reflecting broad global input, the EU's active engagement – particularly its [advocacy](#) for an open, free, secure, and non-fragmented internet, respect for human rights in digital spaces, and risk-based regulation of AI – demonstrates how regional blocs can help steer the conversation and embed their principles in global agreements. The GDC, adopted by consensus at the UN Summit of the Future, thus stands as the first comprehensive UN framework for internet governance and digital cooperation, illustrating how regional efforts can shape global digital governance standards and, by extension, digital resilience.

Diverse intergovernmental organizations are also starting to take shape – for example, the [DCO](#) has emerged to anchor some of these efforts. Founded in 2020, the DCO now has 16 Member States representing about USD 3.5 trillion GDP and 800 million people. It aims to speed up the inclusive growth of digital economy through multilateral efforts and joint initiatives. In early 2025, the DCO adopted a four-year agenda that strongly emphasizes [digital resilience](#).



## 4. Cybersecurity, Data Standards, AI: Multilateral Tools to Build Resilience

Strengthening digital resilience also requires coordinated global action in key technical domains: cybersecurity, data governance, and AI. As threats increasingly transcend borders, national approaches alone are insufficient. Multilateral frameworks, norms, and capacity-building tools can help countries, particularly those with limited institutional resources, address vulnerabilities and close readiness gaps. In this context, international cooperation becomes a vital enabler of **infrastructure, policy, and economic resilience**.

Below are examples of multilateral initiatives to strengthen cybersecurity. **Cybersecurity** has become one of the most prominent areas of multilateral collaboration. **No country can secure its networks alone:** cyber threats such as malware, ransomware, and infrastructure sabotage move across borders, often targeting shared systems and supply chains.

- The UN and its agencies promote global norms: the 2015 UN [Group of Governmental Experts](#) agreed on 11 norms of responsible state behavior that form a baseline. The ITU provides capacity-building tools for countries. For instance, it offers a cybersecurity thematic [priority program](#) that gives members opportunities and tools to increase cybersecurity capabilities at the national level.
- The ITU also publishes the Global Cybersecurity Index, encouraging governments to meet benchmarks for strategy, institutions, and incident response. The Council of Europe's Budapest Convention (1998) with 67 signatories establishes legal cooperation against cybercrime, enabling even non-European countries to align with tested protocols

---

These initiatives collectively support policy resilience by allowing governments to adopt tested models, build Computer Emergency Response Teams (CERTs), and build public trust through stronger incident response capabilities. In the area of **data governance**, multilateral norms help align divergent rules, lower compliance barriers, and uphold standards that can be adopted by countries with limited regulatory capacity.

**The below efforts enhance both infrastructure and policy resilience**, by enabling safer data sharing across jurisdictions and aligning fragmented regulatory systems around common principles.

- Within the DCO joint standards like the [DCO Privacy Principles](#), the proposed DCO interoperability mechanism for cross-border data flows, and DCO model contractual clauses are aimed at helping countries safely share data across boundaries.
- The OECD and UN have issued voluntary principles (e.g. on open data) that set benchmarks for trustworthy data exchange.
- [The EU's GDPR](#) has become a de facto global standard, leading other regions to adopt comparable privacy laws.

Finally, in **AI governance**, early efforts are taking shape to create shared guidelines that can help mitigate risk, build public trust, and support responsible deployment.

- In 2021, UNESCO Member States adopted a [Recommendation on the Ethics of AI](#), the first global AI governance text to which 194 governments are party, urging transparency, fairness, and human oversight.
- The [OECD AI Principles](#), adopted by 42 countries, call for accountability and human-centered design.
- The DCO adopted its [Principles for Ethical AI \(2025\)](#), providing Member States with a common foundation for AI governance and clear policy guidance focused on human rights protection.
- [The Global Partnership on AI](#) – a coalition of 25+ countries – works on AI best practices, from bias prevention to responsible workforce transition.

These instruments build both economic and policy resilience by enabling governments to participate in global AI development without compromising national values, security, or innovation priorities.

In summary, multilateral and multi-stakeholder tools are proving essential in bridging capacity gaps across cybersecurity, data governance, and AI. Through shared benchmarks, capacity-building, and inclusive rulemaking, countries can leapfrog institutional constraints and enhance digital resilience without duplicating effort. This cooperative model supports national preparedness and a more secure and interoperable global digital ecosystem.

# 5 Conclusion: The Future of Digital Resilience

As we look ahead, digital resilience will continue to be a cornerstone of national security, economic stability, and societal well-being for DCO Member States and countries globally. The evolving digital landscape, characterized by rapid technological advancements and increasing interconnectivity, necessitates a proactive and forward-looking approach to policymaking.



## 1. Strengthening Infrastructure Resilience

Governments globally must prioritize the robustness and continuity of their digital infrastructure. This involves investing in secure networks, enhancing cybersecurity measures, and ensuring the availability of backup systems. By doing so, they can mitigate the risks associated with cyberattacks, natural disasters, and other disruptions. Collaborative efforts to develop regional infrastructure projects, such as cross-border fiber links and satellite broadband constellations, will be crucial in achieving this goal.

### Case Study: Google's Umoja Subsea Cable (2024)

In May 2024, Google unveiled its [Umoja subsea cable](#), a 13,000 km fiber-optic route linking Kenya through multiple African nations to Australia, the first direct connection between Africa and Asia-Pacific.

The cable's terrestrial component connects Kenya to South Africa via Uganda, Rwanda, DRC, Zambia, and Zimbabwe, ensuring robust intra-African connectivity before the undersea segment crosses to Perth. Umoja enhances regional redundancy by offering a path independent of conventional northern routes, safeguarding against previous disruptions when multiple undersea cables were [damaged](#) in early 2024.

In addition to infrastructure benefits, Google complemented the project with a [Statement of Collaboration](#) alongside Kenya's Ministry of Information, focusing on cyber security capacity building, digital skills training, and responsible AI deployment. By improving latency, reducing reliance on singular paths, and linking infrastructure investments to policy and capacity efforts, Umoja exemplifies how private-public partnerships can significantly bolster digital resilience across regions.



## 2. Enhancing Economic Resilience

The diversification and security of digital supply chains are essential for economic resilience. Governments globally should reduce their dependence on single suppliers and technologies by fostering local innovation and establishing strategic partnerships with other regions. Policies that promote the development of domestic semiconductor industries, cloud services, and AI capabilities will be vital. Additionally, supporting small and medium-sized enterprises (SMEs) in adopting digital technologies will help create a more resilient and inclusive digital economy.

### Case Study: Japan's Leading-edge Semiconductor Technology Center (LSTC)

Established in December 2022 with backing from the Ministry of Economy, Trade and Industry (METI), the [LSTC](#) received a substantial USD 300 million grant in 2024 to support next generation chip innovation. This public private research consortium pools resources from academia, government institutes, and industry, reflecting a deliberate policy-led effort to revive Japan's semiconductor sovereignty. In April 2025, LSTC-supported [Rapidus](#) advanced to pilot production in Hokkaido and secured further government funding to scale capacity. This initiative exemplifies how policy can boost local high-tech ecosystems to reduce import dependencies and build long term industrial capacity.



## 3. Adapting and Harmonizing Policy and Governance Frameworks

Policy resilience requires adaptive and flexible governance frameworks that can respond to rapid technological changes and emerging threats. Governments globally should focus on developing regulations that are both robust and adaptable, ensuring they can address new challenges such as AI ethics, data privacy, and cybersecurity. Looking ahead, governments, including DCO Member States, should prioritize forward-looking policy design, using scenario planning and horizon scanning to embed resilience across future digital strategies. International cooperation and alignment on digital policies will also be essential to avoid fragmentation and ensure a cohesive approach to digital governance.

### Case Study: ASEAN Digital Economy Framework Agreement (DEFA)

Currently under negotiation, DEFA aims to align [digital trade rules](#), cybersecurity policies, cross-border e-payments, and e-commerce standards across Southeast Asia, reducing regulatory divergence and bolstering trusted data flows. It builds on earlier frameworks (ASEAN's 2018 E Commerce Agreement and the Regional Comprehensive Economic Partnership) and was endorsed by economic ministers in 2023. The accord is being shaped through broad public and private stakeholder engagement, including thousands of MSMEs, ensuring that its provisions are responsive and inclusive. Once implemented, this common framework will help reduce regulatory fragmentation and boost policy agility.



#### 4. Fostering Multilateral and Regional Cooperation

Digital resilience cannot be achieved in isolation. Governments globally must actively participate in multilateral and regional initiatives to enhance their collective resilience. Engaging in global forums, such as the UN, DCO and the OECD, will help harmonize standards, share best practices, and build joint capabilities. These collaborations will be instrumental in addressing cross-border digital challenges and ensuring a stable and secure digital environment.

##### Case Study: EllaLink – Europe-Latin America Subsea Cable (2021–2024)

In 2021, [EllaLink](#) launched a direct submarine cable connecting Portugal and Brazil – the first new intercontinental route in over two decades. This project was driven by a coalition of European and Brazilian partners, reducing dependence on US and other traditional routes, and strengthening digital sovereignty. It delivers ultra low latency and high-capacity connectivity for critical services such as cloud infrastructure, research data exchange, financial transactions, and emergency communications. EllaLink exemplifies how multilateral cooperation between governments, private sector, and regulators can enhance resilience by securing alternative data pathways, improving network redundancy, and ensuring open digital channels across diverse geopolitical landscapes.



#### 5. Promoting Sustainable and Inclusive Digital Growth

Finally, DCO Member States should strive for sustainable and inclusive digital growth. This involves advancing technological innovation

and ensuring that the benefits of digitalization are equitably distributed. Policies that promote digital literacy, bridge the digital divide, and protect vulnerable populations will be key. By fostering a digital economy that is both resilient and inclusive, DCO Member States can build a future where technology serves as a force for good, driving digital prosperity for all.

##### Case Study: Tech Herfrica (Nigeria)

In Nigeria, [Tech Herfrica](#) has emerged as a trailblazing initiative enhancing digital resilience by promoting sustainable and inclusive digital growth among rural women. Since launching in early 2023, the NGO has reached over 4,000 women across six states through programs like EquipHer4Growth (digital literacy training) and HerLocal Market (market linkage support). Participants receive smartphones, financial education, and training in digital payments and e-commerce. As a result, average incomes increased by approximately 50%, indicating a direct economic uplift alongside enhanced digital capability. Herfrica exemplifies how targeted inclusion efforts can build trust in digital tools, strengthen local economies, and bolster resilience by integrating vulnerable communities into the digital ecosystem.

In conclusion, the path to digital resilience for DCO Member States lies in a holistic and forward-looking approach that integrates robust infrastructure, diversified economies, adaptive policies, multilateral cooperation, and inclusive growth. By embracing these principles, DCO Member States can navigate the complexities of the digital age and build a resilient and prosperous future.

## Document Disclaimer

The following legal disclaimer (“Disclaimer”) applies to this document (“Document”) and by accessing or using the Document, you (“User” or “Reader”) acknowledge and agree to be bound by this Disclaimer. If you do not agree to this Disclaimer, please refrain from using the Document.

This Document, prepared by the Digital Cooperation Organization (DCO). While reasonable efforts have been made to ensure accuracy and relevance of the information provided, the DCO makes no representation or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability or availability of the information contained in this Document.

The information provided in this Document is intended for general informational purposes only and should not be considered as professional advice. The DCO disclaims any liability for any actions taken or not taken based on the information provided in this Document.

The DCO reserves the right to update, modify or remove content from this Document without prior notice. The publication of this Document does not create a consultant-client relationship between the DCO and the User.

The designations employed in this Document of the material on any map do not imply the expression of any opinion whatsoever on the part of the DCO concerning the legal status of any country, territory, city, or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

The use of this Document is solely at the User’s own risk. Under no circumstances shall the DCO be liable for any loss, damage, including but not limited to, direct or indirect or consequential loss or damage, or any loss whatsoever arising from the use of this Document.

Unless expressly stated otherwise, the findings, interpretations and conclusions expressed in this Document do not necessarily represent the views of the DCO. The User shall not reproduce any content of this Document without obtaining the DCO’s consent or shall provide a reference to the DCO’s information in all cases.

By accessing and using this Document, the Reader acknowledges and agrees to the terms of this Disclaimer, which is subject to change without notice, and any updates will be effective upon posting.



Follow us on



[www.dco.org](http://www.dco.org)