WORLD
GOVERNMENTS
SUMMIT 2026

REPORT

Harnessing Artificial Intelligence to Build Whole-Of-Society Resilience: A Blueprint for Governments of the Future

in collaboration with

pwc

To Inspire and Enable **The Next Generation of Governments**

The World Governments Summit is a global platform dedicated to shaping the future of governments worldwide. Each year, the Summit sets the agenda for the next generation of governments with a focus on how they can harness innovation and technology to solve universal challenges facing humanity.

The World Governments Summit is a knowledge exchange center at the intersection of government, futurism, technology, and innovation. It functions as a thought-leadership platform and networking hub for policymakers, experts, and pioneers in human development.

The Summit is a gateway to the future as it functions as the stage for analysis of future trends, concerns, and opportunities facing humanity. It is also an arena to showcase innovations, best practice, and smart solutions to inspire creativity to tackle these future challenges.

Contents

Introduction

Introduction

"The question is not whether AI will influence international peace and security, but how we will shape that influence. Used responsibly, AI can strengthen prevention and protection...But without guardrails, it can also be weaponized."

António Guterres,
UN Secretary-General, September 2025[1]

Governments today face an unprecedented range of shocks, from climate-driven disasters, global pandemics, and supply chain disruptions, to cyber threats, inflationary pressures, and geopolitical volatility. The frequency, intensity, and interconnectedness of these crises are stretching traditional models of national resilience to the breaking point.[2] Fragmented, reactive approaches are no longer sufficient. Whole-of-society resilience is now required, which embeds the collective capacity to anticipate, absorb, recover, and adapt at the core of government, governance, and public sector service delivery.

Artificial intelligence (AI) is indispensable to achieving this transformation. Its potential extends far beyond improving crisis response to enabling governments to strengthen trust, transparency, evidence-based policy, and decision-making. At the same time, AI can expand the operational capacity of ministries, agencies, and local authorities across the entire resilience lifecycle: namely, anticipate, assess, plan, prepare, detect, respond, recover, and adapt.[3]

Yet, despite these advances, deploying AI at scale carries challenges that cannot be ignored. Issues of governance, accountability, equity, interoperability, and the need for robust fail-safe mechanisms across national and regional boundaries must be addressed to ensure that AI strengthens resilience responsibly, ethically, and inclusively.[4]

At the heart of these challenges is the fact that AI can now analyze complex problems and propose solutions exponentially faster than humans. In crisis scenarios such as natural disasters, where failures can cascade in minutes across multiple domains, including health, infrastructure, finance, and public trust, there is a risk that AI will take control of decision-making, with no human monitoring or power to override the technology. Governments must include safeguards in all AI-enabled resilience systems to ensure that human agency remains paramount.

This report analyzes how governments can balance rapidly evolving AI innovations with the implementation of robust safeguards to shift resilience policies from fragmented reactive responses and toward secure, proactive, and adaptive whole-of-society capacity-building. It proposes a blueprint for how current and future governments can harness AI responsibly to modernize government institutions, public services, and national resilience systems, balancing innovation with governance, accountability, and equity.

This report highlights how the emergence, since late 2024, of a new generation of AI architectures called Hierarchical Reasoning Models (HRMs) is opening up new vistas for building proactive whole-of-society resilience. In contrast to traditional Large Language Models (LLMs), HRMs can generate intermediate reasoning steps, refine solutions iteratively, and learn from the quality of reasoning processes rather than merely from the correctness of outcomes.

The advent of HRMs illustrates the sheer speed of AI's evolution, with potentially transformative innovations sometimes moving from the pilot phase to full implementation in less than a year. Governments risk failing to exploit the full potential of HRMs in building whole-of-society resilience by remaining dependent on less advanced AI architectures. Yet they must also conduct rigorous, fully informed due diligence to avoid unintended governance and ethical consequences.

The selected national case studies in this report are intended to provide evidence of how a wide range of countries are developing AI-enabled resilience systems. They include Abu Dhabi, in the United Arab Emirates (UAE), which aims to become the world's first AI-native government by 2027; Singapore, whose "Digital Twin Nation" project incorporates virtual resilience-testing scenarios; and Australia, which has implemented an AI-enabled emergency management ecosystem. These are early days. None of these ambitious AI projects has been 'completed' in traditional terms, partly because the technologies are innovative, and, more importantly, because the latest AI architectures are essentially proactive, learning from past mistakes to anticipate new scenarios and responses.

The case studies thus demonstrate that AI-enabled resilience will always be a work in progress. Furthermore, while the selected countries illustrate common AI resilience design principles, the spectrum of highlighted projects and countries—from the United States' (US) defense planning to Estonia's 'X-Road' program – also demonstrates why there is no 'one-size-fits-all' model for building AI-driven whole-of-society resilience. Each model must be adapted to fit a country's political and socio-economic context.

Governments must also be well informed about current research on AI-enabled resilience (see box: Relevant Current Research For Governments) and draw on past experiences of resilience building since 1945 (see box: Evolution Of National Resilience Systems Since 1945).

The rationale for investing in AI is not only about enhancing security and stability. It is also about ensuring economic competitiveness. Global indices and econometrics demonstrate a positive correlation between resilience and GDP growth per capita.[5]

Countries that recover faster from crises are better able to protect economic activity, sustain investor confidence, and strengthen long-term competitiveness.[6]

China, the US, the European Union (EU), and Gulf Cooperation Council (GCC) region governments are investing heavily in scaling AI for national security, infrastructure, economic development, and crisis.[7] Those that delay adoption risk falling behind, in a world where exogenous shocks will increasingly impact national trajectories.

AI Resilience: Relevant Current Research For Governments

Resilience scholarship has progressed from narrow, reactive disaster management paradigms toward comprehensive whole-of-society approaches that emphasize proactive adaptation, multi-level coordination, and transformative capacity.[8]

Andrew G. McClelland et al. demonstrate that contemporary whole-of-society resilience requires synchronization between formal governmental structures and informal community initiatives, while Andreas Duit argues that resilient public administration systems must comprise networked, non-hierarchical arrangements with cross-scale linkages rather than traditional bureaucratic hierarchies.[9] This conceptual shift creates opportunities for AI to serve as an enabling technology for whole-of-society preparedness.

AI applications are fundamentally transforming governmental capacity across multiple domains. Anneke Zuiderwijk, Yu-Chen, and Fadi Salem identify AI's role in enabling service delivery portfolios and governance orchestration functions, while David Valle-Cruz et al. demonstrate how AI facilitates dynamic, data-driven policy cycles from agenda-setting through evaluation.[10] Rony Medaglia, J. Ramon Gil-Garcia, and Theresa A. Pardo emphasize that realizing AI's potential requires novel governance frameworks for coordinating adoption across government entities, including regulatory mechanisms for algorithmic systems.[11] Bernd W. Wirtz, Jan C. Weyerer, and Carolin Geyer outline 10 application areas spanning predictive analytics, automated decision-making, and citizen engagement platforms.[12] This represents what Longbing Cao characterizes as AI's role in the next industrial revolution—transforming intellectual labor and knowledge work through augmented analytical capabilities that fundamentally reshape how governments anticipate, assess, and respond to complex challenges.[13]

However, AI governance raises critical ethical considerations, particularly regarding human oversight and trade-offs in autonomous decision-making. Jovana Davidovic identifies three purposes for meaningful human control: legal accountability, safety assurance, and moral dignity concerns, while Saar Alon-Barkat and Busuioc Madalina reveal cognitive biases in algorithm-supported public sector decisions through experimental evidence.[14] Anton Sigfrids et al. propose comprehensive governance frameworks emphasizing inclusive, institutionalized approaches, while Lena Enqvist critiques gaps in regulatory oversight infrastructure.[15]

Regarding resilience applications, Monique M. Kuglitsch et al. demonstrate AI's capacity to enhance disaster management through improved detection, forecasting, and real-time analytics across the resilience lifecycle, while Saman Ghaffarian, Firouzeh RosaTaghikhah, and Holger R. Maier emphasize explainable AI's importance for stakeholder trust.[16] Academic positions reveal nuanced perspectives: Seth Guikema acknowledges AI's transformative potential while cautioning against an over-reliance on black-box models without physical understanding, and Lazima Faiah Bari et al. identify validation challenges and public reluctance concerns.[17] Cao synthesizes these tensions through a smart disaster resilience framework expanding traditional mitigation-preparedness-response-recovery models into ten interconnected phases.[18] The framework positions AI as complementary augmentation requiring integration with domain expertise for effective whole-of-society resilience building.

Evolution Of National Resilience Systems Since 1945

Period	Model	Features	Strengths	Limitations	Examples
1945-50s	Civil Preparedness (COG)	Continuity of command; nuclear drills	Clear hierarchy; high redundancy	Static; lacks adaptability	US, UK
1960s-70s	Total Defense	Civil-military integration; conscription; national cohesion	Strong deterrence; whole-of-society ethos	Threat-driven; lacks systems logic	Finland, Sweden, Singapore
1980s	Comprehensive Security	Multi-dimensional: social, economic, environmental risks	Broader security lens	Poor implementation	Japan, ASEAN countries
1990s – 2000s	Critical Infrastructure Protection (CIP)	Asset-focused; sectoral resilience	Risk-based; technically grounded	Overlooks community/social elements	US, EU, Australia
2000s	Whole-of-Government	Inter-ministerial planning; policy alignment	Institutional coherence	Hard to scale locally	UK, Singapore, UAE
2004-2015	Community-Based Disaster Risk Management (CBDRM)	Local ownership; grassroots resilience	Culturally embedded; community legitimacy	Not easily scaled	Nepal, Indonesia
2010 – Present	Systems Resilience	Networked systems; adaptive feedback loops	Anticipatory; scalable	Abstract; hard to operationalize in national security	UAE, OECD member countries

Early post-war ***civil preparedness*** systems focused on military security and emphasized maintaining continuity of government under nuclear threat.

The 1951 Swedish ***total defense model*** pioneered integrating military defense with civil, economic, and psychological dimensions within a whole-of-society mobilization framework.[19]

The 1980s ***comprehensive security*** concept, prominent in Japan and ASEAN countries, expanded beyond military threats to encompass economic volatility, environmental degradation, and social cohesion.[20]

In the 1990s, recognition that networked infrastructure created systemic vulnerabilities led to the development of ***critical infrastructure protection (CIP)*** frameworks in the US, the EU, Canada, and Australia.[21]

The 2001 terrorist attacks in the US and the 2004 Indian Ocean tsunami exposed failures in cross-agency collaboration, driving **whole-of-government coordination** approaches that emphasized inter-ministerial coordination.[22]

Since 2004, ***community-based disaster risk management*** (CBDRM) approaches have emerged, particularly in Southeast Asia.[23] CBDRM emphasizes local knowledge, participatory planning, and adaptive capacity-building at grassroots levels.

Since 2010, OECD countries such as the UAE have developed ***systems resilience frameworks***. They encompass cross-sector adaptive capacity for a unified resilience approach, feedback loops to respond dynamically to shocks, scenario planning for stress-testing, and anticipatory governance to manage emerging risks proactively. [24]

Section 1

Exploiting the Emergence of an AI Inflection Point to Build Whole-of-Society Resilience

1.1 AI's Potential Ability To Transform National Resilience Systems

AI can analyze vast amounts of data in real time, anticipate emerging risks, and transform resilience from reactive recovery to proactive anticipation.[25]

Frameworks are already integrating lessons learned from the precision of CIP, the inclusivity of the CBDRM, and the adaptability of whole-of-government systems' resilience. Governments adopting holistic AI-driven resilience systems will move away from siloed coordination toward more integrated, well-orchestrated resilience models. AI-driven multi-agent systems (MAS) will enable central government ministries and operational agencies to share and process real-time data more effectively for informed leadership decision-making.

This will result in more effective intelligence fusion, asset deployment, and coordinated responses.

Unified planning and logistics, and greater societal readiness, will create continuous learning loops in which AI-enabled governments test and refine their resilience practices at scale to improve future preparedness. National resilience will evolve from a static plan to a living, data-driven, and adaptive doctrine that is dynamic, anticipatory, and globally interconnected, capable of learning and adapting faster than the crises it is designed to confront.

To appreciate the significance of MAS for national resilience, it is essential to understand how AI systems have matured from rigid, rule-based programs into dynamic, learning-driven architectures capable of autonomous action, self-learning, negotiation, and adaptation (see Table 1).

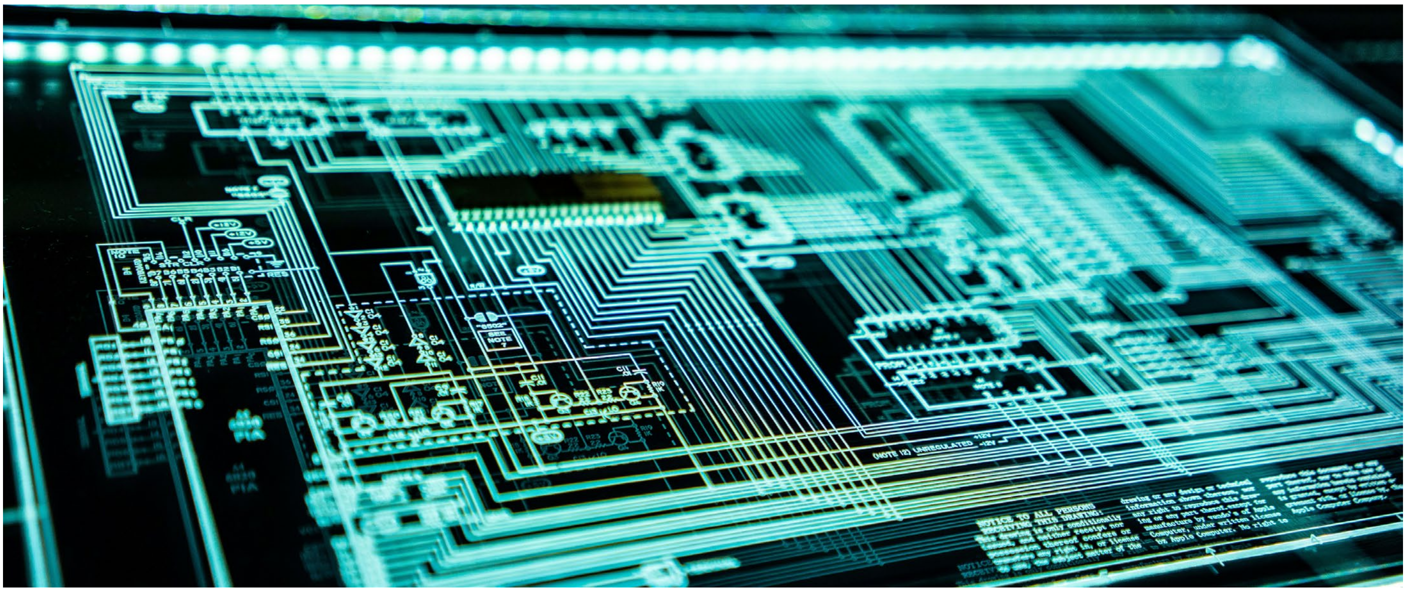


Table 1: Evolution of AI Models and their Relevance to Resilience

AI Generation	Period	Architectural Model	Core Characteristics	Limitations	Resilience contribution
Rule-Based AI	1950s-1980s	Expert systems; logic-based agents	Hand-coded rules; deterministic reasoning; "if-then" logic	Brittle; no learning; poor scalability and generalization	Enabled basic diagnostics and decision trees; useful for static standard operating procedures (SOPs) and contingency plans
Statistical / Machine Learning (ML) Models	1980s-2010s	Single-agent predictive models	Pattern recognition from structured data; regression analysis and decision trees.	Static once trained; narrow scope; limited adaptability	Allowed data-driven early warning systems and basic forecasting tools
Deep Learning Models	2010s-2020	Neural networks and stacks	High accuracy for unstructured data (images, audio, text); end-to-end learning	Requires large datasets; opaque ("black box"); still task-specific	Enabled real-time image/signal analysis (e.g., for flood maps, fire detection)
Foundation Models & Large Language Models (LLMs)	2020-2023	Transformer-based large models	Pretrained on massive data sets; learns new tasks and makes predictions using small range of examples; multi-task capability across domains	High computational cost; prone to hallucination; passive (do not act unless prompted)	Enhanced sense-making from open data; multi-lingual info systems and advisory bots
Multi-Agent Systems (MAS)	2023-present (frontier)	Distributed autonomous agents	Goal-oriented agents with distinct roles; capable of coordination, negotiation, and learning in real time	Complex to govern; emergent behavior; inter-agent conflicts require protocols and oversight	Mirrors real-world governance; enables dynamic, cross-sectoral coordination in crises

Both single-agentic AI systems and MAS are currently widely adopted by countries such as the US, EU member states, the UAE, and Singapore.

These systems are designed and optimized differently for diverse use cases or roles to enhance public service delivery. It is important to note that, given the pace of AI innovation, existing systems and new design variants are being tested and deployed rapidly. This is primarily due to AI model advancements, hardware upgrades, including memory and processing power, accelerated AI learning loops, and AI algorithmic efficiency.[26]

This report does not explain in depth the variant agentic AI architectures that are currently applied in different jurisdictions. However, it is important to note that these variants have strengths and limitations that can impact scalability, performance, and how widely MAS are adopted.

1.2 The Emergence Of Complex Hierarchical Reasoning Models

Current crises often involve cascading failures across overwhelmed emergency and public safety organizations, surging through health sector capacity and preparedness, infrastructure, finance, public trust, and other domains. In these complex, interconnected scenarios, there is an urgent need for next-generation AI-enabled resilience systems that can reason autonomously in real time across multiple domains and levels of government, with distributed datasets that may be partial, incomplete or ambiguous.

Since late 2024, a new generation of AI architectures called Hierarchical Reasoning Models (HRMs) have emerged, fundamentally differing from LLMs in their ability to perform multi-step reasoning and forward strategic planning (see Table 2):

Table 2: Key Advantages of HRMs in Problem-Solving Compared to LLMs

Capability	Standard LLMs	HRMs
Problem Breakdown	Limited; relies on prompts	Innate; automatically breaks complex tasks into manageable steps
Reasoning Transparency	Opaque; difficult to follow the logic	Explicit reasoning chains; each step documented and verifiable
Error Correction	Requires human intervention or re-prompting	Self-correcting; detects logical inconsistencies and revises
Multi-Step Planning	Struggles beyond three to four inference steps	Capable of more than 10 sequential reasoning steps, which maintain accuracy
Mathematical/Logical Rigor	Unreliable for proofs or precise calculations	Approaches human expert level in mathematics, coding, formal logic
Computational Cost	Moderate. Can only manage a single input of data.	High. Iterative reasoning requires multiple inputs of new, unseen data.

This architecture employs multiple AI agents arranged in layers. One agent acts as a high-level 'planner', breaking goals into sub-tasks; specialized lower-level agents execute and report back. The potential benefits of this architecture for resilience systems are strong top-down control and explicit task decomposition, which is good for long-term, multi-step reasoning that mirrors how organizational hierarchies develop policies, programs, and use cases, and make decisions during crises.[27]

Implications Of HRMs For Government Resilience Systems

Governments around the world are already exploring how HRMs can be introduced into existing or planned AI-enabled resilience systems that require rigorous, multi-step analysis. Although these initial efforts are still in development, Abu Dhabi's drive to become the world's first 'digital native' government by 2027 (see Case Study 1) and Singapore's project to build a whole-of-society 'Digital Twin' (see Case Study 3) offer early testing grounds for how HRMs could be integrated into national resilience systems.

Key advantages of HRMs over LLMs in whole-of-society resilience building include:

Crisis scenario planning, which covers complex, cascading failures across multiple domains, such as the AI outages in June 2025 across OpenAI, Cloudflare, Google Cloud, and dependent platforms that highlighted the importance of containment protocols.

Policy impact assessments across diverse populations that identify unintended consequences, enabling policy-makers to monitor and challenge them using HRMs before implementation.

Legal and regulatory analysis to identify regulatory conflicts and propose harmonization strategies across ministries and jurisdictions.

Resource optimization during crises, such as allocating medical supplies, organizing evacuations, and prioritizing infrastructure repairs.

Transparent decision support to enable democratic accountability, with decision-makers reviewing AI recommendations and challenging flawed assumptions.

HRM Governance Challenges and Risks

MAS that incorporate HRMs are the AI equivalent of whole-of-government coordination. Multiple agents represent ministries, cities, infrastructure sectors, and different population groups, all exchanging data, negotiating solutions, and learning from outcomes. They are not just a technical innovation. Deployed effectively, MAS have the potential to become an essential strategic tool for building whole-of-society resilience in a world of increasingly complex, interrelated risks and threats.

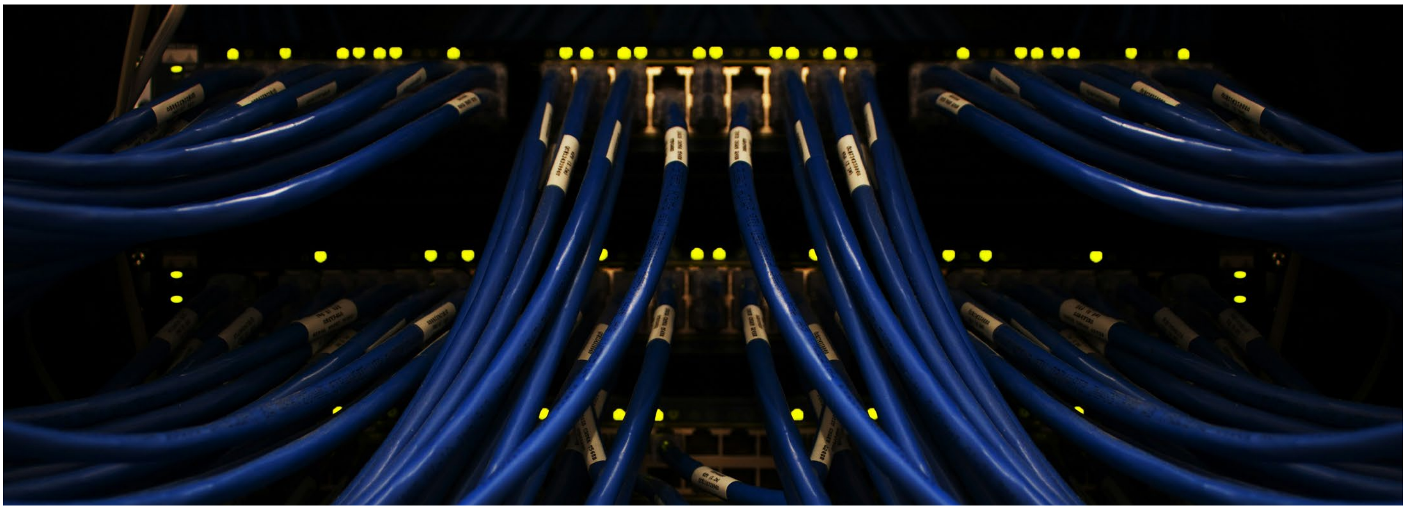
The sophistication of HRMs introduces new governance challenges. Their computational demands limit real-time deployment in some crisis scenarios. While their reasoning chains are more transparent than black-box LLMs, their complexity means they still require specialized expertise to monitor effectively. Most critically, HRMs' ability to generate persuasive but potentially flawed reasoning demands robust verification mechanisms and clear protocols for 'human-in-the-loop' oversight.[28]

In 'first-mover' countries such as the UAE, China, and the US, governments are developing and adopting leading edge AI models to strengthen different aspects of their defense, security, intelligence and resilience systems. They are investing heavily in AI model innovation, infrastructure, computational power, and workforce re-skilling and training.

Civil servants and private sector adopters in these countries recognize the need to acquire:

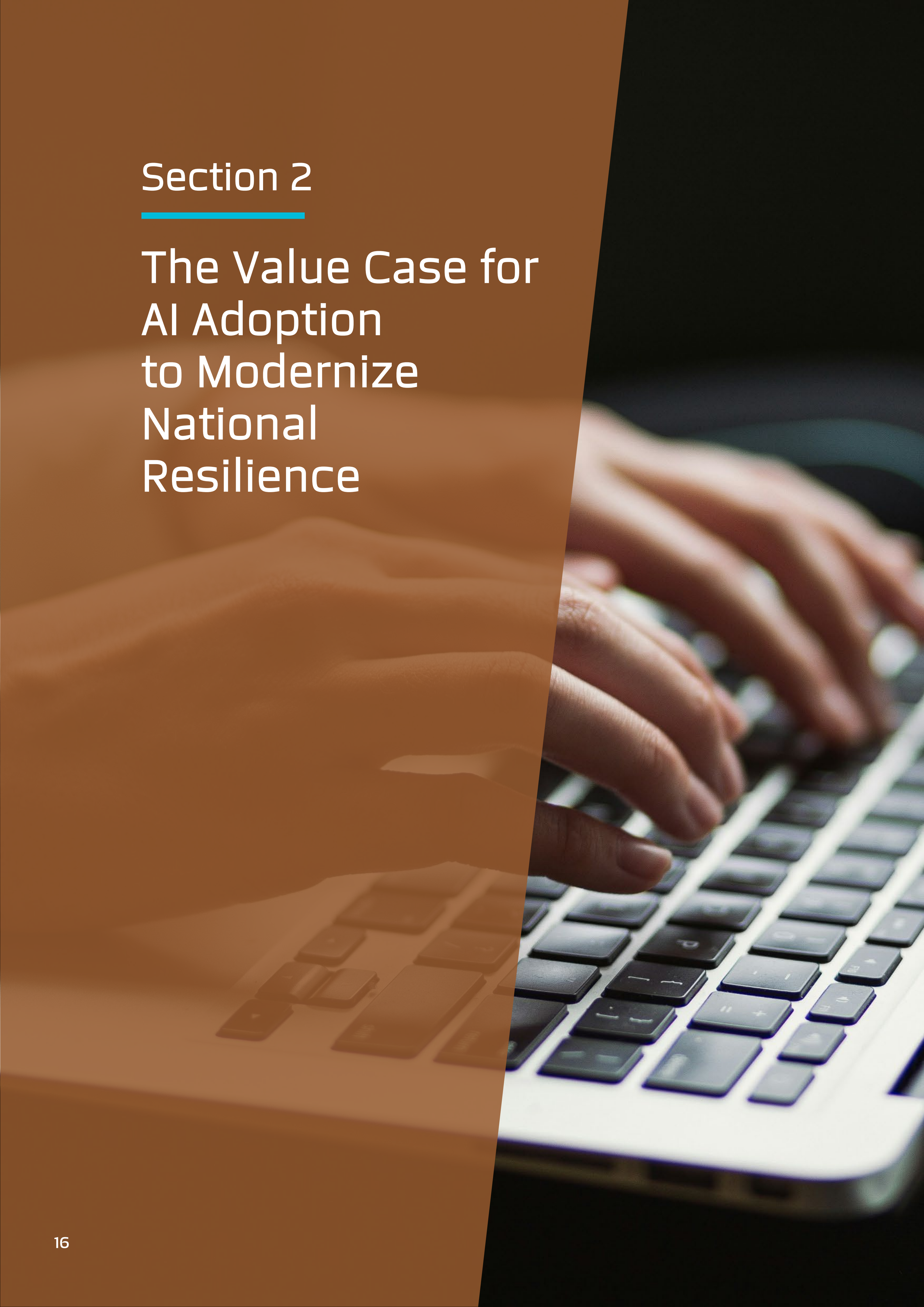
- Rapidly evolving technology
- Data scientists and subject matter experts with the skill sets to interpret reasoning chains, identify logical fallacies, and maintain 'human-in-the-loop' oversight.

However, both the technology and the required skill sets are becoming more complex, creating an increasing challenge that will need to be addressed to ensure the future efficiency of sophisticated AI applications in rapid response service sectors, such as defense, security, policing, and crisis management.



Section 2

The Value Case for AI Adoption to Modernize National Resilience



The value of AI in national resilience systems is no longer speculative. Its role is demonstrable, measurable, and increasingly strategic in an era defined by the increasing frequency and intensity of shocks, and by their interconnected, cascading nature. To realize this value, governments must move beyond piecemeal adoption and embed AI as a core public governance capability for whole-of-society resilience, built around the following dimensions: acceleration, integration, evolution, adaptation, and impact.

Acceleration: Enabling Faster Perception For Government Action At Scale

AI dramatically accelerates time-to-insight and time-to-response. Where human analysts may take hours or days to process complex, multi-source data, AI systems can extract patterns and trigger actions in near-real time.[29]

For example, computer vision AI models can detect wildfire spread from satellite data within minutes, allowing emergency services to be mobilized before fires breach containment lines. During pandemic outbreaks, natural language processing tools can scan news, social media, and health system indicators in seconds to detect early anomalies, enabling preemptive containment.[30] These are order-of-magnitude improvements in agility, with lives, assets, and critical infrastructure at stake. The advent of HRMs is further increasing the speed and scale of AI-enabled crisis responses. For instance, in Australia, HRMs are being added to the country's emergency response system (see Case Study 2).

Integration: Orchestrating Fragmented Systems Into A Cohesive Whole

In most governments, resilience-relevant data are dispersed across ministries, levels of government, and sectors. Health systems, transportation networks, emergency responders, infrastructure operators, and civil society organizations rarely share real-time intelligence. AI systems can act as intermediaries between institutions, enabling 'many-to-many' data exchanges and decision support, provided participants adopt shared cloud infrastructure, semantic data models, and interoperable application programming interfaces (APIs).[31]

For example, an AI platform integrating public health trends, hospital capacity, and transport congestion data can route ambulances optimally during an urban disaster. This is shown by emergency deployments that fuse GPS telemetry from ambulances, hospital data on bed queues, and live traffic feeds and signal controls to pre-clear corridors and alert hospitals.[32] Similarly, AI agents targeted at the economy can flag impending supply-chain disruptions and trigger cross-ministerial alerts by fusing customs manifests, logistics statuses, trade volumes, and risk signals—enabling early warning and human-in-the-loop triage across customs, trade, and economic ministries.[33]

Integration also improves crisis orchestration, reducing cascading failures caused by uncoordinated decisions. Recent incident analyses highlight the need for interoperable, multi-agency AI platforms capable of modeling cross-domain dependencies and issuing coherent guidance for action.[34]

2.3 Evolution: Embedding Continuous Learning Into The Fabric of Governance

Traditional public sector resilience systems become outdated. Complacency sets in, policies lag behind risk trajectories, and institutional memory is lost as personnel rotate. By contrast, AI systems enable knowledge retention, continuous model retraining, constant situational awareness, policy refinement, and systematized learning at a scale and capacity that exceeds current human constraints.[35]

Machine learning (ML) systems that process post-crisis data can improve over time, learning which interventions were effective, where delays occurred, and which populations were underserved. This creates the foundation for adaptive governance, by deploying the latest HRMs to ensure that governance improves with use, evolves under uncertainty, and closes the loop between planning, operations, and after-action review. Critically, these systems can test, simulate, and project different outcomes from changing threat environments, with the resulting data informing policy and risk management programs. Governments can thus invest more efficiently in targeted current and future capabilities to address crisis events that affect citizens' lives.

2.4 Impact: The Intersection Between AI, Resilience And National Prosperity

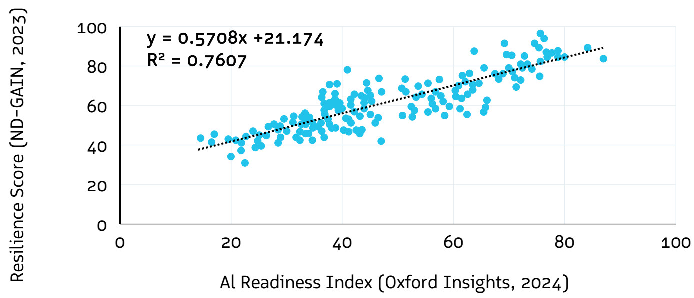
To assess whether these benefits materialize at scale, we examined the intersection of four global indices (see Figure 1): AI readiness (Oxford Insights, 2024), resilience (FM Global Resilience, 2024; ND-GAIN Resilience, 2023), and GDP per capita (International Monetary Fund, 2025).[36]

> **Analysis reveals strong positive correlations** between AI readiness, resilience, and national prosperity (as measured by GDP per capita - set to current year prices and adjusted for purchasing power parity):
>
> - **AI Readiness (2024) × Resilience - ND Gain (2023):** R^2 = 0.76 (n = 121)
> - **AI Readiness (2024) × FM Global Resilience (2024):** R^2 = 0.74 (n = 121)
> - **ND Gain (2023) × GDP per capita (2025):** R^2 = 0.67 (n = 173)
> - **AI Readiness (2024) × GDP per capita (2025):** R^2 = 0.60 (n = 180)

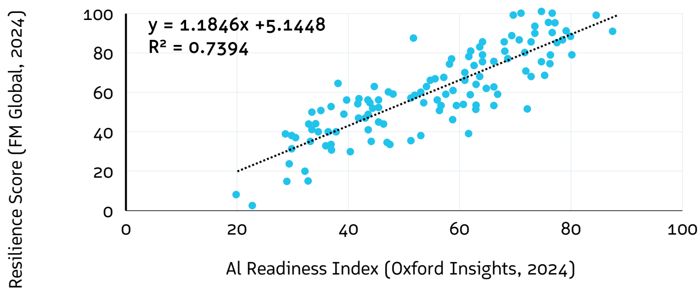
Countries with high AI adoption rates exhibit both stronger institutional resilience and superior relative economic performance, reflecting an ‘AI-enabled resilience dividend’ effect from reduced losses through early warning systems and risk mitigation; enhanced institutional performance driven by real-time, accessible information; and increased national competitiveness.[37]

Figure 1: How AI Readiness Supports Resilience and Increases GDP Per Capita

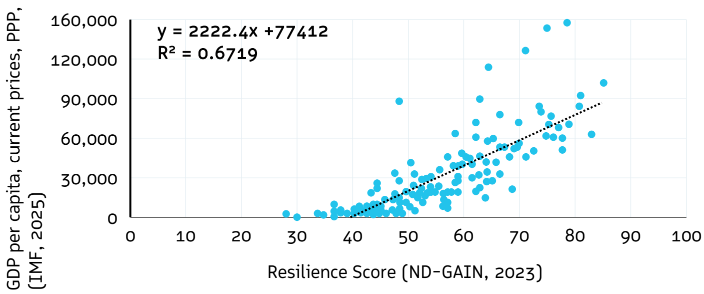
AI Readiness vs. Resilience Scores



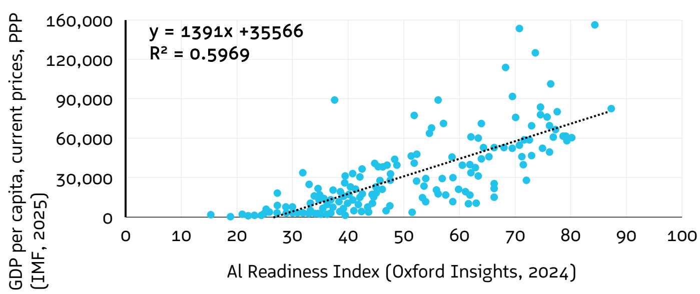
AI Readiness vs. Resilience Scores



AI Readiness vs. GDP per capita



AI Readiness vs GDP per capita



Section 3

A Multi-Layered Framework for AI-Enabled National Resilience Systems

To operationalize AI for national resilience, governments must develop a comprehensive, integrated framework that aligns institutional mandates, technical capabilities, and resilience objectives. We propose an interconnected four-layered framework for AI-enabled national resilience systems that supports anticipation, coordination, recovery, and long-term adaptation.

Layer One: Resilience Domains

The first step in building AI-enabled resilience is identifying which domains must be adaptive, secure, and robust (see Table 3).

Each domain is susceptible to direct shocks and indirect, systemic risks. AI becomes critical when its insights and actions can flow across these domains, enabling resilience to be implemented as a whole-of-society enterprise rather than a series of parallel efforts.

Table 3: Key Resilience Domains And AI Opportunities

Resilience Domain	Definition	Leading Programs	AI Enhancement Opportunities
Economic & Financial	Stability of financial systems, budgets, markets, and trade during shocks	EU Recovery and Resilience Facility US CHIPS and Science Act Singapore's Resilience Budget	Predictive fiscal analytics, early warning for asset bubbles, optimization of fiscal stimuli
Infrastructure & Energy	Reliability of critical infrastructure: energy, water, transport, telecoms	UK's 10-year infrastructure strategy Japan's infrastructure resilience strategy	Predictive maintenance, digital twins for cascading failures, AI-assisted utility restoration
Health & Biosecurity	Continuity and adaptability of public health systems and epidemic preparedness	Korea's smart quarantine system Rwanda drone delivery network WHO Epidemic Intelligence from Open Sources (EIOS) initiative	AI outbreak forecasting, diagnostics, hospital triage, autonomous medical logistics
Food & Water Security	Sustainable access to food and clean water systems under stress	World Food Programme HungerMap LIVE India's drought resilience programs and initiatives	Climate-smart agriculture, predictive drought monitoring, AI supply chain tracking
Public Safety & Cyber	Stability of law enforcement, civil defense, and cyber operations	Estonian Defense League's Cyber Unit New Zealand's Cyber Security Strategy "safecity" online platforms	AI threat detection, predictive policing (with safeguards), automated cyber intrusion prevention
Governance & Institutions	Integrity, adaptability, and trust in government operations during crises	UAE Strategy For Artificial Intelligence United Nations Development Programme's resilient governance policies and initiatives	AI service continuity, NLP for sentiment tracking, automation of claims processing

Layer Two: The Resilience Lifecycle

Resilience is a cyclical process in which AI systems should be integrated at every stage, from foresight and prevention to real-time response and long-term learning (see Table 4). Each crisis generates new data and lessons learned, which, when processed by AI, inform future 'whole-of-society' planning and preparedness. This lifecycle thinking has been in practice since the 1980s in various forms. The detailed lifecycle set out below highlights the importance of 'Anticipation, Assessment, Detection, and Adaption' in standard planning, preparedness, response, and recovery resilience strategies.

Table 4: AI Enablement Across the Resilience Lifecycle

Lifecycle Stage	Definition	Current AI Use Cases	Future AI Enhancements
Anticipate	Identifying and forecasting risks before they materialize	Climate risk models, epidemic early warning systems (BlueDot, EIOS), financial market stress indicators	Multi-agent predictive platforms integrating climate, geopolitical, and economic risks; AI-driven cross-border "resilience radar"
Assess	Mapping vulnerabilities and interdependencies within and across systems	AI-based vulnerability mapping, systemic risk modeling in banking, food system interdependency analysis	Dynamic "digital twin" models of national systems; AI platforms continuously stress-testing resilience capacity
Plan	Designing and stress-testing strategies, budgets, and policies	AI simulations for fiscal shock scenarios; digital twin models for cities; scenario planning in energy transition	AI-assisted adaptive policy platforms that learn from real-time events; automated resilience budgeting
Prepare	Building institutional and community readiness to respond to shocks	AI-enabled readiness dashboards, predictive demand for medical supplies, simulation-based training for first responders	Immersive AI-enabled training environments; predictive allocation models across multiple ministries
Detect	Spotting disruptions as they emerge in real time	AI anomaly detection in cybersecurity; satellite imagery for fire detection; wastewater AI surveillance for pandemics	Integrated AI "sensors" across domains; autonomous detection networks combining Internet of Things (IoT) and AI for multi-hazard awareness
Respond	Coordinating and mobilizing resources during a crisis	AI for dynamic resource allocation (e.g. ambulance routing); drone deployment for firefighting; crisis decision-support tools	Fully autonomous crisis-response orchestration platforms; cross-agency AI systems optimizing inter-ministerial coordination
Recover	Restoring infrastructure, services, and economic activity	AI models for economic recovery forecasting; optimization of infrastructure reconstruction; AI in insurance claim processing	National AI "recovery engines" to optimize investment prioritization; long-term economic restructuring guided by AI scenario modeling
Adapt	Learning and embedding improvements into long-term systems	AI analysis of lessons from crises; updating urban codes with AI risk insights; post-event policy evaluation	Continuous adaptive governance platforms; AI-driven "learning loops" embedded into policymaking and regulation

Layer Three: Core Enablers

Successful AI deployment requires the right enabling conditions across governance, infrastructure, energy, workforce, data integration and oversight, and cyber-security . However, enablers are often seen as 'opt in' investments or back-office functions when they are an essential part of the strategic scaffolding in successful AI-driven resilience systems (see Table 5). The highest-performing countries, from Estonia and Singapore (see Case Studies 3 and 4) to China and the US (see Case Study 6), invest in both AI applications and core enablers to build a solid foundation that enables intelligent governance.

Table 5: **Core Enablers for AI-Resilience Systems**

Enabler	Description	Leading Practices
Data Infrastructure	Secure, standardized, and interoperable platforms for real-time and batch data exchange	Estonia's X-Road EU's Gaia-X cloud, UAE government data fabric
Computing Capacity	High-performance, scalable cloud and edge computing	Abu Dhabi Government Digital Strategy 2025-2027; Japan's Fugaku supercomputer for disaster simulation
Human Capital & Skills	Data literacy, domain-AI fluency, and workforce transformation	UK's Data Science and Data Visualization Accelerator programs UAE's public sector AI training Singapore's Smart Nation Scholarship
Policy & Governance	Ethical frameworks, oversight bodies, procurement standards, legal authorizations for AI in emergencies	UK's Responsible Technology Adoption Unit (RTA) and Algorithmic Transparency Recording Standard Hub (ATRS) Singapore's Model AI Governance Framework for Generative AI
Public-Private Ecosystem	Collaboration between academia, government technology bodies, private sector, and civil society	Rwanda-Zipline drone partnership Singapore's Government Technology Agency (GovTech) and Microsoft's AI labs collaboration
Financial Investment	Dedicated, sustained and flexible funding models for resilience technologies	World Bank's Resilience Bonds UAE's Digital Transformation Fund

Layer Four: AI Architecture

Governments must incorporate subsidiary layers into the AI architecture to improve technical scalability, policy compliance, auditability, and fault tolerance, thereby enabling a national MAS to be fully operational for resilience (see Table 6).

Table 6: Subsidiary AI Architecture For National Resilience Systems

Subsidiary Layers		Purpose & Description	Key Design Features / Examples
1	Agent	Domain-specialized AI agents act independently within a shared environment	Health Agent: tracks outbreaks and hospital capacity Transportation Agent: simulates routing and congestion Power Agent: monitors grid loads; each agent has tailored perception, logic, and action capabilities
2	Communication	Ensures agents can securely and effectively share information, requests, and intentions	Shared definitions of concepts and relationships; real-time asynchronous messaging; agent authentication; LLM-based agent messaging
3	Coordination	Manages negotiation and joint action among agents to avoid conflict and align goals	Task bidding mechanisms; joint intention theory; decentralized decision making; planning protocols
4	Learning	Enables agents to develop their models and behaviors through feedback and experience	Supervised learning from labeled crisis data; reinforcement learning; multi-agent simulations; learning embedded in digital twin testbeds
5	Governance	Enforces ethical, legal, and institutional constraints on agent behavior	Hard-coded constraints; escalation involving humans for high-impact actions; post-event audit logs; machine-readable policy integration
6	Security & Robustness	Protects system integrity from hostile manipulation, malfunction, or cascading failure	Encrypted communications; runtime anomaly detection; intrusion detection; quarantine protocols; system-wide back-ups when servers, networks or components fail

Section 4

Global Case Studies: Governments Pushing the Frontiers of AI Adoption

AI is no longer a potential tool for building resilience. Around the world, a growing number of governments are deploying AI at scale across public services, national security, digital infrastructure, and whole-of-society systems.

This section presents detailed case studies that illustrate common design principles for other countries to follow. As noted in the Introduction, there is no 'one-size-fits-all' model for building AI-driven 'whole of society' resilience. The case studies highlight how each model must be adapted to country's political and socio-economic conditions and to its citizens' needs.

Case Study 1: Abu Dhabi – Aiming To Become The World's First AI-Native Government

Strategic Vision and Investment

In September 2025, the Department of Government Enablement (DGE) launched the Digital Government Strategy 2025-2027, publicly declaring the goal of becoming the world's first fully AI-native government by 2027.[38] The strategy allocates AED 13 billion (US$3.5 billion) toward deploying more than 200 AI use cases across over 40 agencies, aiming to contribute an additional AED 24 billion (US$6.5 billion) to GDP and create more than 5,000 public-sector jobs.[39]

Institutional Backbone

The initiative is coordinated by DGE and delivered via TAMM, a unified citizen services platform.

Digital Infrastructure

A sovereign-cloud mandate requires 100% of government data and services to operate on cloud infrastructure, ensuring data control, secure AI deployment, and scalable computation - the essential foundation for whole-of-government AI integration.

Workforce Transformation

By late 2025, more than 95% of Abu Dhabi's 30,000 civil servants had completed AI training. Each government entity now has an appointed Chief Data and AI Officer, supported by cross-agency forums for governance and accountability.

Use Cases in Action

- Proactive services: AI auto-triggers lifecycle services (e.g., birth registration).
- Virtual assistants: 24/7 support in over 15 languages.
- Smart compliance: AI validates business licenses and visas in real time.
- Emergency services: AI-enabled drones and computer vision assist crowd monitoring and traffic management.

Outcomes

400,000
fewer in-person service visits

64%
fewer requests

23%
fewer process steps

36%
fewer data fields

95%
resolution and

92.5%
satisfaction

Cost savings reinvested into frontline services

Recognized internationally as a benchmark for intelligent governance

Case Study 2: Australia – AI-Enabled

All-Hazard Emergency Management

Australia's National Emergency Management Agency (NEMA), in collaboration with CSIRO Data61 and Geoscience Australia, has established one of the world's most advanced AI-assisted emergency ecosystems. These agencies integrate meteorological, satellite, terrain, and vegetation data into CSIRO's Spark wildfire simulation platform, enabling predictions of fire spread and air quality that support the Australian Disaster Resilience Knowledge Hub Spark. Used nationwide by fire and emergency services, Spark performs real-time, GPU-accelerated simulations to guide evacuations, resource allocation, and hazard reduction.

Quantified Impact (2019-2023):

- Approximately 35% faster emergency response deployment, according to NEMA reports on improved triage and coordination through AI-informed platforms.[40]

- Approximately 22% reduction in property losses via preemptive interventions guided by AI-enabled simulation models.[41]

- 87% accuracy in high-risk fire-weather forecasting, up from around 60%, attributed to CSIRO Data61 predictive modeling.

- 92% user satisfaction with the early warning system, based on surveys from New South Wales and national disaster ready dashboards.

Case Study 3: Singapore - Digital Twin Nation

In 2015, the Singapore Land Authority launched Virtual Singapore, an initiative to create the world's first national-scale digital twin using high-resolution LiDAR scans, IoT sensor data, and geospatial analytics.[42] The platform, developed in collaboration with the Smart Nation and Digital Government Office and GovTech, integrates climate, mobility, infrastructure, and urban datasets to simulate disruptions and optimize resilience planning.[43] AI-powered simulation engines allow policymakers to stress-test scenarios such as floods, transport breakdowns, and heatwaves before they occur.[44] The digital twin is linked to citizen service platforms, enabling adaptive policies such as traffic rerouting, public transport fleet reallocation, and deployment of cooling infrastructure during heatwaves.[45]

Impact:

- **20% faster urban planning approvals**, achieved through integration of Building Information Modeling and geospatial simulation tools.

- **15% improvement in walkability** scores, driven by analytics that identifying pedestrian bottlenecks and optimized routing.

- **40% reduction in properties affected** by flooding, enabled by targeted barrier placement and drainage upgrades tested in Virtual Singapore simulations.[46]

Case Study 4: Estonia - E-Governance Resilience

Estonia's Information System Authority and e-Governance Academy have built one of the world's most resilient digital governance ecosystems. At its core is X-Road, a secure, decentralized data exchange layer that connects all public registries while preserving each entity's autonomy.[47] Estonia integrates AI-enhanced cybersecurity for anomaly detection and automated continuity protocols, supported by its Computer Emergency Response Team (CERT-EE).[48] The country also deploys Bürokratt, an AI-powered virtual assistant, to streamline service delivery and maintain operational continuity.[49] To safeguard national operations during crises, Estonia pioneered 'data embassies'—foreign-hosted mirrored environments with diplomatic immunity, first established in Luxembourg.[50]

Proven Resilience:

- 99.9% uptime during major crises, including the 2007 cyberattacks and COVID-19 pandemic, enabled by X-Road's architecture and CERT-EE's resilience protocols.[51]
- Less than 15 minutes to launch new digital services, supported by Estonia's rapid deployment frameworks and automation tools.[52]
- Annual savings equivalent to around 2% of GDP through digital efficiency and reduced administrative overhead.[53]

Case Study 5: UK - Intelligence Fusion And AI Governance

The UK operates advanced intelligence fusion centers, managed by the Government Communications Headquarters (GCHQ) and the National Cyber Security Centre (NCSC), that integrate multi-source inputs—classified intelligence, network data, open-source intelligence—into unified situational awareness platforms to detect and prioritize national threats.[54] These centers employ graph neural networks, natural language processing, and multi-agent analytics to correlate data and improve triage workflows, enabling human analysts to focus on strategic decisions. NCSC's internal dashboards leverage these capabilities to accelerate detection-to-action timeframes and produce alert summaries for cross-government coordination.

The Office for AI and Responsible Technology Adoption Unit has implemented a comprehensive governance model. This includes the AI Assurance Toolkit (2024), Model for Responsible Innovation, Algorithmic Transparency Recording Standard, and mandatory transparency reporting—now in effect across all central government departments and arm's-length bodies.[55] The AI Assurance (February 2024) framework promotes operational standards such as explainability, impact assessment, and secure-by-design across government.

Impact:

- Approximately 60% reduction in time from intelligence collection to actionable insight, enabled by AI-accelerated triage and federated fusion dashboards at NCSC and GCHQ. [56]

- Improved threat detection accuracy driven by real-time fusion of multiple data sources and machine learning models at NCSC and GCHQ.
- Around 92% decrease in phishing email exposure, as confirmed by NCSC's AI-accelerated filtering during CYBERUK 2024-25.

Case Study 6: US - Agentic AI For Defense Strategic Foresight

The US Defense Advanced Research Projects Agency and Chief Digital and AI Office develop AI-driven multi-agent wargaming systems that support strategic planning and defense readiness. These 'agentic' simulations use reinforcement learning, large language models, and autonomous reasoning agents to test decision outcomes across dynamic, multi-domain battlefields.[57]

The systems integrate live operational data with synthetic environments to evaluate strategy, logistics, and coalition coordination in real time. AI agents play both friendly and adversarial roles, revealing vulnerabilities before actual crises occur.

Table 7: Comparison Of Best Practices In Deploying AI For Resilience Across Countries

Country	Focus Area	Key Capabilities	Lessons for Replication
Abu Dhabi	AI-native government transformation	200+ AI solutions across 40+ entities; sovereign cloud; TAMM 4.0 platform	Visionary leadership and early regulatory alignment critical; workforce-first approach essential
Australia	All-hazard emergency management	Real-time geospatial AI; predictive modeling; national disaster platform linking federal/state actors	Data interoperability and explainable AI vital for trust and coordination
Singapore	Digital Twin Nation	City-scale simulation of climate, mobility, socio-behavioral patterns; agent-based crisis foresight	Start with 3D basemap and layer domain models iteratively; build trust through transparency
Estonia	Cyber-resilient e-governance	Blockchain-secured public registries; AI-driven anomaly detection; "digital embassies" abroad	Distributed architecture and digital sovereignty ensure continuity
UK	Fusion centers & AI assurance governance	GCHQ-led multi-agent data fusion; National AI Ethics Board; algorithmic transparency guidelines	Embed AI governance from outset; "human-on-loop" models sustain legitimacy
US	Military AI agentic wargaming	Defense Advanced Research Projects Agency-led multi-agent simulations for national security, logistics, crisis foresight	Agent-based modeling reveals unknown failure paths; use simulations to test policy pre-emptively

Key Insights:

- **Data interoperability** unlocks cross-sector value.
- **AI governance capacity** enables algorithm audits, transparency, and public engagement to coexist with innovation.
- **Center-led transformation management**, as in Abu Dhabi and Singapore, prevents pilot fragmentation and accelerates transformation.
- **Early adopters** show faster shock recovery, greater adaptive capacity, measurable GDP impacts and investment benefits.

PwC Perspective: Building AI-Enabled Resilience in the Middle East

Across the Middle East, governments are placing transformation at the center of their national strategies, deploying AI across health, mobility, energy and public administration to strengthen whole-of-society resilience. This reflects a clear ambition: to reconfigure how public institutions anticipate shocks, deliver services and sustain trust. In doing so, the region is positioning itself as a global reference point for tech-enabled governance.

AI is no longer an enabling tool at the margins; it is becoming the backbone of transformation. PwC economists have indicated that if the Middle East would see an AI productivity boom amount to an additional 8.3 percentage points of growth between 2023 and 2035, if adoption is widespread and responsible.[58] Through national data strategies, climate-monitoring platforms, digital identity systems and integrated service architectures, intelligence is being embedded into the fabric of governance itself. This allows governments to break down institutional silos, align services around human needs such as care, mobility and energy, and deliver faster, fairer and more connected outcomes.

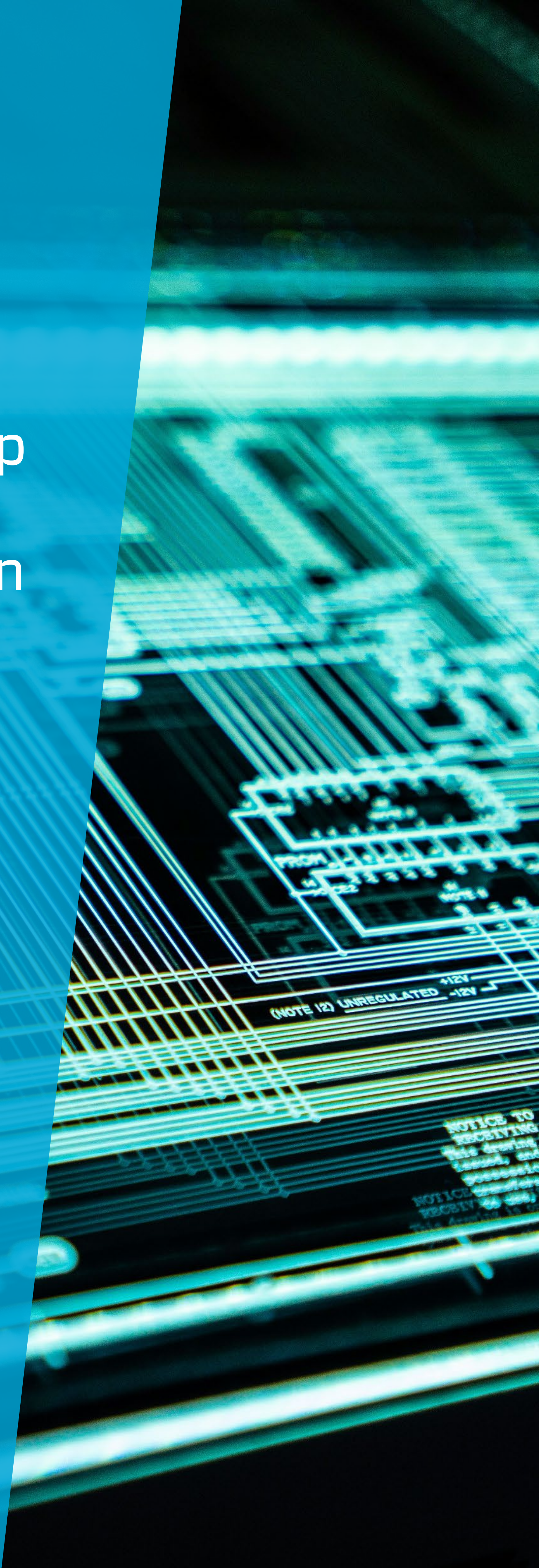
The decade ahead will test the region's ability to lead through this complexity.

Governments that take a whole-of-government approach, investing early in responsible AI frameworks, modernising legacy systems, scaling national digital and technology talent and strengthening coordination across ministries and agencies will be better positioned to anticipate shocks and respond cohesively. By building strong regional and global AI partnerships, these governments will not only future-proof their economies, but also set a new global benchmark for resilient, human-centred governance in the age of AI.

Rami Nazer, Clients and Markets Leader, PwC Middle East and PwC EMEA Government & Public Sector Leader

Section 5

Conclusion: Why Innovative, Agile Leadership is the Critical Human Factor in AI-Enabled Resilience



As AI becomes foundational to national resilience systems, a new kind of leadership is required that is technologically competent, institutionally agile, ethically grounded, and has strategic foresight. Governments must harness the most advanced AI architectures, notably HRMs, while ensuring that AI-enabled systems have robust safeguards that address the following issues (see Table 8):

- What functions should be delegated to AI?
- What should remain in human hands?
- What happens when AI and humans disagree?
- What values should guide the system's actions?
- How does AI manage trade-offs between efficiency, social equity, and security?

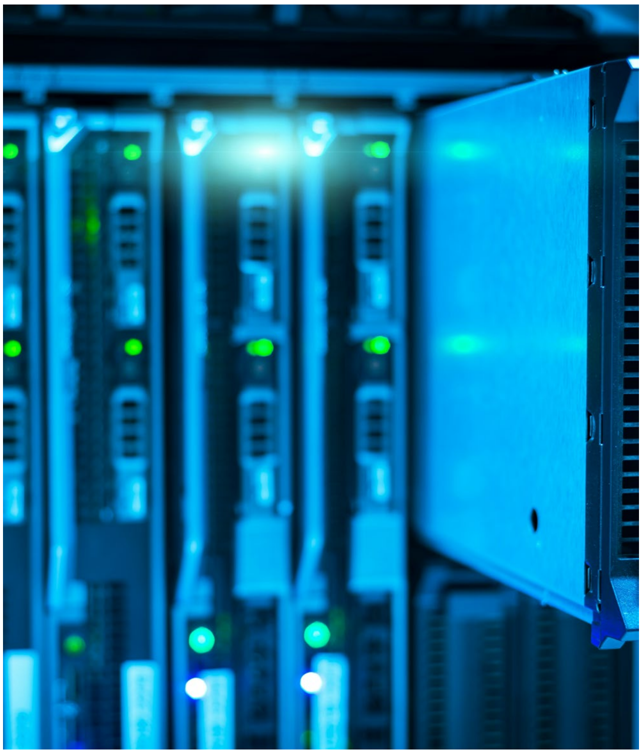
Table 8: Leadership Imperatives for Responsible AI in Resilience

#	Imperative	Strategic Leadership Action
1	Contextual Design	Align AI tools with national risk profiles, cultural expectations, and institutional structures. Avoid transplanting systems from dissimilar environments without adaptation.
2	Polycentric Governance	Enable coordination across central, sectoral, and sub-national levels. Establish shared standards but allow for contextual flexibility and distributed innovation.
3	Ethical Foresight	Institutionalize ex-ante AI risk assessments and ethics reviews for all resilience-related systems, especially those with direct public-facing impact.
4	Human-Centric Design	Maintain human-in-the-loop controls for high-stakes decisions. Build explainable interfaces that allow field responders and policymakers to trust, contest, and override AI.
5	Transparency by Default	Mandate open algorithmic documentation, decision traceability, and public-facing impact summaries for AI systems used in crisis settings.
6	Workforce Transformation	Build AI literacy across all levels of government. Recruit hybrid teams combining technical and policy expertise. Professionalize public sector data science roles.
7	Regulatory Agility	Develop iterative regulatory pathways, including sandboxes, crisis-specific waivers, and performance-based standards that can evolve alongside technology.
8	Fail-Safe Engineering	Require AI resilience systems to incorporate redundancy, kill switches, adversarial simulation, and manual fallback operations by design.
9	Global Stewardship	Participate in multilateral AI resilience governance frameworks. Contribute to open-source models, shared standards, and joint simulation platforms.
10	Trust and Legitimacy	Engage citizens through participatory design, transparent deployment, and inclusive oversight. Treat public trust as a critical infrastructure asset.

The AI Resilience Paradox

New AI technologies that make governments faster, smarter, more coordinated and more resilient can also become new sources of systemic fragility, and even a threat to society, if they are poorly designed or ungoverned. This is the essence of the **AI-resilience paradox.**

AI systems that build and underpin whole-of-society resilience must contain safeguards to ensure that humans retain final decision-making authority. This imperative is especially relevant in sectors where lives are at risk, such as policing and emergency services. In the case of military mobilization and deployment, strict global conventions and monitoring aim to ensure that leaders make ethical decisions with command authority in the 'kill chain'.



The AI resilience paradox is not theoretical. It is a wake-up call for government leaders. Examples are multiplying of systems failing in high-stakes settings due to inadequate human monitoring. They include risk-scoring tools that produce racial bias, predictive models that fail due to limited or inaccurate training data, and misinformation-detection algorithms that silence legitimate dissent. In resilience systems, such failures can escalate rapidly, with each error compounding the next one. Ethical oversight and 'human-in-the-loop' command-level decision-making must be retained in tomorrow's AI-enabled resilience systems to reduce the risk of unforeseen vulnerabilities that could undermine the entire system.

AI-enabled resilience systems must therefore incorporate human oversight, redundancy, auditability, and institutional feedback loops to detect and correct anomalies, errors, and issues. The operating assumption should be that failures will occur, with the system configured to recover without trigger a cascade of failures across multiple domains.

Resilience in the AI age will thus require responsiveness, reflexivity, ethical compliance, and the ability to learn from disruption.[59] It will require governments to accept guidance from a superior form of intelligence and engage it through distributed, adaptive systems that blend machine intelligence with human judgment. This is the indispensable human factor for building AI-enabled resilience.

1. Appendix A: Data Methodology Details Infographics
2. Appendix B: Extended Case Study Technical Details

Appendix A: Data Methodology Details

Data Collection and Processing

The empirical analysis in Section 4 draws on four primary datasets, each selected for comprehensive coverage, methodological rigor, and international recognition:

Government AI Readiness Index

Oxford Insights (2024). *Government AI Readiness Index 2024*. London: Oxford Insights.

Assesses 188 countries across five pillars: government leadership/vision (15%), infrastructure/data (25%), capacity/skills (20%), public service delivery (20%) and the innovation ecosystem (20%). Each pillar comprises eight to ten indicators drawn from public data sources (World Bank, International Telecommunication Union, UNESCO), expert assessments, and government surveys. The composite index ranges from 0 (lowest readiness) to 100 (highest readiness).

FM Global Resilience Index (2024)

FM Global (2024). 2024 *FM Global Resilience Index*. Johnston, RI: FM Global.

Evaluates business environment resilience across 130 countries using 12 key drivers grouped into economic factors (GDP trends, productivity, political risk), risk quality (exposure to natural hazards, risk management quality, corruption control), and supply chain resilience (infrastructure quality, supplier quality, visibility/control). Higher scores indicate greater resilience.

ND-GAIN Country Index (2023)

ND-GAIN (2025). *ND-GAIN Country Index* 2024. Notre Dame, IN: University of Notre Dame Global Adaptation Initiative.

Measures climate vulnerability and adaptive readiness for more than 180 countries through vulnerability score (exposure, sensitivity, adaptive capacity across six life-supporting sectors: food, water, health, ecosystems, habitat, infrastructure) and readiness score (economic, governance, social readiness for adaptation investments). Higher overall scores indicate lower vulnerability and higher readiness.

GDP per Capita, Current Prices, PPP Data (IMF, 2025)

International Monetary Fund (2025). *World Economic Outlook (WEO) database*, April 2025. Washington, DC: IMF.

The IMF's estimate of average output per person in 2025 is adjusted for purchasing power parity so countries are comparable on the same cost-of-living basis. It is expressed in current (nominal) international dollars. The analysis uses current prices and reflects the 2025 price level. It is best for cross-country comparisons at a point in time rather than tracking real growth across years. It is a strong indicator of relative living standards and a reasonable proxy for average material prosperity.

Limitations Of Comparisons Between Datasets

Cross-Sectional Design: Data from 2023-2024 limits causal inference. Observed correlations may reflect AI driven resilience and prosperity, reverse causation, third variables driving all three, or reciprocal relationships.

Measurement Validity: Composite indices blend diverse components potentially obscuring specific mechanisms. AI readiness combines policy frameworks with actual deployments; FM Global emphasizes business continuity over social equity; ND-GAIN focuses on climate adaptation, not broader resilience.

Sample Bias: Data availability skews toward wealthy democracies with greater transparency. Results may not generalize to emerging economies, conflict-affected states, or small island developing states underrepresented in indices.

Appendix B: Extended Case Study Technical Details

Abu Dhabi Technical Architecture

Data Layer:

- Emirate-wide data fabric connecting more than 40 entities through standardized APIs
- Master data management ensuring consistency (citizen IDs, business registrations, land records)
- Privacy-preserving techniques: anonymization, access controls, audit logging
- Real-time data exchange enabling responsive services

AI/ML Platform:

- Centralized platform with pre-built models for common use cases (Natural Language Processing, computer vision, forecasting)
- Model marketplace enabling entities to share and reuse AI capabilities
- Machine Learning Operations pipelines: versioning, deployment, monitoring, retraining
- Explainability tools ensuring transparency for citizen-facing decisions

Application Layer:

- TAMM 4.0 AI-native service gateway integrating more than 900 government services
- Multilingual AI virtual assistants (Arabic, English, more than 13 additional languages)
- Proactive service triggers detecting life events and auto-initiating services
- Intelligent workflow automation reducing processing times from 40% to 60%

Australia Fire Danger Rating System (FDRS)

Technical Components:

- Integrates more than 15meteorological variables (temperature, humidity, wind speed/direction, rainfall, atmospheric instability)
- Vegetation fuel load estimation via satellite imagery (Landsat, Sentinel) processed by computer vision models
- Topographic analysis predicting fire behavior using digital elevation models and slope calculations
- Color-coded risk maps updated hourly across a 72-hour forecast horizon
- Accuracy improvement from 60% to 87% for high-risk fire weather

Implementation Challenges:

- Six states, plus two territories with different emergency management systems
- Solution: Common data standards, APIs, federated architecture allowing local autonomy while enabling federal integration
- Model validation: Hindcasting on historical events, expert review panels, and continuous refinement
- Equity considerations: Redundant communication channels for rural or remote areas, community liaison officers, and multilingual materials

Singapore Digital Twin Technical Specifications

Virtual Singapore Platform:

- 3D city model with semantic data (building usage, demographics, utilities)
- Dynamic data layers from more than 50 government agencies
- IoT sensor networks (traffic cameras, environmental monitors, smart meters)
- Real-time simulation engines for climate, mobility, infrastructure, energy, and health

Use Case: Flood Simulation

- High-resolution terrain modeling (1-meter resolution digital elevation model)
- Rainfall-runoff calculations accounting for soil saturation, drainage capacity
- Real-time updates during storms showing flood progression
- Enabled targeted flood barriers reducing affected properties by 40%

Estonia X-Road Architecture

Technical Foundation:

- Decentralized data exchange linking more than 1,000 organizations and more than 2,800 services
- Cryptographic signing and encryption ensuring integrity and confidentiality
- 1 billion queries annually
- KSI Blockchain for tamper-evident audit trails
- Digital embassies in Luxembourg are creating mirrored backups

AI Enhancements:

- Anomaly detection for cyber intrusions
- Behavioral analytics establishing baseline normal activity
- Automated threat response isolating compromised systems
- Predictive maintenance monitoring digital infrastructure performance

About

PwC Middle East

At PwC, our purpose is to build trust and solve the most important challenges facing government, businesses and communities. We are on a mission, bringing our community of solvers together to deliver human-led, tech-powered

solutions from strategy through to execution, developing talent and scaling exponential opportunities that deliver sustained outcomes for our clients for future generations. We're a network of firms in 149 countries with nearly 370,000 people who are committed to delivering quality in assurance, advisory and tax services.

Find out more and tell us what matters to you by visiting us at www.pwc.com.

Established in the Middle East for over 40 years, PwC Middle East has 30 offices across 12 countries in the region with around 12,000 people. (www.pwc.com/me).

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

Endnotes

1. United Nations, "'Humanity's Fate Cannot Be Left to Algorithm,' Warns Secretary-General in Security Council Debate on Artificial Intelligence", https://press.un.org/en/2025/sgsm22830.doc.htm

2. Lawrence, M., Homer-Dixon, T., Janzwood, S., Rockstrom, J., Renn, O. and Donges, J.F. (2022). Global polycrisis: The causal mechanisms of crisis entanglement. Global Sustainability, 7, e6. 3 Buirski, A., & Lapsley C. (2024). Towards National Resilience: An Integrated Framework for Strengthening Operational Capabilities. Working paper, University of Portsmouth.

3. Buirski, A., & Lapsley C. (2024). Towards National Resilience: An Integrated Framework for Strengthening Operational Capabilities. Working paper, University of Portsmouth.

4. Cath, C., Wachter, S., Mittelstadt, B., Taddeo, M. and Floridi, L. (2018). Artificial intelligence and the 'good society': The US, EU, and UK approach. Science and Engineering Ethics, 24(2), pp. 505-528.

5. FM Global. 2024 FM Global Resilience Index. Johnston, RI: FM Global; Kimhi, S., Eshel, Y., Zysberg, L., & Hantman, S. (2018). National Resilience and Economic Indicators: Correlation Analysis. Journal of Community Psychology, 46(4), pp. 482–495.

6. Briguglio, L., Cordina, G., Farrugia, N. and Vella, S. (2008). Economic vulnerability and resilience: Concepts and measurements. UNU-WIDER Research Paper No. 2008/55. Helsinki: UNU-WIDER; Hallegatte, S. (2014). Economic resilience: Definition and measurement. World Bank Policy Research Working Paper No. 6852. Washington, DC: World Bank.

7. Ding, J. (2018). Deciphering China's AI Dream: The Context, Components, Capabilities, and Consequences of China's Strategy to Lead the World in AI. Oxford: Future of Humanity Institute; European Commission (2021). Coordinated Plan on Artificial Intelligence 2021 Review. Brussels: European Commission.

8. Graveline, M.-H. and Germain, D. (2022) 'Disaster risk resilience: conceptual evolution, key issues, and opportunities', International Journal of Disaster Risk Science, 13(3), pp. 330-341.https://doi.org/10.1007/s13753-022-00419-0; Boin, A. and Lodge, M. (2016) 'Designing resilient institutions for transboundary crisis management: a time for public administration', Public Administration, 94(2), pp. 289–298. https://doi.org/10.1111/padm.12264

9. McClelland, A.G., Jordan, R., Parzniewski, S., Shaw, D., O'Grady, N. and Powell, D. (2022) 'Post-COVID recovery and renewal through whole-of-society resilience in cities', Journal of Safety Science and Resilience, 3(3), pp. 222–228. https://doi.org/10.1016/j.jnlssr.2022.03.003; Duit, A. (2016) 'Resilience thinking: lessons for public administration', Public Administration, 94(2), pp. 364–380. https://doi.org/10.1111/padm.12182

10. Zuiderwijk, A., Chen, Y.-C. and Salem, F. (2021) 'Implications of the use of artificial intelligence in public governance: a systematic literature review and a research agenda', Government Information Quarterly, 38(3), article 101577. https://doi.org/10.1016/j.giq.2021.101577; Valle-Cruz, D., Criado, J.I., Sandoval-Almazán, R. and Ruvalcaba-Gomez, E.A. (2020) 'Assessing the public policy-cycle framework in the age of artificial intelligence: from agenda-setting to policy evaluation', Government Information Quarterly, 37(4), article 101509. https://doi.org/10.1016/j.giq.2020.101509

11. Medaglia, R., Gil-Garcia, J.R. and Pardo, T.A. (2023) 'Artificial intelligence in government: taking stock and moving forward', Social Science Computer Review, 41(1), pp. 123–140. https://doi.org/10.1177/08944393211034087

12. Wirtz, B.W., Weyerer, J.C. and Geyer, C. (2019) 'Artificial intelligence and the public sector—applications and challenges', International Journal of Public Administration, 42(7), pp. 596–615. https://doi.org/10.1080/01900692.2018.1498103

13. Cao, L. (2023) 'AI and data science for smart emergency, crisis and disaster resilience', International Journal of Data Science and Analytics, 15(3), pp. 231-246. https://doi.org/10.1007/s41060-023-00393-w

14. Davidovic, N. (2023) 'On the purpose of meaningful human control of AI', Frontiers in Big Data, 5, article 1017677. https://doi.org/10.3389/fdata.2022.1017677; Alon-Barkat, S. and Busuioc, M. (2023) 'Human-AI interactions in public sector decision making: "Automation bias" and "Selective adherence" to algorithmic advice', Journal of Public Administration Research and Theory, 33(1), pp. 153-169. https://doi.org/10.1093/jopart/muac007

15. Sigfrids, A., Nieminen, M., Leikas, J. and Pikkuaho, P. (2022) 'How should public administrations foster the ethical development and use of artificial intelligence? A review of proposals for developing governance of AI', Frontiers in Human Dynamics, 4, article 858108. https://doi.org/10.3389/fhumd.2022.858108; Enqvist, L. (2023) '"Human oversight" in the EU artificial intelligence act: what, when and by whom?', Law, Innovation and Technology, 15(2), pp. 508-535. https://doi.org/10.1080/17579961.2023.2245683

16. Kuglitsch, M.M., Pelivan, I., Ceola, S., Menon, M. and Xoplaki, E. (2022). 'Facilitating adoption of AI in natural disaster management through collaboration', Nature Communications, 13(1), article 1579. https://doi.org/10.1038/s41467-022-29285-6; Ghaffarian, S., Taghikhah, F.R. and Maier, H.R. (2023) 'Explainable artificial intelligence in disaster risk management: achievements and prospective futures', International Journal of Disaster Risk Reduction, 98, article 104123. https://doi.org/10.1016/j.ijdrr.2023.104123

17. Guikema, S.D. (2020) 'Artificial intelligence for natural hazards risk analysis: potential, challenges, and research needs', Risk Analysis, 40(6), pp. 1117-1123. https://doi.org/10.1111/risa.13476; Bari, L.F., Ahamed, R., Islam, I., Ahmed, A.H.P., Zobair, T.A., Salehin, S. and Islam, M.R. (2023) 'Potential use of artificial intelligence (AI) in disaster risk and emergency health management: a critical appraisal on environmental health', Environmental Health Insights, 17, pp. 1-14. https://doi.org/10.1177/11786302231217808

18. Cao, L. (2023) 'AI and data science for smart emergency, crisis and disaster resilience', International Journal of Data Science and Analytics, 15(3), pp. 231-246. https://doi.org/10.1007/s41060-023-00393-w

19. Wrange, J., Bengtsson, R. and Brommesson, D. (2024). Resilience through total defence: Towards a shared security culture in the Nordic-Baltic region. European Security, 33(3), pp. 390-411.

20. Dobson, H. (2006). Japan's approach to human security: Norms, power and policy. In: Chandler, D. and Hynek, N. (eds.) Critical Perspectives on Human Security. London: Routledge, pp. 118-130.

21. Rinaldi, S.M., Peerenboom, J.P. and Kelly, T.K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Systems Magazine, 21(6), pp. 11-25

22. Christensen, T. and Lægreid, P. (2007). The whole-of-government approach to public sector reform. Public Administration Review, 67(6), pp. 1059-1066.

23. Wisner, B., Blaikie, P., Cannon, T. and Davis, I. (2004). At Risk: Natural Hazards, People's Vulnerability and Disasters, 2nd edn. London: Routledge.

24. Linkov, I., Bridges, T., Creutzig, F., Decker, J., Fox-Lent, C., Kröger, W., Lambert, J.H., Levermann, A., Montreuil, B., Nathwani, J., Nyer, R., Renn, O., Scharte, B., Scheffler, A., Schreurs, M. and Thiel-Clemen, T. (2014). Changing the resilience paradigm. Nature Climate Change, 4(6), pp. 407-409.

25. Helbing, D. (2013). Globally networked risks and how to respond. Nature, 497(7447), pp. 51-59.

26. Kotsiantis, S.B., 2007. Supervised machine learning: A review of classification techniques. Informatica, 31(3), pp.249-268, http://www.informatica.si/index.php/informatica/article/view/148; Van Engelen, J.E. and Hoos, H.H., 2020. A survey on semi-supervised learning. Machine Learning, 109(2), pp.373-440, https://doi.org/10.1007/s10994-019-05855-6; Radhoush, A., Iftikhar, M., Syed, A.Z. and Hameed, I.A., 2023. An Overview of Supervised Machine Learning Approaches for Condition Monitoring and Fault Diagnosis of Wind Turbines. Energies, 16(3), p.1311, https://www.mdpi.com/1996-1073/16/3/1311; Khan, A., Naseer, M., Hayat, M., Zamir, S.W., Khan, F.S. and Shah, M., 2022. A survey on self-supervised learning: Auxiliary pretext tasks and multi- task learning. arXiv preprint arXiv:2204.01089, https://arxiv.org/abs/2204.01089

27. Bo Li, Junwei Ma, Kai Yin, Yiming Xiao, Chia-Wei Hsu, Ali Mostafavi. Disaster Management in the Era of Agentic AI Systems: A Vision for Collective Human-Machine Intelligence for Augmented Resilience. Cornell University, October 2025, https://arxiv.org/abs/2510.16034

28. Amodei, D., Olah, C., Steinhardt, J., Christiano, P., Schulman, J. and Mané, D. (2016). Concrete problems in AI safety. arXiv preprint arXiv:1606.06565.

29. Helbing, D. (2013). Globally networked risks and how to respond. Nature, 497(7447), pp. 51-59.

30. Luengo-Oroz, M., Hoffmann Pham, K., Bullock, J., Kirkpatrick, R., Luccioni, A., Rubel, S., Wachter, S., Tse, B., Azoulay, A., Bihr, P. and Hong, M.K. (2020). Artificial intelligence cooperation to support the global response to COVID-19. Nature Machine Intelligence, 2(6), pp. 295-297.

31. OECD.AI Policy Observatory. Algorithmic Transparency in the Public Sector—Recommendations for Governments (Dec 3, 2024), https://oecd.ai/en/wonk/documents/16-algorithmic-transparency-in-the-public-sector-recommendations-for-governments-to-enhance-the-transparency-of-public-algorithms.

32. Suresh, M. et.al, AI-Driven Smart Ambulance System for Faster Emergency Response, International Journal for Research Trends and Innovation (2025), https://www.ijrti.org/papers/IJRTI2505247.pdf

33. Defense Logistics Agency (US). Utilization of AI to Illuminate Supply Chain Risk (May 2025), https://www.dla.mil/About-DLA/News/News-Article-View/Article/4186367/utilization-of-artificial-intelligence- ai-to-illuminate-supply-chain-risk/; Farrar, O., How AI Is Reshaping Supply Chains, Harvard Magazine, Aug 13, 2025), https://www.harvardmagazine.com/science-technology/harvard-kennedy-school-artificial-intelligence-supply-chains

34. WeNeedAI.org. The Cascading Cloud Crisis: Why Multiple AI Providers Failed Simultaneously in June 2025.

35. Hall, J.W. and Preston, J. (2021). Systems resilience for multi-hazard environments. Philosophical Transactions of the Royal Society A, 379(2197), 20200355.

36. Oxford Insights (2024). Government AI Readiness Index 2024. London: Oxford Insights; FM Global (2024). 2024 FM Global Resilience Index. Johnston, RI: FM Global; ND-GAIN (2025). ND-GAIN Country Index 2024. Notre Dame, IN: University of Notre Dame Global Adaptation Initiative; International Monetary Fund (2025). World Economic Outlook (WEO) database, April 2025. Washington, DC: IMF.

37. Briguglio, L., Cordina, G., Farrugia, N. and Vella, S. (2008). Economic vulnerability and resilience: Concepts and measurements. UNU-WIDER Research Paper No. 2008/55. Helsinki: UNU-WIDER; Hallegatte, S. (2014). Economic resilience: Definition and measurement. World Bank Policy Research Working Paper No. 6852. Washington, DC: World Bank.

38. Abu Dhabi Media Office, "Abu Dhabi Government Digital Strategy 2025-2027 accelerates AI-native government journey", 30 Sept 30, 2025, https://www.mediaoffice.abudhabi/en/technology/abu-dhabi-government-digital-strategy-2025-2027-accelerates-ai-native-government-journey/

39. https://www.mediaoffice.abudhabi/en/topic/tamm/

40. NEMA. National Situation Room Overview. Australian Government, 2024–25 Annual Report. https://nema.gov.au

41. AU Government News. AI Hazard Prevention Strategy Speeds Emergency Response by 35% (May 2025), https://www.australia.gov.au/news

42. OECD OPSI. Virtual Singapore Case Study. https://oecd-opsi.org

43. Singapore Land Authority. Virtual Singapore Overview. https://www.sla.gov.sg

44. GovTech Singapore. Smart Nation Initiatives. https://www.tech.gov.sg

45. Smart Nation & Digital Government Office. Digital Twin Applications. https://www.smartnation.gov.sg

46. Experion Global. Virtual Singapore and BIM Integration. https://experionglobal.com; SmartCitySS. Urban Mobility and Walkability Improvements. https://smartcityss.com; SmartCitySS. Flood Resilience and Digital Twin Simulations. https://smartcityss.com

47. e-Governance Academy. X-Road Data Exchange Layer. https://ega.ee/projects/x-road/

48. Estonian Information System Authority (RIA). Cybersecurity and CERT-EE. https://www.ria.ee/en/cyber-security.html

49. e-Estonia. Bürokratt – AI Virtual Assistant. https://e-estonia.com/solutions/ai/burokratt/

50. Republic of Estonia. Data Embassy Initiative. https://e-estonia.com/solutions/security-and-safety/data-embassy/

51. Belfer Center for Science and International Affairs. Estonia's Cybersecurity Lessons. https://www.belfercenter.org/publication/estonia-cybersecurity

52. Ott Velsberg, Chief Data Officer of Estonia. Interview on Service Deployment. https://e-estonia.com/news/

53. Belfer Center. Digital Governance Impact. https://www.belfercenter.org/publication/estonia-cybersecurity; Vabamu Digital Governance Report. https://vabamu.ee/en/research

54. National Cyber Security Centre (NCSC). The near-term impact of AI on the cyber threat (Nov 2023), https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat; NCSC Annual Review 2025, NCSC Annual Review 2025, https://www.ncsc.gov.uk/collection/ncsc-annual-review-2025; GCHQ. Pioneering a New National Security: The Ethics of Artificial Intelligence (2024), https://www.gchq.gov.uk/artificial-intelligence/index.html

55. UK Government, Responsible AI Toolkit, March 2024, updated Nov 2024.

56. Collective-Security. What did we learn from NCSC 2025 Annual Review? Nov 2025. Reports 204

57. Defense Innovation Unit, DIU's Thunderforge Project to Integrate Commercial AI-Powered Decision-Making for Operational and Theater-Level Planning (March 5, 2025), Thunderforge Project: https://www.diu.mil/latest/dius-thunderforge-project-to-integrate-commercial-ai-powered-decision-making

58. https://www.pwc.com/m1/en/value-in-motion.html

59. Walker, B., Holling, C.S., Carpenter, S.R. and Kinzig, A. (2004). Resilience, adaptability and transformability in social-ecological systems. Ecology and Society, 9(2), art. 5.

Author

Alex Buirski

Defense, Security and Resilience (DSR)

Partner, PwC Middle East

alex.buirski@pwc.com

WORLD GOVERNMENTS SUMMIT

JOIN THE CONVERSATION

@WorldGovSummit

www.worldgovernmentssummit.org