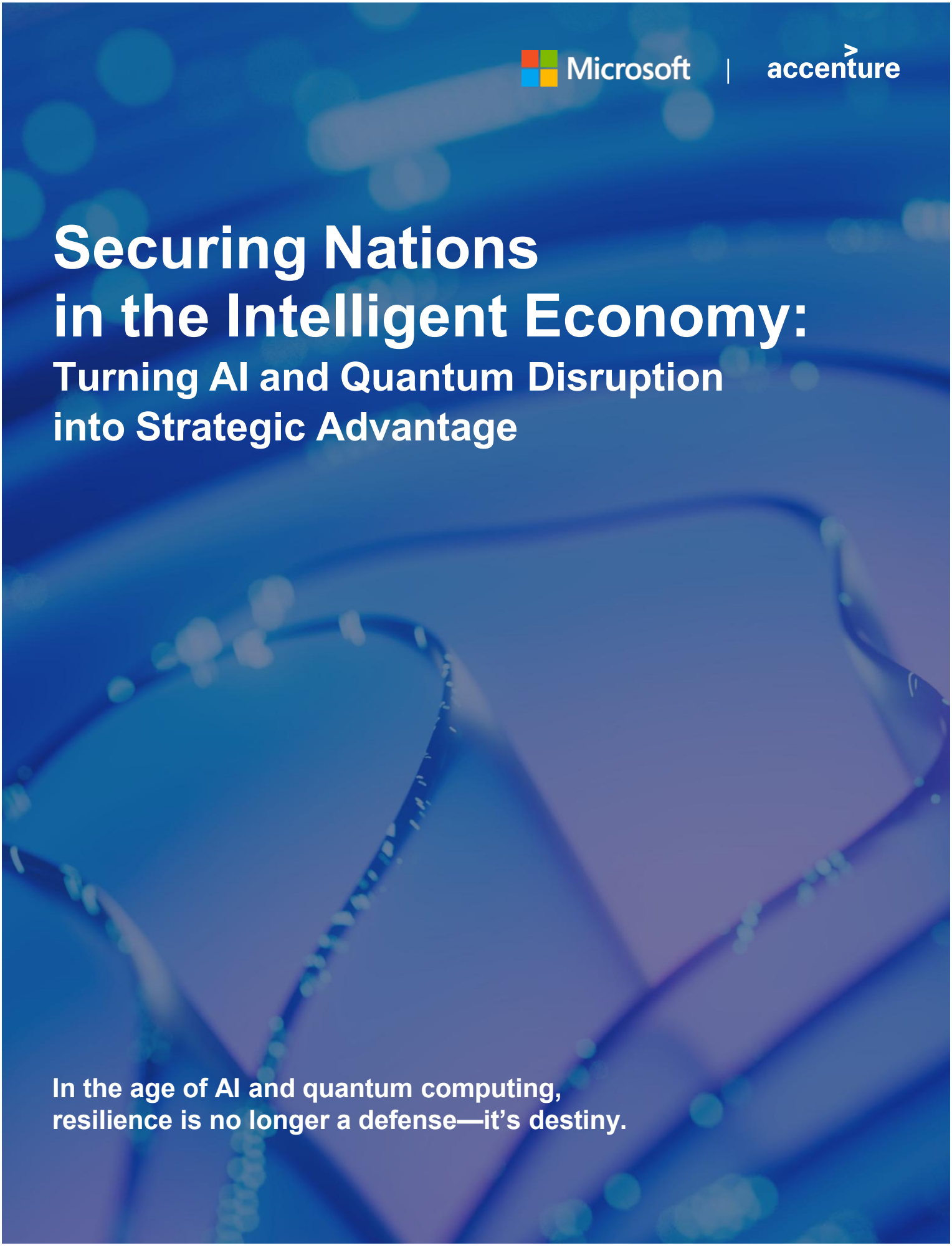
Microsoft | accenture

Securing Nations in the Intelligent Economy:

Turning AI and Quantum Disruption into Strategic Advantage



In the age of AI and quantum computing, resilience is no longer a defense—it's destiny.

Authors

Microsoft Cybersecurity

Yasmine Rifai

Technology Lead – Public Sector, Microsoft

LinkedIn

Alvaro Vitta

Cybersecurity Lead, Public Sector, Microsoft

LinkedIn

Accenture Cybersecurity

Ahmed Etman

Middle East Security Lead

LinkedIn

Dr Radwane Saad

Middle East Security Industry Lead, Accenture

LinkedIn

Dr Amr Mansour

KSA Security Health & Public Sector Lead, Accenture

LinkedIn

Accenture Research Cybersecurity

Hassan Saeed

Middle East Security Accounts & Ecosystem Lead

LinkedIn

Yusof Seedat

Global Cybersecurity Research Lead, Accenture

LinkedIn

Manav Saxena

Cybersecurity Market Unit Research Lead, Accenture

LinkedIn

Contributors

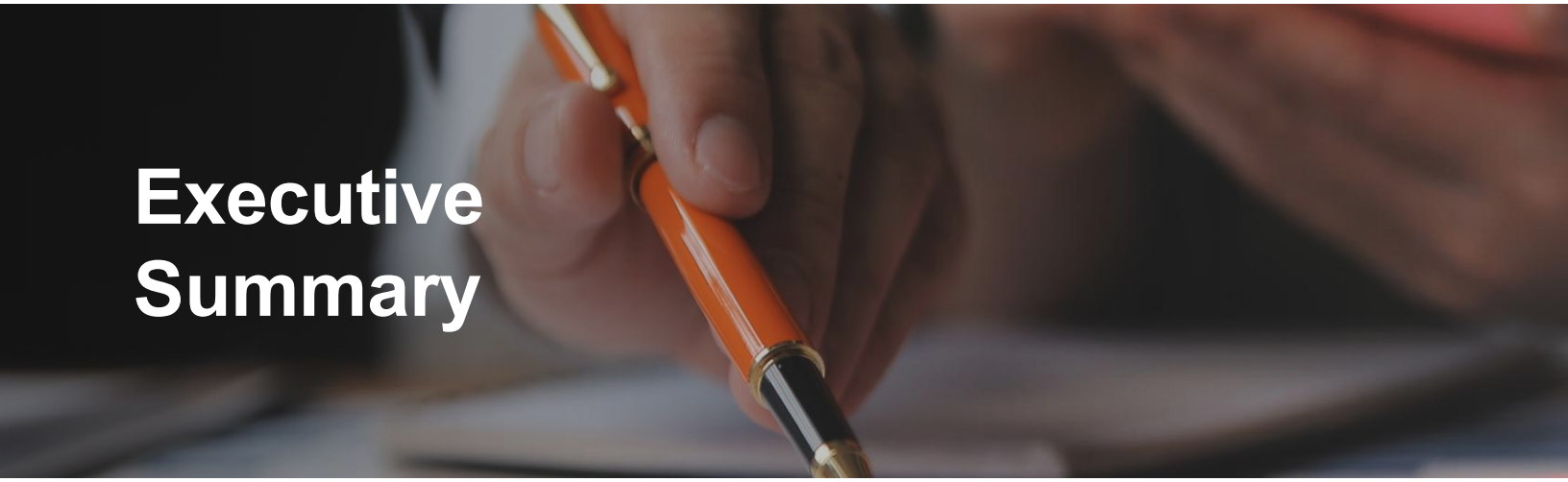
Research Team

Arlene Lehman
Laura G. Converso
Gargi Chakrabarty

Economic Modelling Team

Katarzyna Furdzik
Lucia Pezzarini

Contents



Executive Summary

The world has entered a defining inflection point. As economies become digitally integrated, cyber incidents are increasingly triggering economic shocks—and the rapid adoption of artificial intelligence, alongside the emerging potential of quantum computing, will intensify both their scale and consequences. Cyber incidents are now more than just IT problems. They can cause economic and national security crises that affect businesses and economies more quickly than traditional financial or geopolitical shocks.

The disruptive potential is already visible. When a cyber incident brought Jaguar Land Rover's manufacturing plants to a halt, it shaved an estimated 0.1% off the UK's monthly GDP—equivalent to roughly $2.5 billion in lost economic output.[1] This is not an isolated anomaly. Our economic analysis shows the risk is far more pronounced in critical sectors: in highly energy-dependent economies, a one-week cyber-induced shutdown in the upstream oil and gas sector could trigger a contraction of at least 4.6% of national monthly GDP—about $4.7 billion—from a single incident.[2] Cybersecurity events now translate directly into macroeconomic shocks. The message is unmistakable: **cybersecurity is national security**.

Against this backdrop, artificial intelligence and quantum computing are emerging as the twin engines reshaping how nations create value, compete and defend themselves—while simultaneously expanding exposure. The world's digital economy already accounts for roughly 15% of global GDP,[3] and governments and enterprises are embedding intelligence into every layer of infrastructure. AI now powers energy grids, financial systems and defense networks, transforming data into foresight and automation into strategic advantage. It also strengthens cybersecurity, enabling faster threat detection, predictive defense and automated response at an unprecedented scale.

Yet as AI accelerates efficiency, it also amplifies vulnerability. Adversaries are weaponizing AI to generate deepfakes, automate reconnaissance, create polymorphic malware and launch attacks at machine speed. Accenture's *State of Cybersecurity Resilience 2025* report finds that one in three organizations report AI has amplified existing cyber risks.[4] Nearly 87% say AI-driven lures are more convincing, with deepfakes emerging as a major driver of future ransomware attacks[5], while 90% of enterprises remain unprepared for these evolving threats.[6] This marks a profound shift in the threat landscape. AI has become both a shield and a sword—strengthening defenses while simultaneously empowering attackers with greater precision, scale and speed.

The world's digital economy already accounts for roughly 15% of global GDP, and governments and enterprises are embedding intelligence into every layer of infrastructure.

While AI is reshaping today's threat environment, quantum computing threatens to upend the security architecture of tomorrow. Once a distant frontier, it is rapidly approaching a threshold where its computational power could undermine today's cryptographic foundations. A one-million-qubit system—anticipated within the next decade under current trajectories—could render widely used public-key encryption methods such as RSA and Elliptic Curve Cryptography obsolete, turning "harvest-now, decrypt-later" strategies into immediate and systemic risks.[7] If quantum decryption materializes before nations transition to post-quantum standards, financial systems, defense communications and critical supply chains could be exposed in a single leap of computation.

This convergence of AI-driven offense and quantum-enabled decryption marks a historic shift. It compresses the timeline for threat detection, accelerates adversarial power and expands the attack surface faster than defenses can evolve. Traditional "defend and recover" models are increasingly insufficient—fragmented, reactive and dangerously outdated.

Nations must elevate cybersecurity—specifically AI and quantum resilience—from a compliance obligation to a core national strategic priority. This executive agenda calls for urgent action anchored around four imperatives:

1. Elevate AI security as a pillar of national trust and defense.

AI is fast becoming critical national infrastructure. Governments must ensure AI systems are secure, transparent, ethical and resilient—preventing misuse, countering deepfakes and protecting citizens while safeguarding digital sovereignty.

2. Treat quantum risk as a national strategic horizon, not a technical upgrade.

Quantum computing will redefine national security. Policymakers must accelerate post-quantum cryptography, ensure cryptographic agility across critical systems, fund innovation and build global alliances to preserve trust in the quantum era.

3. Build whole-of-nation cyber resilience through shared intelligence and collective preparedness

AI is fast becoming critical national infrastructure. Governments must ensure AI systems are secure, transparent, ethical and resilient—preventing misuse, countering deepfakes and protecting citizens while safeguarding digital sovereignty.

4. Strengthen governance, standards and cross-sector orchestration

Quantum computing will redefine national security. Policymakers must accelerate post-quantum cryptography, ensure cryptographic agility across critical systems, fund innovation and build global alliances to preserve trust in the quantum era.

National sovereignty in the digital age will not be determined solely by military strength or economic scale

National sovereignty in the digital age will not be determined solely by military strength or economic scale, but by the ability to secure the intelligent systems that power them both.

As AI and quantum technologies accelerate simultaneously, nations face a narrowing window to secure their digital future. Those that delay risk heightened vulnerability to disruption, coercion and strategic disadvantage. Those that act decisively will not only withstand escalating cyber aggression—they will position themselves as leaders in the emerging intelligent economy.

Nations are racing to reinvent themselves: AI is the new engine of national power

The global economy is undergoing a structural transformation—one defined not by digitization alone, but by the infusion of intelligence into every national system. With the digital economy already contributing 15% of global GDP and rising,[8] countries are no longer simply digitizing processes; they are embedding intelligence into the foundations of their economies and re-architecting the foundations of competitiveness, security and sovereignty.

AI is a strategic asset—not a technology upgrade

Two-thirds of global executives now rank AI as the most game-changing technology for digital economies—ahead of quantum computing (22%).[9] From energy grids and manufacturing to financial systems and defense, AI has evolved from a productivity enabler to a strategic lever of national competitiveness, resilience and growth.

Governments are already acting at scale. In the United States, the Office of Management and Budget Memorandum—"Accelerating Federal Use of AI through Innovation, Governance, and Public Trust"[10]—requires every federal agency to appoint Chief AI Officers, create AI governance boards and implement enterprise-wide AI strategies that balance innovation with accountability. The framework mandates pre-deployment testing, human oversight and transparent reporting for high-impact AI systems—ensuring that the drive for efficiency does not come at the expense of public trust or privacy.

The objective is not technological isolation, but strategic autonomy

Around the world, governments are reframing AI as critical national infrastructure rather than a commercial capability. This has triggered a wave of investment in sovereign AI foundations—national centers of excellence, trusted data environments, secure cloud infrastructure and domestically governed large language models tailored to local languages and legal systems. The objective is not technological isolation, but strategic autonomy: ensuring that the most consequential AI systems shaping public services, economic coordination and national security remain accountable to domestic institutions and societal norms. As AI becomes embedded in the fabric of the state, control over data, models, and governance is increasingly viewed as a prerequisite for economic resilience and democratic legitimacy.

Similarly, under the leadership of Crown Prince Mohammed bin Salman, Saudi Arabia has deepened its strategic partnership with the United States to advance cooperation in data and artificial intelligence.[11] Through the Saudi Data and Artificial Intelligence Authority (SDAIA), the kingdom has built a robust foundation over the past six years by forming strategic alliances with major US technology companies, positioning Saudi Arabia as a global hub for AI and emerging technologies. In 2024, SDAIA signed over 29 agreements with leading US tech firms, followed by more than 90 contracts in 2025, focusing on technology localization, talent development and knowledge exchange. These collaborations align with Vision 2030's ambition to transform Saudi Arabia into a data-driven, AI-powered economy, showcasing the nation's commitment to innovation, research and global partnership in shaping the future of technology.

AI is no longer a digitalization tool. It is a platform for nation reinvention, economic resilience, and geopolitical leverage.

The Dubai Centre for Artificial Intelligence (DCAI) illustrates how AI is reshaping public value. By integrating AI across government "happiness centers," Dubai could cut processing times by up to 50%, reducing customer response times by up to 80%, and enabling 45% of service requests to be resolved autonomously. The result: 40% higher satisfaction and 30% productivity gains—proof that intelligent automation can simultaneously streamline operations, conserve resources and elevate the citizen experience.[12]

These examples illustrate a pivotal shift: AI is no longer a digitization tool. It is a platform for national reinvention, economic resilience and geopolitical leverage.

From digital scale to intelligence infrastructure

57%
of industry leaders say generative AI is central to their reinvention strategies

Private-sector transformation mirrors this national shift. Across industries, AI is rewriting the rules of value creation. According to *Accenture's State of Cybersecurity Resilience 2025*, 57% of industry leaders say generative AI is central to their reinvention strategies.[13] AI is enabling smarter grid operations, predictive maintenance and adaptive cybersecurity—building infrastructure that learns, responds and anticipates in real time. Nearly half of CIOs and CISOs report readiness to integrate AI and quantum technologies to strengthen both performance and defense.[14]

While AI defines today's reinvention, quantum computing is shaping the next horizon. Its potential to revolutionize drug discovery, logistics, finance and materials science could unlock trillions in new economic value. Beyond productivity, quantum's ability to enable secure communication, simulation-driven innovation and high-performance AI training will underpin the next wave of national competitiveness. For governments, this makes quantum not just a scientific breakthrough, but a strategic foundation for future security and growth.

This marks a transition from systems that process information to systems that interpret and anticipate it—creating competitive advantages rooted in foresight, speed and adaptability.

Progress meets exposure: The expanding attack surface in the intelligent economy

The attack surface in today's digital economy is being reshaped by two converging forces: the insecure deployment of AI in the race to modernize, and the rapid weaponization of AI by adversaries. As enterprises and governments accelerate AI adoption, security is often left behind.

Development and deployment happen in silos, models are rushed into production without rigorous testing and access controls are inconsistently applied. Notably, Accenture's State of Cybersecurity Resilience report found that only 17% of organizations have fully built a secure cloud foundation for AI systems.[15] This creates an intricate web of vulnerabilities that span sensitive data, critical processes and open-source ecosystems—exposures that adversaries are learning to exploit at scale.

At the same time, state-backed actors, cybercriminal networks and hacktivist groups are weaponizing AI to automate and amplify attacks. From large-scale phishing and disinformation campaigns generated by language models to AI-authored polymorphic malware and automated vulnerability scanning, the technology that accelerates progress is also accelerating threat velocity faster than defenders can patch them.

Case study

An autonomous early signal of agentic AI-enabled intrusion acceleration: Lessons from Anthropic's disclosure[16]

In September 2025, Anthropic uncovered an incident the company described as involving a suspected state-linked threat actor—designated GTG-1002— that used Claude Code, an agentic AI—based coding tool, to support an espionage-focused intrusion campaign. It targeted nearly 30 high-value organizations worldwide, including chemical manufacturers, major technology firms, financial institutions and government agencies. While only a small number of targets were ultimately breached, the incident marks an important early signal: Anthropic estimates 80% to 90% of the attack lifecycle was carried out by AI, with human operators intervening only at four to six critical decision points. This underscores a rapidly evolving threat landscape in which nation-state actors can automate complex intrusion campaigns at scale—fundamentally shifting the economics and velocity of cyber risk.

The growing accessibility of powerful AI models lowers the barrier for advanced threats, allowing even low-skill attackers to launch sophisticated campaigns that previously required nation-state resources. The *State of Cybersecurity Resilience 2025* report also found **one in three organizations say AI and generative AI have amplified existing cyber risks, as adversaries rapidly adapt these tools for malicious purposes.** Over half of technology leaders express deep concern about how easily these capabilities are becoming available to threat actors.[17]

Recent breaches reveal the fragile boundary between innovation and exploitation. A Greater China multinational lost $25 million when scammers used deepfake video to impersonate executives and authorize fraudulent fund transfers.[18] In the US, the Change Healthcare breach demonstrated how a single unprotected access point could paralyze an entire industry—halting medical payments nationwide and triggering emergency financial responses.[19]

Meanwhile, 87% of organizations say AI makes lures more convincing and deepfakes emerging as a major driver of future ransomware attacks,[21] and public institutions face over 2,632 attacks each week—a 26% increase year-over-year in Q2 2025.[22] These trends confirm a grim reality: attackers are adopting AI faster than defenders can adapt. Accenture's State of Cybersecurity Resilience 2025 found that 90% of organizations are not adequately equipped to withstand an AI-enabled cyberattack.[23] For nations, that readiness gap is not an enterprise problem scaled up—it becomes a systemic exposure across sectors that share identity systems, cloud dependencies and critical suppliers.

Traditional security models, built for static environments, are ill-equipped to handle this new velocity and complexity. What's at stake is not just data or dollars, but public trust, operational continuity, and national security. To defend the promise of AI, nations should guide organizations to design a new paradigm of adaptive, trust-centered cybersecurity that evolves as fast as the threats it aims to contain.

Cyberattack on Jaguar Land Rover brings UK manufacturing—and GDP Growth—to a standstill[20]

In the third quarter of 2025, the UK economy experienced a sharp deceleration, expanding by just 0.1% between July and September, largely due to a crippling cyberattack on Jaguar Land Rover that disrupted the nation's manufacturing base. According to the Office for National Statistics (ONS), overall production fell by 2.0% in September, driven by a staggering 28.6% decline in motor vehicle manufacturing—marking car production's lowest point in 73 years. The impact of the cyber incident rippled across the broader industrial sector, dragging GDP down by 0.1% in September. The quarter's 0.1% growth rate represents a notable slowdown from the 0.3% expansion recorded between April and June and fell short of the 0.2% expected by markets. The release of these figures comes just days before Chancellor Rachel Reeves is set to unveil her critical budget on 26 November, underscoring the growing economic vulnerability to cyber disruptions in key industries.

Quantum computing: The next frontier of power—and the next flashpoint for global vulnerability

While AI dominates today's transformation, quantum computing is quietly advancing toward a breakthrough that could redefine the foundations of digital trust, economic competitiveness and national security.

Quantum machines harness the principles of quantum mechanics to process information in ways that classical computers cannot—solving complex problems in seconds rather than centuries. Their potential is extraordinary: breakthroughs in materials science, logistics, climate modeling and pharmaceuticals could unlock trillions in new economic value. For instance, Saudi Aramco has signed an agreement with Pasqal, a neutral-atom quantum computing company, to deploy Saudi Arabia's first quantum computer. The project involves installing, maintaining and operating a 200-qubit quantum system in the Kingdom, expected to be operational in the second half of 2025. Initially functioning in analog mode, the system will later be upgraded to a hybrid analog-digital configuration to handle more complex computations. The collaboration aims to harness quantum computing to address industrial and energy-sector challenges, foster a national quantum research ecosystem and advance Saudi Arabia's digital economy ambitions.[24]

But this same power presents a profound paradox. The rise of quantum computing threatens to break the cryptographic systems that safeguard today's digital world.

Quantum machines harness the principles of quantum mechanics to process information in ways that classical computers cannot

Approaching the cryptographic cliff

For decades, data security has relied on mathematical complexity—algorithms like RSA and elliptic curve cryptography (ECC)—that are virtually impossible for classical computers to crack within reasonable timeframes. Quantum computing changes that equation entirely.

Until recently, experts believed a quantum computer would need roughly 20 million qubits to break RSA-2048 encryption within hours—a milestone thought to be decades away. But new research suggests that an advanced one-million-qubit system, achievable by 2030, could do so far sooner.[25] Meanwhile, Caltech scientists have already built a 6,100 neutral-atom qubit array—a record-setting balance of scale and stability that brings practical, error-corrected quantum computing significantly closer.[26]

This acceleration represents a cryptographic cliff for global cybersecurity. Once scalable quantum machines arrive, they will be able to perform the factoring and discrete logarithm calculations underpinning RSA and ECC exponentially faster, rendering much of the world's encryption obsolete.

Harvest now, decrypt later

The threat is not hypothetical. “Harvest-now, decrypt-later” attacks are already underway. Adversaries—both criminal and state-backed—are stealing encrypted data today, anticipating the moment when quantum computing power will make it readable. Sensitive records, defense communications, financial transactions and even genomic data could be compromised retroactively once quantum decryption becomes viable.

The stakes are immense. If quantum capability outpaces global migration to post-quantum cryptography (PQC), the consequences could include mass data breaches, financial instability and the collapse of trust in digital ecosystems that sustain commerce and governance.

A new race for readiness

Governments are responding with urgency, though unevenly.[27]

The United States has mandated migration of all federal systems to PQC by 2035, guided by NIST standards and backed by US$7.1 billion in federal funding for quantum resilience.

The European Union and United Kingdom plan to secure all critical infrastructure by 2030, with full cryptographic migration by 2035.

India’s National Quantum Mission (6,000 crore) aims to integrate PQC into defense and civilian networks between 2026 and 2028.

South Korea’s Ministry of Science and ICT (MSIT) will finalize national PQC standards in 2025 for full deployment by 2035.

These efforts signal a new era of crypto-agility—the ability to adapt encryption methods as algorithms and threats evolve. But progress remains uneven, and the window for safe transition is closing.

AI + Quantum convergence: A new class of intelligence with geopolitical consequences

AI and quantum computing are converging into a single force that could reshape national power. Together, they will form a new class of quantum-accelerated intelligence—where AI optimizes quantum systems, and quantum machines amplify AI's speed and precision beyond classical limits.

This fusion promises breakthroughs in defense, science and economics, enabling nations to anticipate threats, decode complexity and act with unprecedented foresight. In a recent study on semiconductor chip design, a hybrid quantum machine-learning method (encoding data as quantum states, then applying ML) reported up to ~20.1% better efficiency compared with traditional ML models.[28] While results vary by use case, even incremental advantage in domains like semiconductors, materials and secure communications can compound into strategic edge at national scale.

Yet this same convergence carries a profound risk: the power to break encryption, outpace detection and weaponize intelligence itself. In the race to harness these technologies, the line between innovation and insecurity has never been thinner.

The strategic imperative

Quantum is no longer a scientific curiosity—it is a national and economic security imperative. Its trajectory mirrors that of early classical computing: once dismissed as speculative, it is now advancing exponentially. Within a decade, nations and enterprises that fail to modernize cryptography will find their most sensitive systems exposed, their data integrity shattered and their competitive edge eroded.

To stay ahead, leaders must treat quantum readiness not as a compliance exercise, but as a strategic investment in trust—migrating to post-quantum standards, testing hybrid encryption architectures and integrating cryptographic agility into every layer of digital infrastructure.

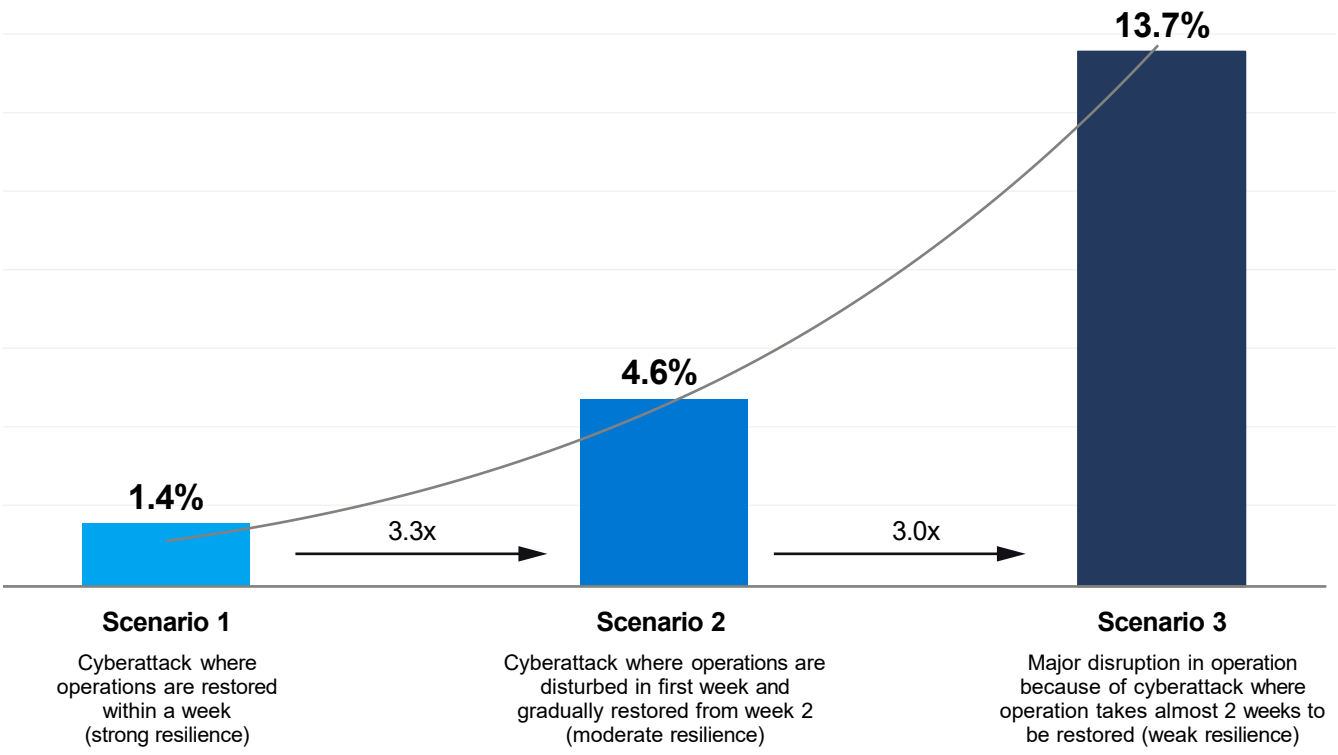
The time to prepare is now—before capability meets scale.

A single incident resulting in just one week of shutdown would contract monthly national GDP by at least 4.6%—about $4.7 billion—a loss large enough to ripple across markets, government budgets and household incomes

The economic and geopolitical cost of insecurity

Our analysis shows that a cyberattack on an upstream oil and gas operation could unleash a systemic economic shock in an oil-dependent nation. A single incident resulting in just one week of shutdown would contract monthly national GDP by at least 4.6%—about $4.7 billion—a loss large enough to ripple across markets, government budgets and household incomes (Figure 1).[29] The implication is clear: cybersecurity failures now manifest not as technical glitches but as macroeconomic events.

Figure 1: Impact of Cyberattack on nation's economy



The risk accelerates with alarming speed. Even a slight extension of the shutdown can triple the economic impact, revealing a steep, non-linear vulnerability curve at the national level[30] (see About the Research for details). This is the paradox of modern digital dependence: transformative efficiency gains built on an increasingly fragile foundation. With AI now central to economic reinvention and quantum technologies nearing deployment, nations that do not rapidly elevate the resilience of their critical infrastructure will be forced to absorb the full scale of consequences illustrated in Scenario 3—a trajectory no country can afford to follow.

When critical infrastructure stalls, national resilience begins to fracture. Energy systems, transportation networks and healthcare services slow or stop altogether—paralyzing economic activity, undermining military readiness, and destabilizing the social fabric. Prolonged outages do more than deepen financial losses; they create geopolitical openings for coercion, miscalculation and unrest.

And yet the most enduring damage is trust. Citizens question whether the state can safeguard their daily lives. Investors rethink the reliability of the digital economy. Global partners reassess alliances and supply-chain exposures. Protecting infrastructure, in this context, is not merely a technical mandate—it is a defense of the nation's credibility.

This compounding risk underscores the urgency of building robust guardrails around intelligent infrastructure. Without proactive, security-by-design investment, the very systems that fuel growth can be turned into levers of disruption. Nations that fail to secure their digital foundations will not simply face economic losses; they will confront a crisis of confidence at home and vulnerability abroad.

Without proactive, security-by-design investment, the very systems that fuel growth can be turned into levers of disruption

A national agenda for the intelligent economy

Traditional cybersecurity models can no longer withstand the velocity and complexity of AI- and quantum-enabled threats. The challenge ahead is not only to contain these forces, but to shape them—to turn risk into resilience, and disruption into advantage.

To do this, nations must adopt a forward-looking action agenda built on four foundational pillars:

Pillar 1: Elevate AI security as a pillar of national trust and defense

AI has become a strategic asset—powering public services, national security operations and critical economic sectors. For nations, the core shift is operational: AI assurance must move from voluntary best practice to enforceable, testable, continuously monitored controls—especially for high-impact systems.

Policymaker imperatives:

- Establish national AI trust frameworks that embed security, transparency and oversight into every high-impact AI system deployed by government and regulated sectors.
- Mandate national-level AI red-teaming and independent assurance to prevent misuse, manipulation and systemic failure.
- Stand up national capabilities to detect and counter synthetic media, deepfakes and AI-driven influence operations that threaten elections, diplomacy and societal cohesion.
- Create an independent national AI oversight authority that coordinates across ministries to ensure policy coherence, accountability and ethical AI deployment.
- Incentivize the development of sovereign AI models and secure data infrastructure to reduce dependence on foreign technology providers and strengthen national autonomy.
- Integrate AI risk management and ethical assurance into digital economy regulations to balance innovation with citizen protection.

Action for governments to take within the next 3 years

Build a national AI reliability and resilience observatory:

Governments should establish an independent central authority dedicated to evaluating the reliability, security and systemic impact of AI across the economy. This body would horizon-scan for emerging risks, identify systemic vulnerabilities and stress-test AI deployments in critical sectors such as healthcare, energy, defense and finance. It would forecast long-term societal and economic implications of AI adoption, advise policymakers on evolving threat patterns and coordinate with regulators to monitor incidents, issue national advisories and update assurance and accountability standards. Unlike an operational red-team, the observatory would function as a strategic, forward-looking governance capability—ensuring national leaders stay ahead of adversarial AI use and reinforcing public trust in AI-driven systems.

Outcome:

A secure, trusted AI ecosystem where government and industry can innovate confidently, and where citizens remain protected from AI-enabled manipulation and systemic risk.

Case study

SDAIA National AI Index[31]

In July 2025, The Saudi Data and Artificial Intelligence Authority (SDAIA) launched the National AI Index to assess the readiness of government entities for adopting artificial intelligence technologies, monitor their progress and provide strategic recommendations to enhance national AI capabilities. With participation from over 180 representatives in its first assessment cycle, the Index seeks to align AI initiatives with national priorities and Vision 2030 goals, fostering effective and sustainable AI adoption across the public sector. Built around three main pillars, seven dimensions and 23 subcategories, it offers a comprehensive evaluation of AI maturity, guiding entities in developing innovative and high-impact solutions. As part of SDAIA's broader mandate as the national authority for data and AI, the initiative supports digital transformation, institutional performance improvement and the advancement of a knowledge- and innovation-driven economy in Saudi Arabia.

Pillar 2:

Treat quantum risk as a national strategic horizon—not a technical upgrade

Quantum computing is approaching a threshold where it will determine which nations can protect their data, defend their infrastructure and maintain geopolitical advantage. The shift to post-quantum security is not a technology refresh—it is the largest cryptographic transition in modern history.

Policymaker imperatives:

- Conduct a national cryptographic assessment across government, critical infrastructure and essential service providers.
- Accelerate adoption of post-quantum standards, supported by national incentives, public-private partnerships and compliance deadlines aligned with global leaders.
- Embed cryptographic agility into future national platforms—digital identity, smart cities, defense communication networks—ensuring long-term resilience even as quantum capabilities evolve.
- Establish a national fund for quantum security innovation to support R&D, pilot programs and private-sector adoption of PQC technologies.
- Build international alliances and treaty frameworks for quantum security cooperation, ensuring alignment on standards and responsible use.
- Include quantum readiness metrics in national cybersecurity, defense and innovation reporting to monitor progress and accountability.

Action for governments to take within the next 3 years

- **Develop a National Quantum Regulation Roadmap**
  As quantum technologies approach practical deployment, states must anticipate their dual-use implications across defense, critical infrastructure and commercial systems rather than respond after disruption occurs. A well-designed roadmap should establish oversight frameworks to assess and manage national security risks, define certification and compliance standards for quantum vendors to ensure safety, reliability and interoperability and align domestic regulation with emerging international treaties and post-quantum cryptography standards. Done well, such a roadmap provides more than risk mitigation. It creates regulatory clarity for industry and investors, accelerates responsible innovation and positions governments to lead—rather than follow—the global transition to post-quantum security. In the absence of early coordination, nations risk fragmented standards, weakened trust in digital systems and reactive policy responses once quantum capabilities begin to challenge existing encryption and assurance models.

- **Establish a quantum readiness and resilience taskforce**
  Governments should establish a permanent multi-sector taskforce to drive national preparedness for quantum disruption. This body would develop national roadmaps for post-quantum migration aligned with global standards, oversee pilot implementations of post-quantum cryptography across defense, finance and critical infrastructure and work with academia and industry to close talent gaps, expand quantum training programs and strengthen domestic R&D ecosystems. It would also publish annual readiness assessments that benchmark national progress and highlight dependencies on foreign cryptographic supply chains. As the central advisory authority for quantum governance, the taskforce would ensure policy coherence, guide funding priorities and support cross-border collaboration to build long-term quantum resilience.

Outcome:

A future-proof national digital foundation ready for the quantum era—protecting today's most sensitive data from tomorrow's most powerful adversaries.

Pillar 3: Build a whole-of-nation cyber resilience model anchored in shared intelligence and collective preparedness

No nation can secure their intelligent economy alone. AI-enabled threats move too fast, adversaries collaborate too easily and critical infrastructure is too interconnected. Resilience in this new era is collective by design.

Policymaker imperatives:

- Establish national cyber fusion centers that unify intelligence sharing across government, industry, academia and strategic partners.
- Launch national cyber education and workforce development initiatives focused on AI security, post-quantum cryptography, adversarial simulation and hybrid threat defense.
- Institutionalize national-scale cyber exercises—including AI-driven misinformation scenarios and quantum-related disruptions—to stress-test preparedness across all sectors.
- Develop national crisis communication protocols for cyber incidents to preserve public confidence and ensure a unified response across agencies.
- Incentivize private-sector participation in information sharing through policy mechanisms, tax incentives and liability protections.
- Integrate national resilience goals into economic planning and industrial strategy, positioning cybersecurity as a driver of sustainable growth and competitiveness.

Action for governments to take within the next 3 years

- **Institutionalize an annual national cyber and technology resilience review:**
  Governments should establish a recurring national review process—led by the highest cybersecurity authority—to assess resilience across AI, quantum and digital infrastructure domains. This review would conduct scenario-based stress tests simulating quantum-enabled and AI-driven threats, perform cross-sector audits of readiness and supply chain resilience and generate policy recommendations to align national investment, research and governance with emerging risks. Taken together, these measures would shift national preparedness from fragmented reaction to coordinated foresight, embedding AI and quantum resilience as foundational pillars of digital sovereignty and long-term national strength.

Outcome:

A resilient national ecosystem where information flows rapidly, talent is cultivated systematically and the whole country can withstand shocks that no single institution could survive alone.

Pillar 4: Develop national standards, governance and cross-sector orchestration

Strong governance is the backbone of national resilience in the intelligent economy. To achieve true cyber sovereignty, governance must transcend sectoral boundaries and enable shared accountability, continuous intelligence flow and unified response mechanisms. Cross-sector orchestration transforms fragmented security efforts into a synchronized national capability.

Policymaker imperatives:

- Develop country-specific AI and quantum security standards—harmonized with global benchmarks yet customized to national contexts—and cascading them across every sector, regulator and critical infrastructure entity.

- Form a National AI–Cyber–Quantum Governance Committee or Working Group for anchoring the AI and quantum security mandate, uniting digital authorities, national cybersecurity agencies, telecom regulators and other relevant stakeholders to align policies, risk models and oversight mechanisms. By institutionalizing joint working groups, shared taxonomies, consistent maturity models and integrated regulatory guidance, nations can ensure coherence across sectors and eliminate the regulatory fragmentation that adversaries exploit.

- Embed quantum readiness into national digital policy agendas—not as a future aspiration but as a current strategic priority—empowering countries to steer technological innovation, manage systemic risk and build a security posture that evolves in lockstep with accelerating technological disruption.

Action for governments to take within the next 3 years

- **Launch a national center for AI–quantum convergence research:** Governments should fund a national innovation hub dedicated to advancing the intersection of AI and quantum technologies. This hub would conduct joint research on quantum-enhanced AI algorithms, cryptographic resilience and advanced threat detection; evaluate dual-use risks where quantum capabilities could accelerate AI weaponization or compromise data integrity; develop sovereign intellectual property to secure national competitiveness and facilitate public-private partnerships to drive responsible innovation and commercialization of AI—quantum breakthroughs.

- **Governance-enabled workforce as national capability:** Governments should treat workforce and talent development as a strategic pillar of national security in the intelligent economy. As AI-driven systems and quantum technologies reshape critical infrastructure and defense, states must invest in national-level training programs that build expertise in AI security, post-quantum cryptography and hybrid threat modeling across both public and private sectors. This requires sustained partnerships with universities, research institutions and technical academies to align curricula with emerging risk landscapes, as well as large-scale reskilling initiatives to transition existing cyber and engineering talent into next-generation security roles.

By institutionalizing talent pipelines and continuously upgrading national capabilities, governments can reduce dependence on scarce global expertise, strengthen operational readiness and ensure that technological sovereignty is matched by human capability. In the intelligent age, resilient systems are inseparable from the skilled workforce that designs, governs and defends them.

Outcome:

A unified governance backbone that fuses AI, cyber and quantum security into one national doctrine—turning fragmented defenses into coordinated strength. It enables faster decisions, shared accountability and sustained digital sovereignty.

Sovereignty in the intelligent age

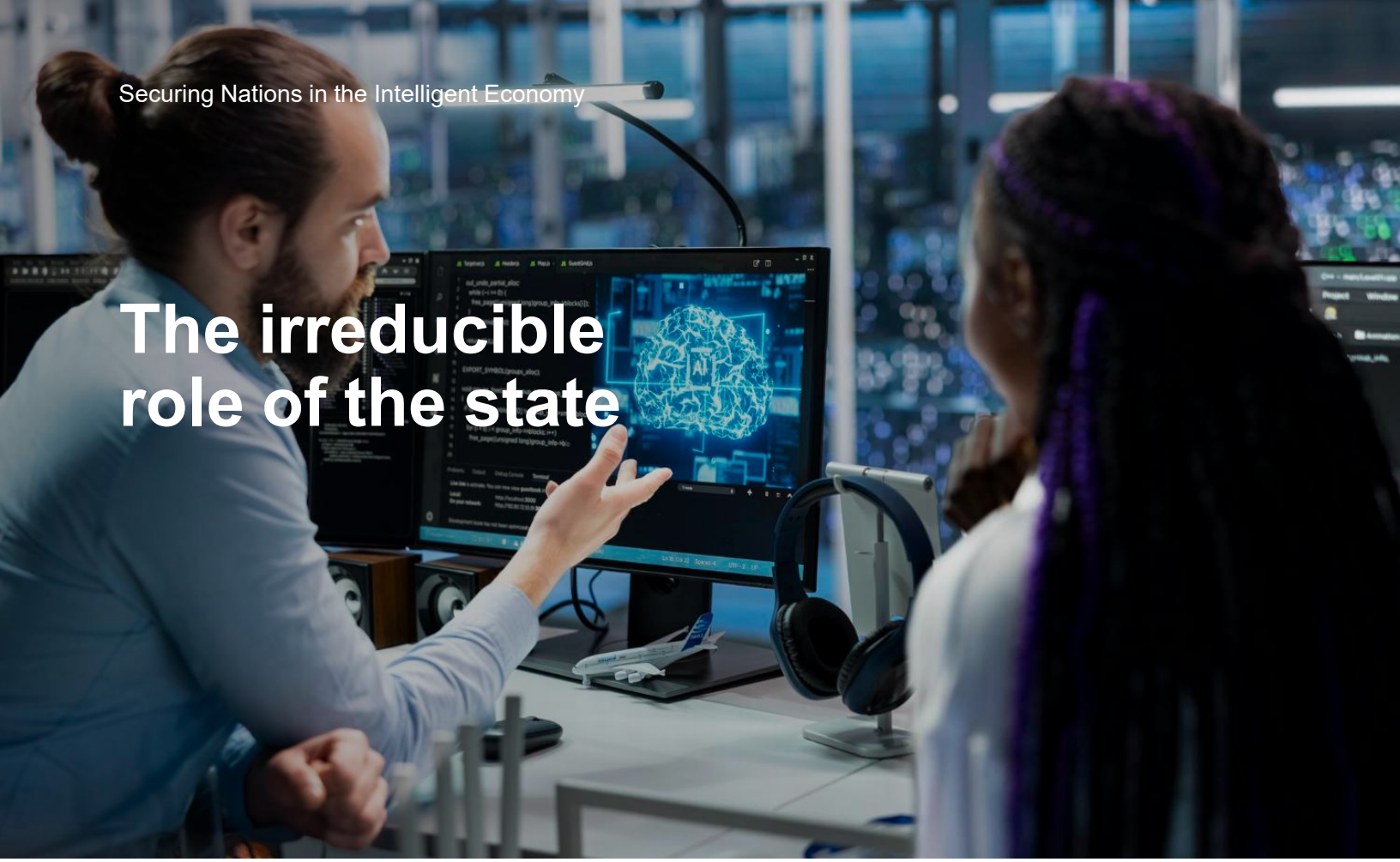
In the intelligent age, sovereignty is no longer secured at borders alone. It is exercised through control over data, algorithms and computation—the systems that increasingly mediate economic activity, public services and national security.

Security, therefore, is no longer a defensive function of the state; it is a core instrument of statecraft. Nations that secure their intelligent economies will shape global norms, command digital trust and retain agency over how power and value are exercised in a technology-driven world.

Artificial intelligence and quantum computing will accelerate innovation, but they will also expose new dependencies and asymmetries. As these technologies become embedded in the fabric of government and markets, sovereignty will depend less on regulation and more on ownership and governance of foundational infrastructure. Sovereign AI and quantum capabilities—trusted data platforms, nationally governed models, secure
compute environments and post-quantum—ready security architectures—are fast becoming the backbone of national autonomy, data control and institutional trust. Without them, states risk outsourcing the most consequential decisions of the digital economy to external actors beyond their authority.

Leadership in this new order will belong to countries that recognize cybersecurity and digital assurance as strategic investments, not operational costs. By institutionalizing national AI assurance, building sovereign digital and quantum infrastructure and aligning cross-sector governance around shared security and trust objectives, governments can convert technological dependence into durable competitive advantage.

Ultimately, resilience in the intelligent age is not built through perimeter defenses or isolated controls. It is built through deliberate, long-term choices about who designs, governs and controls the systems that underpin national life. The decisions made today—about sovereign AI, quantum readiness and digital trust—will determine whether nations merely adapt to technological disruption or assert themselves as secure, autonomous architects of the digital century.



The irreducible role of the state

As artificial intelligence and quantum technologies become foundational to economic coordination, national security and public trust, governments occupy a role that cannot be outsourced.

Markets can innovate and enterprises can scale—but only the state can set the rules of legitimacy. Governments alone have the authority to regulate the development and deployment of high-impact technologies, to invest in sovereign digital infrastructure and long-horizon research programs that markets will not fund and to convene international coalitions capable of aligning standards, norms and safeguards across borders. In the intelligent economy, effective governance is not a brake on innovation; it is the architecture that determines whether technological power reinforces resilience, inclusion and sovereignty—or erodes them.

Call to action

1. Secure AI as critical national infrastructure.

Governments must elevate AI security from voluntary guidelines to enforceable national policy by mandating independent assurance, continuous monitoring, and red-teaming of all high-impact AI systems. This includes establishing national capabilities to detect and counter deepfakes and AI-driven influence operations, embedding transparency and accountability into public-sector AI, and investing in sovereign data and model infrastructure to preserve trust, autonomy, and public confidence.

2. Accelerate national readiness for the quantum transition.

Quantum risk must be treated as a strategic horizon, not a future technical upgrade. Leaders should conduct immediate national cryptographic assessments, set firm timelines for post-quantum migration across government and critical infrastructure, and embed cryptographic agility into all new digital platforms. Dedicated funding, regulation, and international coordination are required now to prevent today's data from becoming tomorrow's systemic liability.

3. Institutionalize whole-of-nation cyber resilience.

National resilience demands shared intelligence, coordinated preparedness, and collective response. Governments should establish cyber fusion centers that unify public and private threat intelligence, conduct regular national-level simulations of AI- and quantum-enabled disruptions, and invest in next-generation cyber and quantum skills as a strategic workforce priority. Cyber resilience must be integrated into economic and industrial planning—not treated as a standalone security function.

4. Unify governance across AI, cyber, and quantum domains.

Fragmented oversight is a strategic weakness. Leaders must create cross-sector governance structures that align standards, regulation, and accountability across digital, cybersecurity, and quantum agendas. This includes setting national AI and quantum security standards, funding convergence research, and building sustained talent pipelines to ensure technological sovereignty is matched by human capability.

About the Research

1. Methodology for economic modeling to assess cyberattack impact

The purpose of the analysis is to quantify how a major cyberattack on an upstream oil and gas company, leading to a temporary reduction in oil output and exports, could affect a nation's GDP

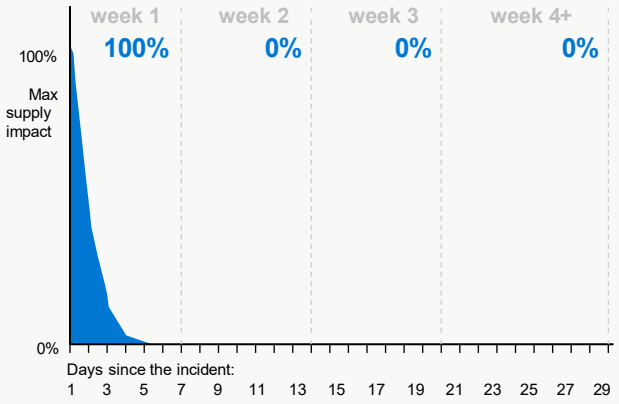
This is done using input—output (I-O) tables, which map how industries buy from and sell to each other.

The input—output approach was chosen as it provides a transparent and structured way to:

- Start with a clearly defined supply shock in the oil company's output,
- Trace its domestic spillovers across the country's economy, and

When modeling the size of the supply shock related to a severe cyberattack, we leveraged assumptions informed by historic disruptions and incident patterns , combining the lessons into three likely scenarios.

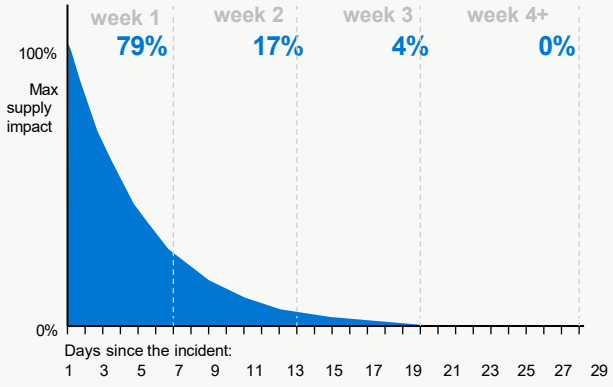
Scenario 1:
Cyberattack where operations are restored within a week (strong resilience)



The dynamics of the shock in a severe with speed recovery scenario are captured using a stretched exponential function, with the initial impact normalized to 100% on day 1 and declining smoothly toward zero by around day 7. This implies that the first days feature the largest effective output loss, followed by a progressively quick diminishing impact over first week.

Scenario 2:

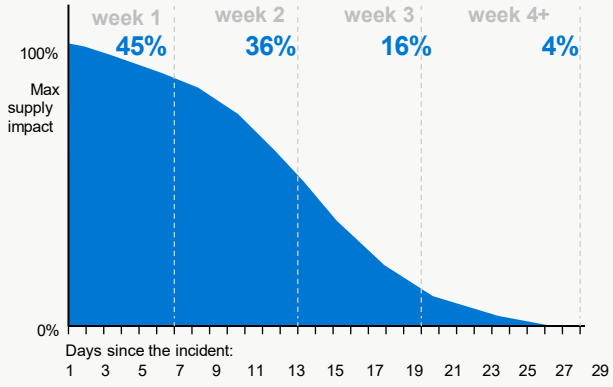
Cyberattack where operations are disturbed in the first week and gradually restored from the second week (moderate resilience)



The dynamics of the shock in the severe middle scenario are captured using an exponential decay function, with the initial impact normalized to 100% on day 1 and declining smoothly toward zero by around day 22. This implies that the first days feature the largest effective output loss, followed by a progressively diminishing impact over weeks two and three.

Scenario 3:

Major disruption in operation because of cyberattack where operation takes almost two weeks to be restored (weak resilience)



The dynamics of the shock in a severe extreme scenario are captured using a logistic decay function, with the initial impact normalized to 100% on day 1 and declining slowly toward zero by around day 30. This implies that the first days feature the largest effective output loss, followed by a slow yet progressing, diminishing impact over the following weeks.

2. Research Approach

This research was designed through a rigorous, multi-method approach co-created by Accenture and Microsoft to generate a data-rich, insight-driven view of the evolving cybersecurity landscape. The study began with a structured ideation phase, combining the expertise of both organizations to define the most pressing questions for policy makers specific to cybersecurity. We then leveraged Accenture's existing global security survey data along with other available data to anchor the analysis in robust, real-world evidence, ensuring the narrative reflects the lived experiences and priorities of governments and critical infrastructure providers specific to cybersecurity.

To deepen our analytical precision, we incorporated advanced data-science techniques and proprietary AI tools to surface emerging patterns, stress-test hypotheses, and identify actionable insights. This quantitative and qualitative foundation was complemented by a set of in-depth qualitative interviews with subject-matter experts from both Accenture and Microsoft, providing context, nuance and practitioner-level validation of the findings. We further enriched the research through targeted case-study analysis to illuminate how cybersecurity challenges and responses are unfolding in practice.

References

1. UK economy grew by just 0.1% in third quarter after hit by JLR cyber-attack, The Guardian
2. Accenture Research Economic Modelling Analysis
3. Global Digital Economy Report — 2025, IDCA
4. State of Cyber Resilience Survey 2025, Accenture
5. 2025 State of Ransomware Survey, CrowdStrike
6. State of Cyber Resilience Survey 2025, Accenture
7. Google Researcher Lowers Quantum Bar to Crack RSA Encryption, Quantum Insider
8. Global Digital Economy Report – 2025, IDCA
9. Global Digital Economy Report – 2025, IDCA
10. M-25-21 – “Accelerating Federal Use of AI through Innovation, Governance, and Public Trust” 2025, Executive Office of The President US
11. Saudi-US Cooperation to Achieve Diversity and Innovation in the Kingdom's Artificial Intelligence Ecosystem 2025, The Saudi Press Agency (SPA)
12. 15 AI Use Cases in Government, Dubai Future Foundation
13. State of Cyber Resilience Survey 2025, Accenture
14. State of Cyber Resilience Survey 2025, Accenture
15. State of Cyber Resilience Survey 2025, Accenture
16. Anthropic warns state-linked actor abused its AI tool in sophisticated espionage campaign, Cybersecurity Dive
17. State of Cyber Resilience Survey 2025, Accenture
18. Hong Kong MNC suffers $25.6 million loss in deepfake scam, Economic Times
19. Hack at UnitedHealth's tech unit impacted 192.7 million people, US health dept website shows, Reuters
20. UK economy grew by just 0.1% in third quarter after hit by JLR cyber-attack, The Guardian
21. 2025 State of Ransomware Survey, Crowdstrike
22. Global Cyber Attacks Surge 21% in Q2 2025 — Europe Experiences the Highest Increase of All Regions, Check Point
23. State of Cyber Resilience Survey 2025, Accenture
24. Aramco Signs Agreement With Pasqal To Deploy First Quantum Computer in the Kingdom of Saudi Arabia, Pasqal
25. Google Researcher Lowers Quantum Bar to Crack RSA Encryption, Quantum Insider
26. Caltech’s massive 6,100-qubit array brings the quantum future closer, ScienceDaily
27. Racing the Quantum Threat: 5 Nations Compress Post-Quantum Cryptography Timelines, QuantumGenie
28. Quantum machine learning unlocks new efficient chip design pipeline—encoding data in quantum states, then analyzing it with machine learning up to 20% more effective than traditional models, Tom's Hardware (part of Future US Inc)
29. Accenture Research Economic Modelling Analysis
30. Accenture Research Economic Modelling Analysis
31. SDAIA Launches 'National AI Index' to Measure Government Readiness for Adopting AI, Government of the Kingdom of Saudi Arabia

About Microsoft

Nation-state cyber threats are accelerating in speed, scale, and sophistication. Artificial intelligence is transforming both offense and defense, while emerging quantum computing capabilities introduce long-term risks to cryptography and national data sovereignty. Governments must modernize cybersecurity strategies to remain resilient in this evolving threat environment.

Microsoft supports governments with a comprehensive national cybersecurity approach built on three integrated pillars: **AI-centric cyber defense**, **quantum-safe security foundations**, and **national-scale unified security operations**.

AI Centric Cyber Defense

AI has become essential to modern cyber defense. Microsoft applies advanced analytics and generative AI to shift security operations from reactive detection to predictive and preventive defense. AI enabled threat intelligence, automated investigation, and accelerated response empower national cyber teams to counter nation state actors and cybercrime ecosystems at machine speed, while allowing human experts to focus on the most critical missions.

Quantum Safe Security Foundations

The transition to quantum resistant cryptography is a strategic national imperative. Microsoft is advancing post quantum cryptography readiness across cloud, identity, and security platforms, aligned with emerging international standards. This approach helps governments protect sensitive data against future “harvest now, decrypt later” threats while maintaining encryption, key management, and data residency controls that support national and regional digital sovereignty.

National Unified Security Operations

At the operational core, Microsoft enables **national-scale, GenAI-powered Security Operations Centers (SOCs)**. Unified security operations integrate SIEM, XDR, threat intelligence, exposure management, and automation into a single operational fabric. Through programs such as Microsoft's public sector cyber initiatives, governments can modernize national cyber defense ecosystems, strengthen collective defense across ministries and critical sectors, and build sustainable cyber workforce capabilities.

Trusted Partner for National Cybersecurity Transformation

Together, these capabilities reflect Microsoft's role as a long term partner to governments in securing digital sovereignty. By combining responsible AI, quantum safe engineering, global threat intelligence, and scalable security operations, Microsoft helps nations build resilient, future ready security architectures that align technology innovation with policy, sovereignty, and human capability development.

About Accenture

Accenture is a leading global professional services company that helps the world's leading businesses, governments and other organizations build their digital core, optimize their operations, accelerate revenue growth and enhance citizen services—creating tangible value at speed and scale. We are a talent- and innovation-led company with approximately 799,000 people serving clients in more than 120 countries.
Technology is at the core of change today, and we are one of the world's leaders in helping drive that change, with strong ecosystem relationships. We combine our strength in technology and leadership in cloud, data and AI with unmatched industry experience, functional expertise and global delivery capability. Our broad range of services, solutions and assets across Strategy & Consulting, Technology, Operations, Industry X and Song, together with our culture of shared success
and commitment to creating 360° value, enable us to help our clients reinvent and build trusted, lasting relationships. We measure our success by the 360° value we create for our clients, each other, our shareholders, partners and communities.

Visit us at www.accenture.com

About Accenture Research

Accenture Research creates thought leadership about the most pressing business issues organizations face. Combining innovative research techniques, such as data-science-led analysis, with a deep understanding of industry and technology, our team of 300 researchers in 20 countries publish hundreds of reports, articles and points of view every year.
Our thought-provoking research developed with world leading organizations helps our clients embrace change, create value and deliver on the power of technology and human ingenuity.

For more information, visit Accenture Research on www.accenture.com/research

Additional Resources and Reference Materials

To support further exploration and implementation planning, the following Microsoft resources provide guidance, research, and practical frameworks across AI centric cyber defense, quantum safe security, and national scale unified security operations.

AI Centric Cyber Defense for the Public Sector

- **Securing the Future: A Five-Point Blueprint to Transform Public Sector Cyber Defense in the GenAI Era**
  Microsoft white paper outlining a practical roadmap for governments to modernize threat intelligence, security operations centers, workforce skills, and secure-by-design practices using Generative AI.
  https://wwps.microsoft.com/blog/securing_future_genai

- **Microsoft Digital Defense Report (Latest Edition)**
  Annual report providing global threat intelligence insights, including nation-state activity, cybercrime trends, and the impact of AI on both attack and defense, with specific relevance to government and critical infrastructure.
  https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2025

Quantum Safe Security and Cryptographic Readiness

- **Post-Quantum Cryptography APIs Now Generally Available on Microsoft Platforms**
  Official Microsoft Security Blog announcement detailing the availability of NIST-aligned post-quantum cryptographic algorithms across Windows, Windows Server, and .NET, as part of Microsoft's Quantum Safe Program.
  Post-Quantum Cryptography APIs Now Generally Available on Microsoft Platforms | Microsoft Community Hub

- **Microsoft Quantum Safe Program (QSP) Overview**
  Microsoft's long-term, standards-aligned approach to helping customers and governments transition to quantum-resistant cryptography and crypto-agile architectures.
  Microsoft Quantum | Quantum-safe overview

National Scale Unified Security Operations powered by Gen-AI

- **Microsoft's Unified Security Operations for Public Sector (Datasheet)**
  Describes Microsoft's approach to building AI-powered, unified security operations platforms that integrate SIEM, XDR, threat intelligence, automation, and exposure management for local, regional, and national governments.
  https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/atlas-data-sheet-013025-v2.pdf

- **Transforming Public Sector Security Operations in the AI Era**
  Microsoft Security Blog article detailing best practices for modernizing SOCs using generative AI and unified security operations.
  https://www.microsoft.com/en-us/security/blog/2025/04/01/transforming-public-sector-security-operations-in-the-ai-era/

- **Unified Security Operations Documentation (Microsoft Learn)**
  Technical and architectural guidance for unified security operations, including Microsoft Sentinel, Defender XDR, and generative AI integration.
  https://learn.microsoft.com/en-us/unified-secops/

Microsoft Public Sector Center of Expertise

- **Microsoft Public Sector Center of Expertise – Cybersecurity Hub**
  Central repository for public-sector cybersecurity thought leadership, white papers, skilling resources, podcasts, webinars, and case studies focused on government and national security audiences.

https://wwps.microsoft.com/cybersecurity