REPORT

Developing a National Cybersecurity Strategy

FEBRUARY 2026

CENTER FOR
CYBERSECURITY
POLICY AND LAW

Executive Summary

Developing a National Cybersecurity Strategy (NCS) is one of the most important investments a government can make to secure its digital future. As the global digital ecosystem expands, nations that act early to establish a clear, coordinated approach to cybersecurity are far better positioned to safeguard their citizens, economies, and critical infrastructure.

A national cybersecurity strategy offers a shared vision and roadmap for government, industry, and society to work together in managing risks. Without such a framework, efforts are often fragmented, leaving critical gaps that adversaries can exploit. By setting priorities, aligning resources, and clarifying responsibilities, an effective strategy ensures that cybersecurity is not an afterthought but a fundamental pillar of national security, economic resilience, and public trust in the digital age.

While every country faces unique circumstances such as differences in digital maturity, governance structures, economic priorities, and geopolitical realities, the NCS serves as the mechanism through which these factors can be organized into a coherent national approach.

Developing an NCS is a critical first step toward safeguarding a country's digital ecosystem from a complex and rapidly-advancing threat environment. The purpose of an NCS is to coordinate government resources in the most efficient and effective manner possible, addressing national security concerns, economic risks, fraud, and other challenges created by cyber threats.

This paper offers practical, step-by-step guidance for drafting or updating an NCS, a series of policy-pillars that have proven to be effective, a discussion of best practices and similarities among existing NCS, and in-depth review of nine countries' NCS and three relevant international agreements.

The playbook presents the following guidance:

- Determine Risks
- Establish Clear Strategic Objectives
- Engage and Involve the Private Sector and Civil Society
- Design an Effective Governance Structure
- Resource Cybersecurity Appropriately

After following these steps, the playbook recommends the following actions while constructing policy pillars:

- Invest in Cybersecurity Education and Workforce Development
- Raise Technology Standards for a Secure Digital Ecosystem
- Adapt to Artificial Intelligence
- Prepare for Quantum Computing and Emerging Technologies
- Protect Government Systems
- Incorporate Resilience and Response Planning into Critical Infrastructure
- Harmonize Incident Reporting Requirements
- Incorporate Information Sharing Guidelines
- Ensure Flexibility and Review Mechanisms

By developing and implementing an NCS, governments can change the culture surrounding cybersecurity, creating the whole-of-society resilience needed to withstand current threats and adapt to the challenges of the next decade in a manner that fits that country's abilities and culture. In all instances, policymakers should view these strategies not as a static document, but as a living framework that evolves alongside technology, threats, and national priorities.

This document serves to help governments in the process of developing or reviewing their NCSs to understand the key elements to address and actions to prioritize that will improve a country's overall cybersecurity posture.

Table of Contents

Introduction

Developing a National Cybersecurity Strategy (NCS) is one of the most important investments a government can make to secure its digital future. As the global digital ecosystem expands, nations that act early to establish a clear, coordinated approach to cybersecurity are far better positioned to safeguard their citizens, economies, and critical infrastructure. A national cybersecurity strategy offers a shared vision and roadmap for government, industry, and society to work together in managing risks. Without such a framework, efforts are often fragmented, leaving critical gaps that adversaries can exploit. By setting priorities, aligning resources, and clarifying responsibilities, an effective strategy ensures that cybersecurity is not an afterthought but a fundamental pillar of national security, economic resilience, and public trust in the digital age.

The urgency to act has never been greater. Artificial intelligence (AI) is already reshaping the digital ecosystem by accelerating innovation, transforming economies, and creating new efficiencies. But it is also amplifying the scale, speed, and sophistication of cyber threats. As AI technologies become embedded across every layer of society and critical infrastructure, governments must ensure their national cybersecurity posture is equipped to both mitigate emerging risks and harness the opportunities AI presents. An effective NCS provides guidance not only to government institutions, but also to private sector organizations, civil society, and academia, ensuring that all stakeholders can align efforts and respond to evolving threats, including those accelerated by AI and quantum computing.

While every country faces unique circumstances such as differences in digital maturity, governance structures, economic priorities, and geopolitical realities, the NCS serves as the mechanism through which these factors can be organized into a coherent national approach. A strategy enables governments to move beyond fragmented or ad hoc initiatives and instead establish a whole-of-society framework that promotes accountability, fosters collaboration, and ensures that every agency plays a defined role in strengthening national resilience against AI-era threats.

In many cases, protecting public systems is a natural starting point. By securing their own networks and services, governments not only safeguard vital operations but also demonstrate leadership to the private sector and citizens alike. When paired with clear direction for agencies to collaborate with industry, academia, and critical infrastructure operators, a strategy can extend this protection outward, helping to secure the broader digital ecosystem on which modern economies and societies depend. In doing so, a well-communicated strategy can also help normalize cybersecurity awareness across society, embedding it into everyday decision-making and reinforcing a culture in which security is seen as a collective responsibility rather than solely a government function.

This paper begins by giving a playbook for developing an NCS and looking at what needs to go into the document. It recognizes that other resources surrounding drafting an NCS exist; the goal of this paper is not to compete with other resources, but rather to provide governments complementary resources to ensure they are as prepared as possible. There are no one-size-fits-all solutions, but instead the idea is to provide a framework that equips governments with the necessary tools to design, implement, and continuously improve a comprehensive and effective strategy most relevant for their environments. The paper then examines common lessons and best practices from countries around the world, offering practical examples that governments can adapt to their own contexts.

About the Center

The Center for Cybersecurity Policy and Law is a nonprofit 501(c)(6) organization that develops, advances, and promotes best practices and educational opportunities among cybersecurity professionals. The Center provides a forum for thought leadership for the benefit of those in the industry including members of civil society and government entities in the area of cybersecurity and related technology policy. The Center seeks to leverage the experience of leaders in the field to ensure a robust marketplace for cybersecurity technologies that will encourage professionals, companies, and groups of all sizes to take steps to improve their cybersecurity practices.

The Center has been engaging with many stakeholders and has compiled the lessons learned into this playbook. We want to thank Cisco for funding this paper, as well as contributing their knowledge and expertise to the final product.

Playbook

As cyber threats grow more frequent and sophisticated, no nation can afford to be without a clear, up-to-date strategic vision for cybersecurity. Developing an NCS is a critical first step toward safeguarding a country's digital ecosystem. The purpose of an NCS is to coordinate government resources in the most efficient and effective manner possible, addressing national security concerns, economic risks, fraud, and other challenges created by cyber threats. A strategy is not a checklist of what others are doing; it is a tailored, whole-of-government plan for securing both public and private digital ecosystems.

AI is reshaping how cyber threats emerge, evolve, and propagate. It is enabling both defenders and adversaries to act faster, smarter, and at greater scale. From deepfake-driven disinformation to automated network exploitation and synthetic identity fraud, AI is already expanding the threat surface in ways that traditional cybersecurity models were never designed to address. At the same time, AI offers powerful tools for defense like enhancing threat detection, incident response, and resilience. An NCS can lay the foundation for national security, economic stability, and digital sovereignty.

Every country faces different challenges. The maturity of digital infrastructure, the share of publicly versus privately owned critical infrastructure, geopolitical realities, the structure of government, and willingness to cooperate on security issues all impact a nation's cybersecurity posture. For an NCS to succeed, it requires broad buy-in, not just from the private sector, but also from all relevant government agencies. Defense, diplomacy, law enforcement, regulatory, standards, energy, health, and even environmental authorities must collaborate to achieve the strategy's objectives.

This section offers practical, step-by-step guidance for drafting or updating an NCS, drawing on international best practices while recognizing that each country must create its own path. The recommendations are designed to be adaptable across varying levels of cybersecurity maturity, economic development, and governance structures. Rather than prescribing specific technologies or policies, this playbook highlights options for governments to evaluate and adapt based on their national context. By providing high-level yet actionable advice, it equips decision-makers with a clear starting point for building a comprehensive and effective NCS.

Determine Risks

Before a country can craft a meaningful and effective NCS, it must first develop a clear understanding of the risks it faces. Identifying relevant threats, such as malicious cyber actors targeting critical infrastructure, disinformation campaigns that undermine public trust, and systemic weaknesses like an insufficient cybersecurity workforce or an aging information infrastructure, will help define the priorities and shape the objectives of the strategy. AI adds a new and complex dimension to this risk landscape by enabling more sophisticated attacks such as automated vulnerability discovery, AI-generated phishing, and large-scale misinformation, while also introducing dependencies on AI systems that themselves must be secured. Assessing how AI is transforming both offensive and defensive cyber capabilities is now a critical component of any national risk evaluation. Each country's threat landscape is unique, shaped by its digital maturity, geopolitical position, and social and economic context, so it is crucial to perform an extensive review of all relevant national ecosystems.

Engaging public and private sector stakeholders at this early stage can help ensure that the strategy reflects the real challenges faced by those responsible for delivering essential services, securing networks, and protecting data. Their input can validate risk assessments, highlight overlooked vulnerabilities, and build buy-in for the strategy's long-term implementation. A grounded risk assessment ensures that the strategy addresses real vulnerabilities rather than hypothetical concerns, and it creates a foundation for targeted action that protects national interests, public safety, economic vitality, and digital resilience. In addition to informing the creation of an NCS, governments should use the results of risk assessments to regularly inform and educate the public about these risks.

Establish Clear Strategic Objectives

Following a thorough risk assessment, governments developing an NCS should establish clear, high-level strategic objectives. These objectives form the foundation of the strategy, guiding all subsequent actions and investments. They should directly address the most pressing risks identified, or those likely to impact the country over the next 3 to 10 years, and align with broader national development and security goals.

To ensure long-term support and implementation, the objectives must be seen as both necessary and achievable by public and private stakeholders alike. In addition to defining national priorities, strategic objectives also reflect the country's vision and values. These might include promoting a secure and open Internet, enhancing digital resiliency, or supporting innovation and inclusion, among other options.

Align Cybersecurity with National Development and Security Goals

Strategic objectives must be tightly aligned with a country's overarching development and security priorities. Whether a government is focused on accelerating digital transformation, boosting economic competitiveness, strengthening national defense, or expanding public access to services, the cybersecurity strategy should directly support those ambitions. As AI becomes a central driver of national innovation and productivity, cybersecurity objectives must also account for securing AI systems, data pipelines, and algorithms to ensure that the benefits of AI can be realized safely and sustainably.

For example, in countries pursuing e-government initiatives, objectives might prioritize securing digital public services and protecting citizen data. In contexts where national security is a dominant concern, objectives could focus more on resilience against foreign cyber operations or protecting critical infrastructure. Aligning cybersecurity with national priorities ensures political relevance, encourages cross-government cooperation, and helps unlock resources for implementation.

Articulate Vision and Values

Beyond addressing risks and enabling development, strategic objectives also serve as a vehicle for expressing a country's values and long-term vision for cyberspace. Before moving towards drafting, the government should determine if any gaps exist within the cybersecurity culture of the public. For instance, certain countries' private sector organizations tend to not report cybersecurity incidents or ransomware payments, even if they are required by law. Intentionally working on changing the culture can have a lasting impact on a nation's cybersecurity posture.

A well-crafted NCS should reflect how the government views the role of technology and the Internet in society. It might be seen as a tool for open access to information, a driver of inclusive growth, a catalyst for innovation, or a domain requiring public-private collaboration.

For instance, a nation committed to democratic norms might emphasize objectives that protect freedom of expression and privacy online. Clearly articulating these values in the strategy helps guide decision-making, builds public trust, and shapes international engagement, especially as global debates over digital governance and norms intensify.

Engage and Involve the Private Sector and Civil Society

An NCS is only as effective as the engagement of those it most directly affects. Active participation from the private sector, particularly large technology, telecommunications, and cybersecurity firms, is critical throughout the strategy's development. For example, the majority of the Internet and critical infrastructure in many countries is privately owned. The private sector can help not only support but also deliver on the government's cybersecurity objectives and is key to a secure and resilient nation. Equally important, in the drafting of national legislation and implementing rules (e.g., on matters relating to critical infrastructure protection, incident reporting, testing, certification, licensing, resiliency, data residency, sovereignty and other requirements, private sector input is necessary to ensure that they meet their objectives, and not become impractical or overly onerous such that they fail to satisfy the policy intention. International best practices should also be considered for adoption to enable consistency of regulations across jurisdictions. Mechanisms such as requests for information (RFIs), roundtables, public consultations, and closed-door reviews of draft texts can help facilitate meaningful input.

Broad, inclusive engagement ensures that the strategy addresses sector-specific concerns while building widespread support for its implementation. When stakeholders share a common understanding of the risks and agree on the overarching strategic goals, the drafting process becomes significantly more streamlined and effective.

Involving private sector actors, civil society organizations, and key government entities early in the process also helps foster trust-based partnerships for ongoing collaboration. Policymakers must ensure high level buy-in from private and public sector stakeholders in order to ensure that the outcomes are relevant and will be acted upon, instead of falling short immediately after being published. Rather than relying solely on top-down regulatory measures, such partnerships can support more effective, voluntary information sharing and collective problem-solving, and also ensure that different perspectives are taken into consideration. Jointly developing incentives for meeting cybersecurity baselines further ensures that expectations are realistic, proportionate, and broadly supported across sectors.

Design an Effective Governance Structure

After identifying risks, determining strategic objectives, and engaging with the private sector, it is essential to establish a governance structure that supports the successful implementation of the NCS. Without clear organization and accountability, even well-crafted objectives may fail to produce tangible outcomes.

To avoid this, goals should be logically grouped. This often takes the form of grouping by a responsible ministry or agency. For instance, national defense-related objectives may fall under the purview of the defense ministry, while international cooperation may be led by the foreign affairs ministry. Structuring the strategy in this way enables more coherent execution and facilitates coordination.

Equally important is the designation of an overall lead authority with a clear mandate and authority to oversee national cybersecurity efforts. A centralized body, such as the UK's (NCSC), can serve as the focal point for coordination, guidance, and information sharing. This helps ensure that stakeholders across government and the private sector know where to turn for leadership, support, and accountability.

The governance structure must also be grounded in and compatible with the nation's existing legal and regulatory framework. Ensuring legal coherence not only strengthens enforceability and accountability but also allows the NCS to evolve alongside future legislation without creating conflicts or gaps in authority.

The lead authority should also be empowered to coordinate across military, intelligence, and civilian agencies, aligning their capabilities, technologies, and objectives with the broader strategy, while also addressing potential issues regarding an overlap of responsibilities between different agencies. Given the number of institutions with roles in cybersecurity, strong coordination mechanisms are essential to avoid fragmentation and turf issues. A well-designed governance structure ensures that all relevant actors, public and private, are working toward shared national goals with clarity and purpose.

Resource Cybersecurity Appropriately

Policymakers must ensure that the cybersecurity priorities outlined in the NCS are properly resourced, funded, and implemented. Once policies are developed, the corresponding programs need sustained financial, logistical, and personnel support from both national authorities and the private sector. Without adequate investment and attention, the actions envisioned in the strategy's policy pillars will remain unfulfilled, and its goals will not be achieved.

Policy Pillars of a Strategy

While the final content of a nation's NCS must reflect the country's unique priorities, capabilities, and context, certain foundational principles are widely recognized as essential. Regardless of their stage of digital development, all nations seeking to strengthen their cybersecurity posture will find the following core policy components relevant in a strategy.

Invest in Cybersecurity Education and Cyber Workforce Development

An educated, skilled cyber workforce is essential to implementing and sustaining any national cybersecurity strategy. Governments should both invest in cybersecurity education for the entire nation, raising the bar for citizen security, and create more pathways for students to enter the cybersecurity workforce. No matter how ambitious the policy goals or how robust the technological tools, progress is not possible without qualified individuals to lead, support, and scale efforts across sectors. It is important to note that the concept of "qualified individuals" will vary from sector to sector, and the diversity of skills required represents both a unique challenge and opportunity for educational institutions. As AI transforms the nature of work and the cyber threat landscape, nations must also prepare a workforce capable of securing and responsibly leveraging AI technologies. This means agility and flexibility will be the key drivers of success when it comes to empowering the professionals of tomorrow. Building literacy around AI-driven threats and the ethical use of AI in cybersecurity is now a core element of national capacity building. Governments should consider a multi-pronged approach to workforce development that includes:

- Launching comprehensive, whole-of-nation cybersecurity education campaigns designed to upskill all citizens on current cyber risks and equip them with practical strategies to protect themselves and their information online.

- Integrating cybersecurity into national education systems, from primary school to university-level curricula, to build long-term digital awareness and attract students into the field.
- Incorporating AI literacy and security into educational programs—teaching how AI can both enhance cybersecurity (through automation and analytics) and introduce new vulnerabilities (such as model manipulation or data poisoning).
- Expanding technical and vocational training programs, especially those focused on reskilling and upskilling workers in adjacent sectors such as IT, telecommunications, and engineering.
- Ensure crucial trades such as electricians, plumbers, construction supervisors include pivotal digital skills content to ensure that these sectors pro-actively guide and leverage the digital transformation instead of enduring its repercussions.
- Supporting public-private workforce development partnerships, where industry can:
  - Incorporate industry training platforms and content in education programs, customised to align with national curricula.
  - Provide content with large scale "train the trainer" initiatives, to ensure adoption and buy in from educators.
  - Create skills-to-jobs pathways, including apprenticeships, internships, and more cybersecurity job opportunities.
  - Upskilling of SMEs and non-tech sectors on digital transformation (IoT, Cyber, AI) and how to leverage the evolution of the world of work to reinforce resilience and competitiveness.
  - Targeted communication towards SMEs and non-tech sector employers around the need for skills based hiring.
- Investing in diversity and inclusion efforts to broaden the talent pipeline and ensure that the workforce reflects the full population, improving both equity and resilience.
- Adopting international certification and professional standards for cybersecurity roles to ensure consistency, credibility, and career mobility across government, critical infrastructure, and private sector roles.

Additionally, governments can incentivize growth in the cyber workforce by aligning job creation efforts with national digital transformation initiatives, promoting cybersecurity not only as a security imperative but also as an engine for economic development. Developing expertise at the intersection of AI and cybersecurity can further position a country as a regional leader, both in defending against AI-enabled threats and in innovating secure, responsible AI systems. A well-developed cyber workforce strategy can also serve as a foundation for regional leadership and international cooperation in the cyber domain.

Raise Technology Standards for a Secure Digital Ecosystem

Developing a national strategy is not only about high-level policies, but is also about empowering those on the front lines of cybersecurity with the tools, guidance, and mandates they need to succeed. Defenders working today across government agencies, critical infrastructure, private sector entities, and academia must be equipped to make measurable improvements in national cyber resilience.

A critical component of raising technology standards is managing and reducing "technical debt"—the accumulation of outdated, insecure, or poorly maintained technology that hinders modernization and increases cyber risk. End-of-life (EoL) systems are among the most severe forms of technical debt. When software or hardware reaches EoL, it no longer receives vendor updates, patches, or security support, leaving it inherently vulnerable to exploitation. In 2020, nearly half of business network infrastructure globally was estimated to be obsolete or aging, making it harder to secure and easier to exploit.[1] When legacy systems are allowed to persist without adequate updates or integration with newer infrastructure, they create vulnerabilities that adversaries can exploit.

A robust NCS should explicitly include mechanisms for identifying and addressing legacy systems across the public and private sectors before they become cyber liabilities.[2] This includes funding and incentives for system modernization, mandates for timely decommissioning or replacement of EoL assets, and transparent processes for reporting on the age and security posture of critical systems. Proactively addressing EoL risk is essential to ensuring that national infrastructure does not depend on obsolete, unsupported technologies. By tackling technical debt, governments can accelerate the adoption of secure architectures, promote interoperability, and ensure that new technologies are built upon a resilient, standardized foundation. Doing so will raise the overall baseline of cybersecurity across the national ecosystem.

To promote a secure digital environment, the NCS should establish clear expectations and minimum standards for cyber hygiene and operational security across all sectors, either directly or indirectly tied to international standards. Using international standards as the means to demonstrate the specific national objectives have been met will ensure harmonization around the world, and ease a potential burden on private sector entities hoping to comply with standards. Standards like ISO 15408, 27001, 29147, SOC 2, and many others are common-ground standards that raise the bar for cybersecurity. Similarly,

[1] https://www.wpi-strategy.com/end-of-life-tech-report
[2] https://www.wpi-strategy.com/end-of-life-tech-report

an NCS should strive to leverage commercial standards where feasible. Using international and commercial standards will not only foster harmonization, easing the regulatory burden and lowering the costs of delivering technology for private sector entities. Countries should investigate which standards most support their national goals, including standards surrounding:

- The identification and timely decommissioning of EoL systems that no longer receive vendor support and pose critical security risks.
- The implementation of Multi-Factor Authentication (MFA) for all systems handling sensitive or mission-critical data.
- Establishing consistent patch and vulnerability management protocols to reduce exploitable weaknesses across networks.
- Developing national guidance for threat detection and incident response, aligned with best practices and updated regularly to reflect emerging threats.
- Encouraging the use of secure-by-design and secure-by-default principles in technology procurement and development.
- Providing technical assistance and resources—especially to small and medium enterprises (SMEs) and under-resourced public institutions—to implement security measures effectively.

By explicitly integrating EoL management into technology standards, the NCS can ensure that cybersecurity resilience is not undermined by aging infrastructure. EoL planning creates a predictable, secure lifecycle for digital assets, preventing outdated technologies from becoming systemic vulnerabilities.[3]

Raising technology standards is fundamental to building a resilient and trustworthy digital ecosystem. A National Cybersecurity Strategy that prioritizes modernization, includes proactive EoL management, addresses technical debt, and aligns with international and commercial standards creates a unified framework for secure growth. By embedding strong, consistent expectations for security across sectors, governments can not only reduce systemic vulnerabilities but also foster innovation and global cooperation. Ultimately, elevating technology standards ensures that national resilience is not a one-time achievement, but a sustained, adaptive effort in the face of evolving threats.

[3] https://blogs.cisco.com/gov/critical-infrastructure-technical-debt

Adapt to Artificial Intelligence

Artificial intelligence is no longer an emerging technology; its impact is already being felt globally. AI carries significant security implications for both defenders and attackers, reshaping how digital systems are built, used, and targeted. The cybersecurity workforce must adapt quickly to these realities, leveraging the benefits of AI while mitigating its risks. An effective NCS should not treat AI as an isolated issue but instead embed AI security principles throughout the strategy. Preparing for an AI-driven future means developing an AI-ready workforce, deploying AI-enabled tools to strengthen defenses, anticipating increasingly sophisticated AI-enabled attacks, and addressing vulnerabilities that may arise from the incorporation of AI into systems and processes.

Strong AI governance is also essential. Governance frameworks must safeguard fundamental rights like privacy, equity, cybersecurity, and human dignity, while still enabling the responsible growth of AI technologies. This requires principles that emphasize social responsibility, maintain high levels of cybersecurity, ensure system reliability and human oversight, and promote inclusive, multistakeholder design. Governments, businesses, academia, civil society, and international organizations all have a role to play in shaping this environment.[4]

Striking the right balance is crucial. An NCS must both promote AI development, which is in the public's interest, and ensure that AI technologies are deployed safely and responsibly. Some governments might also need to consider how their approach to AI in an NCS aligns with their National AI Strategy. Overall, governments can harness the promise of AI while minimizing its risks, ultimately creating a more secure and resilient digital ecosystem.

Prepare for Quantum Computing and Other Emerging Technologies

Quantum computing and other emerging technologies have the potential to fundamentally transform the cybersecurity landscape. Quantum computing is "an emergent field of computer science and engineering that harnesses the unique qualities of quantum mechanics to solve problems beyond the ability of even the most powerful classical computers."[5] While it offers significant benefits in fields such as healthcare, engineering, and cybersecurity itself, it also poses severe risks.

[4] https://digiamericas.org/wp-content/uploads/2025/08/AI-Governance-in-Latin-America_EN.pdf
[5] https://www.ibm.com/think/topics/quantum-computing

Cryptographically-relevant quantum computers (CRQCs) could break today's encryption standards in minutes or even seconds, tasks that would take classical computers years or decades.[6] This vulnerability makes the development of post-quantum cryptography (PQC), algorithms resistant to CRQCs, an urgent priority.[7] Without timely adoption, adversaries could exploit "harvest now, decrypt later" strategies, storing encrypted data today with the intention of decrypting it once CRQCs become available. Governments must begin investing in PQC and other quantum-resilient technologies now to safeguard critical systems, protect sensitive information, and ensure a smooth transition to a quantum-enabled future.

Protect Government Systems

Every government agency must prioritize cybersecurity, regardless of its perceived relevance to digital threats. In many countries, only a limited number of entities may have explicit cybersecurity mandates, making it even more important that an NCS establish a whole-of-government approach. This requires equipping all agencies, whether focused on defense, healthcare, transportation, or environmental policy, to anticipate and respond to cyber threats.

Governments should lead by example. Proactive investment in cybersecurity not only strengthens national defenses but also demonstrates to the private sector the tangible benefits of doing so. By adopting international best practices regarding secure procurement practices, building resilient supply chains, and embedding security into government operations, public institutions can model the kind of forward-looking behavior that inspires confidence, saves money in the long term, and deters adversaries.

National strategies should remain flexible and context-driven, recognizing that approaches must be adapted to each country's market realities and level of cybersecurity maturity. Regular supply chain assessments and the identification of trusted vendors are key steps in protecting government systems while maintaining space for innovation. In addition to technical cybersecurity approaches, non-technical factors may be relevant to assess the overall trustworthiness of a vendor or ecosystem. Countries should center partnership efforts for critical ICT supply chains with technology providers from like-minded countries with shared fundamental values like democracy and the rule of law. By setting a strong standard for their own systems, governments create both a safer public sector and a benchmark for private-sector organizations to follow.

[6] https://postquantum.com/post-quantum/crqc/#definition-of-crqc
[7] https://postquantum.com/post-quantum/crqc/#definition-of-crqc

Incorporate Resilience and Response Planning Into Critical Infrastructure

Protecting critical infrastructure is a cornerstone of an NCS. These sectors, such as energy, telecommunications, water, healthcare, finance, and transportation, are vital to national security, economic stability, and public safety. Cyber incidents in these areas can have detrimental, cross-sector impacts. To mitigate these risks, the NCS should provide guidance to critical infrastructure operators on implementing robust resilience and response planning. This includes:

- Risk assessments and business continuity planning tailored to cyber threats.
    - The NCS should encourage, regulate, or incentivize the adoption of recognized, risk-based frameworks such as C2M2 or ISO 27001, while providing flexibility on selecting which standard is most appropriate to their risk environment.
- Incident response plans, regularly tested through exercises and drills.
- Sector-specific resilience guidelines in line with international best practices and in coordination with relevant regulators and industry bodies.
- Reporting for significant cyber incidents to national authorities, with mechanisms for rapid coordination and support.
- Public-private coordination mechanisms, such as information sharing forums or joint response teams, to streamline responses during emergencies.
- Integrating OT security and cybersecurity with IT security.
- Requiring appropriate product testing and certification for critical digital products and services to ensure they meet baseline security standards before deployment, either through accredited external labs available globally or other testing and certification mechanisms, with the recognition of the audit results and test reports of such accredited labs to avoid unnecessary duplicative local re-testing or re-certification. This will reduce systemic vulnerabilities introduced through insecure technologies.

In addition to investing in the previous ideas, an NCS should focus on the importance of establishing Security Operations Centers (SOCs). The SOC is the nerve centre for detecting, responding and mitigating cyber threats in near real time. Without SOCs and SOC modernisation, organisations risk falling behind adversaries who are increasingly automating and accelerating their attacks. A modern SOC should not only leverage automation and AI, but also be measured against key operational metrics such as Mean Time to Detect (MTTD) and Mean Time to Triage (MTTT). Embedding these requirements into regulatory and policy frameworks would drive greater accountability, enhance visibility, and ensure that organisations are continually improving their defensive posture.

The goal should be to ensure that critical services can withstand, recover from, and adapt to cyber disruptions. A national strategy should prioritize resilience, focusing on national preparedness and public trust.

Harmonize Incident Reporting Requirements

Building on national resilience and response planning, incident reporting is a tactic being used by many countries to support the NCS's goals. A core objective of most NCS frameworks is to strengthen the overall cybersecurity ecosystem of a country, not just the defenses of individual organizations. To achieve this, timely and structured communication is essential. Providing opportunities for organizations to share information on cyber incidents with a designated central authority enables other stakeholders to anticipate, prepare for, and mitigate similar threats. For some countries or sectors, mandatory information sharing requirements might be necessary to ensure adequate levels of sharing. For others, providing spaces and resources to facilitate sharing are likely enough, given the incentive structure of the sharing itself. Lessons learned from one incident can serve as early warnings for others, thereby enhancing collective resilience.

While approaches vary across countries, the key is to develop precise and transparent guidelines. Complexity caused by duplicative and inconsistent reporting requirements can ultimately cause businesses to divert resources away from mitigation, response and recovery from the incident itself to compliance. Countries should be looking to emerging international norms on reporting, and align on the thresholds, timelines and content of reporting. This should include a significance threshold for reporting that is tied to in-country impact and starting the clock for reporting only once the organisation has a reasonable degree of certainty the incident occurred. Moreover, to streamline the process, there should be a single national entry point for reporting and a harmonised reporting template. Establishing such clarity not only ensures compliance but also maximizes the utility of incident reporting as a tool for national cybersecurity resilience.

Incorporate Information Sharing Guidelines

In addition to required incident reporting in certain situations, governments should incentivize cyber threat information sharing. Public and private sector organizations all benefit from information sharing, whether through formal information like information sharing and analysis centers (ISACs), information sharing and analysis organizations (ISAOs), or other less structured mechanisms. By pooling threat information, organizations can be better prepared against threats that have not yet reached them. Information sharing must not be a one-way channel. Governments must ensure that information sharing is bidirectional: while organizations share with authorities, those authorities should, in turn, disseminate anonymized threat intelligence, best practices, and remediation guidance back to the reporting entities and other relevant stakeholders in a timely manner. This reciprocal exchange not only incentivizes compliance but also ensures that the system strengthens defenses across the entire ecosystem rather than creating a regulatory burden without tangible benefit.

National defenders must also be enabled to collaborate, detect and respond to cyber threats in real time. This includes facilitating cross-sector information sharing, establishing sector-specific Computer Security Incident Response Teams (CSIRTs) and integrating threat intelligence from both domestic and international sources. Ultimately, a secure digital world depends on active, capable defenders. A strong NCS should provide the policies, incentives, and infrastructure necessary to turn security recommendations into security realities across the entire digital ecosystem.

Information sharing also helps reduce the stigma surrounding cyber incidents. When organizations establish structured relationships with regulators and cybersecurity authorities, they are more likely to engage constructively during crises. This cooperation ensures that affected entities can access government support, including expertise in areas such as ransomware response and recovery, to mitigate and contain the damage during an incident.

Ensure Flexibility and Review Mechanisms

A successful NCS must be a living document that is responsive to a rapidly evolving threat landscape and emerging technologies such as AI, quantum computing, and the Internet of Things (IoT). To remain relevant and effective, the strategy should include periodic review processes or specific deadlines for action items to evaluate progress, adapt goals, and incorporate lessons learned. By designing the strategy with built-in mechanisms for flexibility and accountability, countries can stay ahead of emerging risks while continuously improving their national cybersecurity posture.

Similarities and Best Practices Across National Cybersecurity Strategies

After reviewing NCSs from countries spanning the globe, the Center for Cybersecurity Policy and Law (Center) distilled relevant cross-cutting lessons for policymakers as described in the previous section. The Center first identified common themes across national approaches, then highlighted best practices that can serve as practical guidance for those responsible for developing or updating an NCS.

Although each country operates in a distinct political and economic context, the experiences of others provide valuable insights that can be adapted to local conditions. Common priorities that emerge include:

- Protection of critical infrastructure and enhancement of national resilience.
- Establishment of centralized coordination mechanisms.
- Promotion of strong public–private partnerships.
- Advancement of workforce development and research and innovation.

This section builds on the review of national cybersecurity strategies and international frameworks presented in the case studies in the annex. While the annex provides the detailed country-level analysis, the focus here is on distilling cross-cutting lessons that are most relevant for policymakers.

Protecting Critical Infrastructure, Enhancing Resilience, and Deterring Adversaries

While NCSs can cover a wide range of topics, protecting critical infrastructure (CI), enhancing national resilience, and deterring adversaries should be a top priority. All of the countries surveyed provide some structure around all three. Canada's *Detect and Disrupt Cyber Threat Actors*, the United States' *Defend Critical Infrastructure* and *Disrupt and Dismantle Threat Actors*, and Australia's *Protected Critical Infrastructure* and *Strong Businesses and Citizens* are just a few examples of the many countries which recognize the importance of protecting CI and promoting national resilience.

The CI sectors, such as energy, health, transportation, and others, play an extremely important role in countries' economic, physical security, and cybersecurity ecosystems. By prioritizing their protection in an established strategy, a government can ensure adequate resources are being applied. For example, Australia provides specific legislative focus on protecting critical infrastructure entities across 11 sectors as well as enhanced regulatory oversight of "systems of national significance" – a smaller subset of critical infrastructure assets, most crucial to the nation by virtue of their interdependencies across sectors and potential for cascading consequences if disrupted.[8] Japan also prioritizes protecting CI and enhancing resilience by aligning these goals with their digital transformation goals. Similarly, Rwanda's NCS highlights the importance of making infrastructure resilient and secure against cyber threats in supporting the country's economic and social development goals. Critical infrastructure operators, law enforcement agencies, sector regulators, key cybersecurity stakeholders, and more all saw the importance of cybersecurity as a key enabler for economic growth and social mobility.[9]

A shared priority across the nine national cybersecurity strategies outlined in the annex is the enhancement of national resilience, particularly in the areas of incident response and recovery. Each country emphasizes the importance of maintaining essential services during cyber disruptions and rapidly restoring functionality after an incident.

Strategies include:

- Strengthening national response frameworks.
- Expanding the capabilities of Computer Security Incident Response Teams (CSIRTs).
- Conducting regular cyber exercises.
- Investing in sector-specific contingency planning.

Alongside resilience, these countries also prioritize deterring malicious cyber activity. This includes efforts to improve attribution capabilities, coordinate more effectively with domestic and international law enforcement, and apply diplomatic or economic pressure to hold cyber adversaries accountable. Some countries also integrate active defense measures into their posture, signaling a willingness to disrupt or preempt cyber threats where legally and strategically appropriate. Together, these approaches reflect a shift toward more proactive, whole-of-nation cybersecurity postures.

[8] https://www.google.com/url?q=https://www.paloaltonetworks.com/blog/2022/07/australias-critical-infrastructure-reforms/&sa=D&source=docs&ust=1758047696543965&usg=AOvVaw09yjlnHCjxsk8tqVYziCBg
[9] https://cyber.gov.rw/index.php?eID=dumpFile&t=f&f=427&token=6375c4cab9b091a9747cd9f07f8dc616ba825245

Strong Public-Private Partnerships

As many national strategies explicitly acknowledge, cybersecurity goals cannot be achieved without the active involvement of the private sector. Large technology and cybersecurity firms, privately owned critical infrastructure companies, and the thousands of small and medium enterprises (SMEs) all play a critical role in protecting a country's digital environment.

Developing an NCS requires recognizing that cybersecurity is inherently a collaborative effort. Due to the interconnectivity of the current digital world, when one system is compromised, it can quickly spread to others. To address this, governments have implemented a range of measures to strengthen public-private cooperation, including information sharing, sector-specific guidance, voluntary standards, and structured engagement platforms.

Many countries have already taken concrete steps to operationalize this collaboration. In the U.S., the Cybersecurity and Infrastructure Security Agency (CISA) launched the Joint Cyber Defense Collaborative (JCDC)[10] to "integrate cyber defense planning and operations across the Federal Government and with the private sector and international partners."[11] Australia committed to investing in a "Threat Sharing Acceleration Fund" to support the development of sector-specific ISACs in Australia.[12]

The Australian Signals Directorate's (ASD) Cyber Threat Intelligence Sharing (CTIS) platform allows ASD to disseminate observable indicators of compromise to participating organizations rapidly, in addition to bi-directional information sharing.[13]

In Colombia, the government has built coordination mechanisms with the telecom and banking sectors to advance sector-specific resilience, guided by its core principle of multisectoral collaboration.[14]

In Rwanda, all citizens and users are recognized as part of the security chain, with calls for awareness, digital hygiene, reporting, and cooperation with national programs. Public

[10] https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative

[11] https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

[12] https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf

[13] https://www.cyber.gov.au/about-us/view-all-content/news-and-media/join-the-cyber-threat-intelligence-sharing-service-through-sentinel

[14] https://www.mintic.gov.co/portal/715/articles-403023_recurso_2.pdf

institutions, SMEs, and technology providers are encouraged to adopt risk management practices, engage in capacity building, and partner in innovation ecosystems.

The Netherlands' NCS is guided by the vision that "people and businesses should be able to benefit fully from participation in the digital society" and that "security is an essential part of this."[15] Recognizing the growing dependence on digital technologies and connections, the strategy frames cybersecurity as a critical investment in the country's future, something that the public and private sectors must work together on to ensure the country moves in the right direction.

These examples demonstrate that strong, sustained public-private partnerships are essential for building a resilient cybersecurity ecosystem and should be a cornerstone of any effective national strategy.

Workforce Development and R&D Investment

In addition to short- and medium-term investments in cybersecurity capabilities, many national strategies emphasize long-term commitments to workforce development and research and development (R&D). While initiatives such as critical infrastructure protection, national resilience, and public-private partnerships are essential, none can succeed without a competent, well-resourced, and self-sustaining cyber workforce.

Several countries highlight workforce development as a foundational pillar of their strategy, with a focus on expanding STEM education, supporting academic research, and establishing robust training programs. These programs include:

- Australia is implementing dedicated cyber skills initiatives through partnerships between government and academia.
- Japan is cultivating highly skilled cybersecurity professionals as part of its broader digital transformation goals.
- Colombia is investing in training programs to build cyber capabilities within the government and defense sectors.
- The Netherlands has as one of its core pillars to enhance the cybersecurity labor market, education, and the cyber resilience of the public.
- In Rwanda, education institutions, researchers, and training bodies are asked to integrate cybersecurity into curricula, support research and innovation, and develop relevant certifications and professional pathways.

[15] https://english.nctv.nl/topics/netherlands-cybersecurity-strategy-2022-2028/documents/publications/2022/12/06/the-netherlands-cybersecurity-strategy-2022-2028

In parallel, long-term investment in R&D is another recurring theme across national strategies. While today's cyber threats are already severe, the risks of tomorrow could be even greater if defenders fail to keep pace with or outpace attackers. Sustained investment through government grants, public-private collaboration, and international cooperation is critical for staying ahead in a field defined by rapid technological change and innovation. Together, these efforts to build a skilled cyber workforce and invest in forward-looking R&D form the foundation for sustainable, long-term national cybersecurity resilience.

International Capacity Building and Cooperation

The online world is borderless. In order to adequately defend against threat actors, which may themselves be a multinational, countries must work together. Bilateral and multilateral engagement, in forums both dedicated to cybersecurity and not, is critical. Adhering to international norms and engaging with partners through formal and non-formal means enables countries to grow together, rather than having to do so independently.

Singapore has committed over $30 million over five years to establish the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE), highlighting their continued commitment to engaging with key international partners. Japan's strategy and action plan showcase their commitment to promoting capacity-building in the Association of Southeast Asian (ASEAN) region, while advocating for a free, open, and secure cyberspace. Canada, the U.S., and Colombia are all active players in the Americas, promoting multi-lateral standards and supporting resilience in Latin America through organizations like the Organisation of American States (OAS), among others.

This shared commitment to international cooperation not only enhances collective resilience but helps establish a common understanding of responsible state behavior in the online world. As threat actors exploit jurisdictional gaps and differences in national capabilities, unified efforts can close these vulnerabilities and reduce duplication of effort. Regulatory harmonization, especially in areas like data protection, incident reporting, and critical infrastructure standards, can further streamline cross-border coordination and reduce compliance burdens for multinational firms. Furthermore, consistent collaboration can lead to better interoperability between nations' cyber defenses and more timely sharing of threat intelligence.

Centralized Cybersecurity Coordination and Interagency Coordination

To ensure cohesive national responses to cyber threats, many countries have established centralized leadership models through National Cybersecurity Centers or equivalent bodies. These entities serve as the primary coordinators for cybersecurity policy, threat response, and information sharing across government and with the private sector. Effective interagency coordination mechanisms help streamline decision-making, reduce duplication, and enable faster, more unified responses to incidents.

The United Kingdom's National Cyber Security Centre (NCSC) is a great example, offering proactive threat intelligence and technical guidance to both public and private stakeholders. Canada exemplifies a clear division of responsibilities, with the Canadian Centre for Cyber Security leading technical operations and individual federal departments managing sector-specific risks. In Colombia, central oversight is achieved through coordination between its CSIRT and the Ministry of Defense, helping align national defense and civilian cyber functions. And in Singapore, the Cyber Security Agency of Singapore (CSA) was set up as the central agency to oversee and coordinate all aspects of cybersecurity for the nation, including following through on the country's NCS. These centralized models demonstrate the value of empowered institutions in achieving a coordinated, whole-of-nation approach to cybersecurity.

Conclusion

A well-designed National Cybersecurity Strategy is no longer optional—it is a foundational element of national security, economic stability, and societal resilience. Experiences from around the world demonstrate that effective strategies share common features: clear objectives, centralized coordination, strong public-private partnerships, investment in workforce and innovation, and active international engagement. Yet no single model can be copied wholesale. Each nation must tailor its approach to its unique context while planning for a rapidly evolving threat environment.

Technologies such as AI and quantum computing are already reshaping the cyber domain, underscoring the need for strategies that are flexible, forward-looking, and actionable. Protecting government systems, fostering collaboration across agencies, and building trust with the private sector are not just defensive measures, they are essential for securing the entire digital ecosystem. As AI accelerates both opportunity and risk, nations that embed AI awareness, governance, and security throughout their cybersecurity strategies will be best positioned to innovate safely and defend effectively in the years ahead. The AI era demands not just stronger defenses, but smarter, adaptive strategies that can evolve as quickly as the technologies they are designed to protect.

Countries that have strategies need to make sure they are reviewing them regularly and have a plan to update and refresh them. Many of the countries without a strategy have smaller and underfunded national budgets and agencies, but those cases are exactly the countries that need a strategy most. Nations that delay risk falling behind adversaries and leaving critical systems exposed.

By developing and implementing an NCS, governments can create the whole-of-society resilience needed to withstand current threats and adapt to the challenges of the next decade in a manner that fits that country's abilities and culture. In all instances, policymakers should view these strategies not as a static document, but as a living framework that evolves alongside technology, threats, and national priorities. This document serves to help governments in the process of developing or reviewing their NCSs to understand the key elements to address and actions to prioritize that will improve a country's overall cybersecurity posture.

Annex

National Cybersecurity Strategies: Case Studies

Australia

Australia released its 2023-2030 Cyber Security Strategy[16] in November 2023 as a roadmap to help realize the Australian Government's vision of becoming a world leader in cybersecurity by 2030. The strategy seeks to improve the country's "cyber security, manage cyber risks, and better support citizens and Australian businesses to manage the cyber environment around them."[17] The Australian government conducted thorough consultation processes with the private sector during the process of developing their national strategy. Following the public consultation period and consultation events, the published strategy emerged with the following 6 "shields", or pillars which build upon each other: Strong Businesses and Citizens; Safe Technology; World-Class Threat Sharing and Blocking; Protected Critical Infrastructure; Sovereign Capabilities; and Resilient Region and Global Leadership. The Australian Government will work with industry to reinforce these shields and build its national cyber resilience.[18] The following sections outline the process Australia underwent to develop its strategy, elaborate on the strategy, and explain how Australia is holding itself accountable regarding implementation.

Strategy Development

Australia's National Cyber Security Strategy offers a valuable case study in how a government can identify key risks and align national efforts across sectors. Recognizing the growing complexity of the cyber threat landscape, Australia began its strategy development by conducting a comprehensive risk assessment to determine which assets, sectors, and vulnerabilities posed the greatest danger to national security, economic stability, and public trust.

[16] https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/2023-2030-australian-cyber-security-strategy

[17] https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/2023-2030-australian-cyber-security-strategy

[18] https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf

Following their risk assessment, the Australian government placed strong emphasis on collaboration with the private sector, particularly those managing critical infrastructure. Through the Strategy Discussion Paper[19], which received over 330 submissions, and structured consultations and joint working groups, the government was able to better understand the benefits and potential drawbacks of the proposed strategy from the private sector perspective. The Discussion Paper highlights that "Like Australia's cybersecurity, the Strategy will be a team effort, building on our history of collaborative cyber resilience".[20] Due to the mutual understanding of the collaborative nature of this effort, they were able to integrate private-sector insights, operational realities, and innovative solutions into the national strategy. This cooperative model ensured that the strategy was not only technically sound and risk-informed, but also actionable and aligned with industry capabilities and incentives.

Strategy

Australia's 2023–2030 Cyber Security Strategy outlines an ambitious vision to become a world leader in cyber security by the end of the decade. Rather than framing cyber security as a purely technical challenge, the Strategy redefines it as a whole-of-nation priority, one that requires the active engagement of individuals, businesses, government, and international partners alike. At its core is a commitment to protecting Australians by managing cyber risks, supporting victims, and building a cyber-resilient society. The Strategy's strategic vision centers around three goals: shifting from a technical topic to a whole-of-nation endeavour; delivering tangible action on cybersecurity issues that matter to most Australian communities and business; and harnessing the whole country to tackle cyber problems, enabled by stronger public-private partnerships.[21] To achieve this, the Australian Government introduced a framework built around six "cyber shields", with each representing a distinct yet interconnected layer of national defense.

These six shields—*Strong businesses and citizens, Safe technology, World-class threat sharing and blocking, Protected critical infrastructure, Sovereign capabilities,* and *Resilient region and global leadership*—form the backbone of Australia's approach. Within each shield, the Strategy provides the following objectives to help them achieve their 2030 vision:[22]

[19] https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/2023-2030-australian-cyber-security-strategy-discussion-paper

[20] https://www.homeaffairs.gov.au/reports-and-pubs/files/2023-2030_australian_cyber_security_strategy_discussion_paper.pdf

[21] https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/2023-2030-australian-cyber-security-strategy

[22] https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf

1. **Strong Businesses and Citizens**
    a. Support small and medium businesses to strengthen their cybersecurity.
    b. Help Australians defend themselves from cyber threats.
    c. Disrupt and deter cyber threat actors from attacking Australia.
    d. Work with industry to break the ransomware business model.
    e. Provide clear cyber guidance for businesses.
    f. Make it easier for businesses to access advice and support after a cyber incident.
    g. Secure our identities and provide better support after a cyber incident.
    h. Secure our identities and provide better support to victims of identity theft.
2. **Safe Technology**
    a. Ensure Australians can trust their digital products and software.
    b. Protect our most valuable datasets.
    c. Promote the safe use of emerging technology.
3. **World-class Threat Sharing and Blocking**
    a. Create a whole-of-economy threat intelligence network.
    b. Scale threat-blocking capabilities to stop cyber attacks.
4. **Protected Critical Infrastructure**
    a. Clarify the scope of critical infrastructure regulation.
    b. Strengthen cybersecurity obligations and compliance for critical infrastructure.
    c. Uplift cybersecurity of the Commonwealth Government.
    d. Pressure-test our critical infrastructure to identify vulnerabilities.
5. **Sovereign Capabilities**
    a. Grow and professionalise our national cyber workforce.
    b. Accelerate our local cyber industry, research, and innovation.
6. **Resilient Region and Global Leadership**
    a. Support a cyber resilient region as the partner of choice.
    b. Shape, uphold, and defend international cyber rules, norms, and standards.

Together, they aim to make it easier for citizens and businesses to access guidance, respond to cyber incidents, and protect their identities. By embedding cyber security across sectors and scaling up threat intelligence sharing, Australia is creating a more agile and responsive national posture.

Implementation and Accountability

Through the phased implementation outlined in the accompanying Action Plan[23], Australia is advancing a multi-year roadmap that strengthens foundational protections (Horizon 1), scales cyber maturity across the economy (Horizon 2), and positions the country at the global forefront of cybersecurity innovation and leadership (Horizon 3). Constructed in collaboration with key stakeholders in the public and private sectors, the Action Plan provides concrete action items tied to key goals laid out in each "shield" of the Strategy. Each action item is assigned to a "Lead Agency", with other "Contributing Agencies" where applicable.[24] Each of the 20 action items, each with at least several sections connecting to the Strategy seeks to ensure the Strategy's goals are met within each specified Horizon. By assigning different agencies responsibilities, the Action Plan ensures accountability within the whole-of-government approach.

Canada

Canada's 2025 National Cybersecurity Strategy[25] highlights Canada's commitment to secure Canada's digital future.[26] The Strategy hopes to ensure that "cyberspace is safe, open and secure for all Canadians."[27] To do this the government provides two overarching principles. The first is a whole-of-society approach, engaging in partnerships with other levels of government, Indigenous communities, the private sector, academia, and civil society to be more resilient against malicious cyber actors. The second principle is "Agile Leadership". They state that "it is critical for Canada to be equipped to respond to emerging risks as they occur…therefore Canada's cyber security solutions will be deployed in close collaboration with partners and stakeholders" which will be laid out in specific action-plans every few years. With these overarching principles covering three pillars that each have their own strategic objectives, Canada's National Cybersecurity Strategy is ensuring Canada grows as one of the world's leaders in cybersecurity while protecting its citizens.

Strategy Development

Canada's National Cyber Security Strategy builds upon a strong foundation of cyber strategies. Canada's 2018 National Cyber Security Strategy established the Canadian Centre

[23] https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy-action-plan.pdf
[24] https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy-action-plan.pdf
[25] https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2025/ntnl-cbr-scrt-strtg-2025-en.pdf
[26] https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2025/index-en.aspx
[27] https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2025/index-en.aspx

for Cyber Security (Cyber Centre)[28] and the National Cybercrime Coordination Centre (NC3)[29] under the Royal Canadian Mounted Police. Following this progress, the Canadian government performed an assessment to understand what risks remained. Varying levels of cyber maturity, a lack of a comprehensive awareness of the cybersecurity risk environment, disparate approaches in various security capabilities, and issues surrounding the culture of cybersecurity, among others, comprise the gaps found.[30] And these risks are only exacerbated by the current environment which is rapidly changing. Technology modernization, cybersecurity incidents affecting government and private sector operations, ESG commitments, and the future of work are all challenges currently facing Canadians. With this environment and set of risks in mind, the process for developing an updated strategy could begin.

The vision for the new Strategy involved "building a world-class, sustainable and resilient Government of Canada (GC) to reduce cyber security risks so that federal departments and agencies can enable secure and reliable digital service delivery."[31] Following consultation with key stakeholders, the GC establishes four strategic objectives regarding the updated strategy: *Articulate cyber security risks and their business impacts for effective, action-oriented and accountable decision-making; Prevent and resist cyber attacks more effectively, leading to greater protection of GC information and assets; Strengthen capabilities and resilience across the GC to proactively prepare for, respond to, and recover from cybersecurity events; and Foster a diverse GC workforce with the right cybersecurity skills, knowledge, and culture.*[32] Following the establishment of these strategic objectives, the Government outlined an implementation approach and key performance indicators to ensure the finalized Strategy would follow through on its goals.

Strategy

The Canadian National Cybersecurity Strategy incorporates the two principles - whole-of-society engagement and agile leadership - into three core pillars: Work with Partners to Protect Canadians and Canadian Businesses from Cyber Threats; Make Canada a Global Cyber Security Industry Leader; and Detect and Disrupt Cyber Threat Actors.[33] The

[28] https://www.cyber.gc.ca/en
[29] https://www.rcmp-grc.gc.ca/en/nc3
[30] https://www.canada.ca/en/government/system/digital-government/online-security-privacy/enterprise-cyber-security-strategy.html
[31] https://www.canada.ca/en/government/system/digital-government/online-security-privacy/enterprise-cyber-security-strategy.html
[32] https://www.canada.ca/en/government/system/digital-government/online-security-privacy/enterprise-cyber-security-strategy.html
[33] https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2025/ntnl-cbr-scrt-strtg-2025-en.pdf

pillars are designed to provide Canada with the necessary tools to not only protect itself, but to thrive in an increasingly digital world. Each pillar provides a set of overarching goals and actionable objectives to be able to achieve those goals. The strategy is laid out as follows:[34]

Pillar 1: Work with Partners to Protect Canadians and Canadian Businesses from Cyber Threats

Canada will:

- Forge whole-of-society partnerships
- Defend and advocate for Canadian interests and values internationally
- Advance national cyber awareness and hygiene

Pillar 2: Make Canada a Global Cyber Security Industry Leader

Canada will:

- Make Canada a trusted innovator that prioritizes cyber security
- Grow the foundational workforce of the future
- Identify and support targeted areas of research to meet Canadian needs

Pillar 3: Detect and Disrupt Cyber Threat Actors

Canada will:

- Identify, deter, and defend against cyber threats
- Improve capacity to combat cybercrime
- Make critical systems more resilient

Together, these three pillars form the backbone of Canada's National Cybersecurity Strategy, offering a comprehensive and future-ready framework to address today's threats and tomorrow's opportunities. By integrating whole-of-society partnerships with agile, forward-looking leadership, the strategy moves beyond reactive security toward proactive resilience, innovation, and global leadership. It emphasizes collaboration across sectors, investment in people and technology, and a strong posture against malicious actors.

[34] https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2025/index-en.aspx

Ultimately, the strategy equips Canada not only to defend itself in the digital domain, but also to lead with confidence in shaping a secure and prosperous cyber future.

Implementation and Accountability

Accompanying this Strategy is a call for partnership. It urges "Canadians and Canadian organizations of all sizes to report cyber incidents and cybercrime - of all kinds… To inform policy and regulation. To improve cyber hygiene, digital literacy, and public awareness. Here is where stakeholders can turn."[35] By continuing to engage with those who contributed to its development, Canada reinforces its whole-of-society approach, ensuring it endures beyond the Strategy's publication. Following the Strategy, they provide an in-depth outlook into the roles and responsibilities of different government agencies.[36]

The document also provides a detailed overview of the roles and responsibilities of various government agencies. For example, the Canadian Centre for Cyber Security is responsible for incident reporting and mitigation, public cybersecurity awareness, and the operation of the Canadian Cyber Defence Collective (CCDC), among other duties. Similar responsibilities are outlined for Public Safety Canada, the Royal Canadian Mounted Police, the Canadian Security Intelligence Service, and others. By offering comprehensive resources and clear points of contact, the Strategy ensures that no sector is left to face cybersecurity challenges alone.

Colombia

Colombia suffered nearly 36 billion attacks in 2024, accounting for 17% of all attacks in the region.[37] These attacks, which particularly affected the financial, healthcare, and energy sectors, spurred a movement within the Colombian government to develop The National Digital Security Strategy 2025-2027.[38] The Strategy lays out a vision to propel itself into a position to better handle these attacks, stating that "By 2034, Colombia will be a regional powerhouse in digital security, with a secure and resilient cyber ecosystem that fosters digital trust, economic growth, and social well-being, promoting an inclusive, innovative, and competitive society in the digital age, and ensuring the protection of the freedoms,

[35] https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2025/index-en.aspx
[36] https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2025/index-en.aspx
[37]https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/403023:La-Estrategia-Nacional-de-Seguridad-Digital-llega-para-enfrentar-las-crecientes-amenazas-ciberneticas#:~:text=El%20Gobierno%20Nacional%20present%C3%B3%20la,desarrollo%20integral%20de%20las%20personas.
[38] https://www.mintic.gov.co/portal/715/articles-403023_recurso_2.pdf

dignity, and development of all people."[39] The following section lays out how Colombia designed their strategy and what mechanisms it uses to help meet that ambitious goal.

Strategy Development

Before developing its national cybersecurity strategy, Colombia undertook the critical step of thoroughly assessing its risks and challenges—a foundational move that underscores the importance of understanding the "why" before defining the "how." By identifying institutional weaknesses, coordination gaps, talent shortages, outdated legal frameworks, and a lack of inclusivity as its core challenges, Colombia recognized that any effective plan must be grounded in a clear-eyed view of existing vulnerabilities[40]. This diagnostic approach not only informed the strategy's priorities but also ensured that proposed solutions would be relevant and actionable.

The development of the strategy, including identifying current gaps and challenges, is the next step in a long line of security strategies, legislation, and actions taken by the Colombian government. The government was able to put the determined risks and challenges into four categories:

1. Institutional weakness and a lack of effective coordination in digital security represent a significant obstacle to the protection of Colombian cyberspace.
2. Colombia faces a worrying lack of preparedness for increasingly sophisticated cyber threats. The country's insufficient capacity to comprehensively and effectively identify, assess, and mitigate cyber risks leaves it vulnerable to attacks that could have devastating consequences.
3. The shortage of specialized talent and the lack of a widespread digital security culture represent a significant obstacle to strengthening Colombia's digital defenses.
4. The outdated and inadequate Colombian regulatory framework to address current and emerging cyber challenges represents a significant obstacle to the effective protection of national cyberspace.

Within each of these subsections, the Strategy provides concrete examples for how each challenge was determined, laying the foundation for the Strategy to follow with specific recommendations targeting the risks and challenges. By clearly identifying areas that need improvement, the Strategy aligns all stakeholders on its goals and expected outcomes.

[39] https://www.mintic.gov.co/portal/715/articles-403023_recurso_2.pdf
[40] https://www.mintic.gov.co/portal/715/articles-403023_recurso_2.pdf

Strategy

Colombia's National Digital Security Strategy 2025–2027[41] represents clear growth in the country's approach to cybersecurity, building on the foundational policies laid out in the CONPES documents 3701[42] (2011), 3854[43] (2016), and 3995[44] (2020). These earlier documents established a baseline for digital security governance, upon which the new strategy expands to meet modern threats and seize opportunities in the rapidly evolving digital environment.

The new strategy serves as a roadmap to consolidate a more secure, reliable, and resilient digital environment. It emphasizes the protection of rights, the dignity of individuals, and the integral development of all Colombians. It is guided by a long-term vision of becoming a regional digital security powerhouse by 2034, with a resilient, trustworthy cyber ecosystem that promotes economic growth, social well-being, innovation, and inclusivity, while ensuring the protection of civil liberties and human dignity.[45]

Colombia's strategy is shaped by four key guiding approaches:

- Whole-of-society approach: Recognizing that cybersecurity is not just a government issue but one that involves all stakeholders—from civil society to the private sector and academia.
- Human-centered approach: Ensuring that technological advances enhance, rather than threaten, the rights and well-being of individuals.
- Risk management approach: Prioritizing proactive identification, mitigation, and response to cyber risks.
- Innovation and capacity-building approach: Promoting the development and deployment of new technologies and investing in human capital to strengthen national capabilities.

These approaches are supported by six core principles: protection of human rights and privacy; multisectoral coordination, collaboration, and cooperation; resilience; innovation; transparency; and digital trust. The strategy targets four priority areas, each with specific

[41] https://www.mintic.gov.co/portal/715/articles-403023_recurso_2.pdf
[42] https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf
[43] https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf
[44] https://colaboracion.dnp.gov.co/cdt/Conpes/Econ%C3%B3micos/3995.pdf
[45] https://www.mintic.gov.co/portal/715/articles-403023_recurso_2.pdf

objectives tied to the outlined challenges, and action items to strengthen Colombia's digital security posture:

1. Consolidate Digital Security Governance: Colombia seeks to reinforce national leadership and coordination in cybersecurity while fostering international cooperation and strong public-private partnerships.

    - Strengthen national leadership and coordination mechanisms
    - Promote international collaboration
    - Encourage public-private alliances

2. Improve National Cyber Resilience: Building resilience involves enhancing risk management, securing critical infrastructure, and expanding national cyber defense capabilities.

    - Bolster risk management and incident response
    - Protect critical national infrastructure and essential services
    - Strengthen cyber defense capabilities

3. Promote Innovation and Technological Development: The strategy encourages safe adoption of emerging technologies and investment in digital security research and innovation.

    - Manage risks related to emerging technologies
    - Support the growth of national technological capabilities

4. Develop the Digital Security Workforce: Investing in people is essential to national cyber readiness. The strategy focuses on strengthening digital security culture and training future professionals.

    - Promote a strong culture of cybersecurity
    - Foster talent development in digital security
    - Ensure privacy and data protection
    - Provide support to small and medium-sized enterprises (SMEs)

In addition, Colombia will work to modernize its cybersecurity legal framework, including revising current regulations, updating criminal procedures for cybercrime, and establishing clear rules for data protection and privacy.[46]

Implementation and Accountability

Action Plan

To ensure that the Strategy achieves its goals, the government included an "Action Plan" in the strategy.[47] The action plan directly responds to the risks and challenges posed at the beginning of the strategy and is designed to provide different areas of the government actionable objectives tied to the principles of the strategy. Each action includes the action itself; a defined output indicator aligned with the strategic goals; a classification based on relative importance; a timeframe; a responsible entity ranging from sector-specific ministries to national coordination bodies and local governments; and a monitoring method which will be used to hold the responsible entities, and the strategy itself, accountable.[48]

For instance, actions related to strengthening national coordination and cyber governance are led by the Ministry of Information and Communications Technologies (MinTIC) in coordination with defense and justice institutions. Capacity-building initiatives are guided by academic and vocational institutions under the leadership of the National Planning Department (DNP), while policies on the ethical adoption of emerging technologies fall under the joint purview of MinTIC and the Ministry of Science, Technology, and Innovation.

Governance Structure and Alignment with Legal and Policy Instruments

The Strategy is embedded in both legal and political instruments at the national and international levels. From a legal standpoint, the Strategy aligns with Colombia's constitutional principles and with relevant international agreements and treaties related to human rights, privacy, non-discrimination, and sustainable development. It reinforces the country's commitment to international digital norms while ensuring that national implementation respects fundamental freedoms.

From a policy perspective, the Strategy is carefully aligned with key national frameworks including The National Development Plan 2022–2026[49] and The National Digital Strategy

[46] https://www.mintic.gov.co/portal/715/articles-403023_recurso_2.pdf
[47] https://www.mintic.gov.co/portal/715/articles-403023_recurso_2.pdf
[48] https://www.mintic.gov.co/portal/715/articles-403023_recurso_2.pdf
[49] https://procolombia.co/en/transparency/national-development-plan

2023–2026.[50] This alignment guarantees that cybersecurity is not treated in isolation, but as a transversal issue that intersects with defense, justice, innovation, and economic development.

Japan

Strategy Development

Japan's *Cybersecurity Strategy: Cybersecurity for All* is guided by the strategic vision of "ensuring a free, fair and secure cyberspace."[51] The government developed the strategy around three key elements: Japan's trajectory in the 2020s, the foundational principles of the strategy, and the evolving issues related to cyberspace. By aligning cybersecurity with national policy goals—including the expansion of the digital economy, the promotion of digital transformation (DX), the realization of Society 5.0 with an emphasis on the UN Sustainable Development Goals (SDGs), and shifts in the national security environment—the government seeks to ensure that cybersecurity policy supports broader societal and economic objectives. This strategy, the third since the Basic Act on Cybersecurity[52] mandated the creation of a national cybersecurity strategy, provides a medium to long term perspective on securing cyberspace in the new digital age.[53]

In addition to the core vision of a "free, fair, and secure" cyberspace, the strategy reaffirms the five principles set forth in previous strategies: the assurance of the free flow of information, the rule of law, openness, autonomy, and multi-stakeholder collaboration.[54] It emphasizes that "cybersecurity policies should safeguard their free economic and social activities, secure their rights and convenience, and protect them by deterring the activities of malicious actors through law enforcement and legal systems in a timely and appropriate manner."[55] To that end, the strategy leverages Japan's political, economic, technological, and diplomatic strengths to promote resilience and national empowerment.

Finally, the strategy addresses pressing issues in cyberspace, including risks arising from environmental change, vulnerabilities in the economy and society, and evolving cyber threats. By considering Japan's long-term direction, reaffirming core principles, and

[50] https://www.mintic.gov.co/portal/715/articles-334120_recurso_1.pdf
[51] https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-en-booklet.pdf
[52] https://www.japaneselawtranslation.go.jp/en/laws/view/3677/en
[53] https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-en-booklet.pdf
[54] https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-en-booklet.pdf
[55] https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-en-booklet.pdf

responding to the shifting cyber threat landscape, the government crafted a policy framework tailored to the cybersecurity challenges of the 2020s.

Strategy

In order to achieve the goal of “Cybersecurity for All: Cybersecurity which leaves no-one behind,” the Japanese strategy provides three interwoven directions which guide the policy approaches. The three policy approaches, Advancing digital transformation (DX) and cybersecurity simultaneously; Ensuring the overall safety and security of cyberspace as it becomes increasingly public, interconnected, and interrelated; and Enhancing initiatives from the perspective of Japan’s national security, each fuel the strategy’s objectives and policy recommendations.[56] Within each pillar are several specific actions and objectives which will help guide the implementation of the strategy. Advancing digital literacy with no one left behind; ensuring cybersecurity is integrated with digital transformation; and strengthening Japan's capabilities for defense, deterrence, and situational awareness are just a few examples of the many objectives defined in the strategy.[57]

Under the first policy approach, Japan aims to enhance socio-economic vitality and sustainable development by tightly integrating cybersecurity with digital transformation efforts across society. This includes raising executive awareness, promoting DX and cybersecurity efforts among local governments and small-to-medium enterprises (SMEs), and fostering digital and cybersecurity literacy through inclusive programs. The strategy also emphasizes the trustworthiness of supply chains and the role of cybersecurity in sustaining innovation and economic competitiveness.

The second pillar addresses the safety and resilience of cyberspace as a shared, public domain. As digital technologies increasingly blur the lines between the cyber and physical worlds, the strategy promotes multi-stakeholder efforts to protect critical infrastructure, cloud services, and supply chains from systemic cyber threats.[58] Government agencies, academic institutions, and the private sector are encouraged to coordinate more closely.

The third direction focuses on bolstering national security and addressing the increasingly severe international cyber threat landscape. It calls for a fundamental strengthening of the Ministry of Defense and Self-Defense Forces’ cyber capabilities, the use of disruption

[56] https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-en-booklet.pdf
[57] https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-en-booklet.pdf
[58] https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-en-booklet.pdf

capabilities to deter attacks, and active participation in international cooperation with allies such as the United States and Association of Southeast Asian Nations (ASEAN) partners.[59]

Cross-cutting initiatives such as human resource development, public awareness campaigns, and expanded R&D further support the strategy's overarching vision of a "free, fair, and secure cyberspace" and help Japan build a cybersecurity framework suited for the demands of the digital era.[60]

Implementation and Accountability

The strategy emphasizes that cybersecurity should be "in line with the digital transformation that the government is pursuing – promoting a policy of improving cybersecurity measures to ensure Japan's national security."[61] This digital transformation, spearheaded by the Digital Agency[62], will work collaboratively with The Cybersecurity Strategic Headquarters (the Headquarters)[63] and other relevant entities to implement this strategy. To ensure accountability on following through on the plan, the Headquarters will create "an annual plan for each fiscal year, verifying the progress of each measure, summarizing the findings in an annual report, and reflecting them in the annual plan for the next fiscal year during the period of the three-year plan."[64] The National Center for Incident Readiness and Strategy for Cybersecurity (NISC) was reconstituted in 2025 as the National Cybersecurity Office[65], with an expanded mandate, responsible for assessing and monitoring threats across Japan's critical infrastructure, serving as the country's control tower for active cyber defense.

Each policy item within the strategy is assigned to specific responsible and supporting organizations, enhancing transparency and coordination. By clearly identifying implementing entities across the government and promoting active private sector participation—particularly from operators of critical infrastructure—the strategy aims to ensure measurable progress and sustained commitment. This structured approach is intended to drive accountability and establish clear expectations for fulfilling the strategy's objectives.

[59] https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-en-booklet.pdf
[60] https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-en-booklet.pdf
[61] https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-en-booklet.pdf
[62] https://www.digital.go.jp/en
[63] https://www.nisc.go.jp/eng/index.html
[64] https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-en-booklet.pdf
[65] https://japannews.yomiuri.co.jp/politics/politics-government/20250701-266862/

Ultimately, the strategy's implementation framework reflects a deliberate effort to institutionalize cybersecurity governance and promote a culture of continuous improvement. By combining centralized oversight with clearly assigned responsibilities and annual performance reviews, Japan seeks to maintain momentum and adapt to evolving threats throughout the strategy's duration. This accountability-driven model not only reinforces the government's commitment to national cybersecurity but also fosters trust and cooperation among public and private stakeholders in securing Japan's digital future.

Netherlands

Strategy Development

The Netherlands launched its first international cybersecurity strategy in 2017, laying the foundation for national cybersecurity efforts and establishing a permanent team of cyber diplomats to represent the country abroad. Building on the lessons learned from that strategy and its implementation, as well as through extensive consultations with government, industry, and civil society, the Netherlands released an updated National Cybersecurity Strategy in 2022.[66] [67] This new strategy is guided by the vision that "people and businesses should be able to benefit fully from participation in the digital society," while emphasizing that "security is an essential part of this."[68] Guided by that strategic vision, and the lessons learned through extensive collaboration, the government settled on 5 priorities which the strategy will help achieve: Be more aware of cyber threats so that we know and understand them; Ensure sufficient cyber expertise is available on the labour market so that we can meet the challenges we face; Be aware of and understand risks and threats; Legislation to ensure that frameworks are clear and verifiable; and Review of national cybersecurity system to ensure effective and efficient use of cyber capabilities.[69] Recognizing the growing dependence on digital technologies and connections, the strategy frames cybersecurity as a critical investment in the country's future.

Strategy

To achieve its vision of "working towards a future in which cyber resilience can always keep pace with any cyber threats,"the Netherlands Cybersecurity Strategy 2022–2028 is

[66] https://hcss.nl/news/understanding-the-dutch-national-cyber-security-strategy-with-arthur-laudrain/
[67] https://english.nctv.nl/topics/netherlands-cybersecurity-strategy-2022-2028/documents/publications/2022/12/06/the-netherlands-cybersecurity-strategy-2022-2028
[68] https://english.nctv.nl/topics/netherlands-cybersecurity-strategy-2022-2028/documents/publications/2022/12/06/the-netherlands-cybersecurity-strategy-2022-2028
[69] https://english.nctv.nl/topics/netherlands-cybersecurity-strategy-2022-2028/documents/publications/2022/12/06/the-netherlands-cybersecurity-strategy-2022-2028

structured around five key priorities and four strategic pillars. These pillars are: (1) strengthening the cyber resilience of government, businesses, and civil society organizations; (2) ensuring digital products and services are both secure and innovative; (3) countering cyber threats posed by state and criminal actors; and (4) enhancing the cybersecurity labor market, education, and the cyber resilience of the public.[70] Each pillar is supported by specific strategic aims. These aims are concrete, actionable goals designed to guide implementation and progress.

The five priorities further define desired outcomes that will safeguard citizens, strengthen public-private collaboration, and help position the Netherlands as a secure and forward-looking digital society. Taken together, these elements form a comprehensive roadmap for building national cyber resilience in an increasingly interconnected world.

Implementation and Accountability

To ensure the strategic aims are implemented effectively, the Dutch government released an accompanying Action Plan which contains "Ambitions and actions for a digitally secure society."[71] This plan outlines concrete actions linked to each strategic aim, detailing the responsible agency, supporting agencies, and a timeline for execution. Notable measures include "the merging of several overlapping organisations into a single National Cybersecurity Incident Response Team, or CSIRT, and the extension of the government's procurement requirements, which will be made available for companies to use for their own activities."[72] By translating strategic goals into actionable steps with clear accountability, the Action Plan provides a practical framework for turning the Netherlands' cybersecurity vision into reality.

Rwanda

Strategy Development

The Government of Rwanda (GoR) released the *National Cybersecurity Strategy of the Republic of Rwanda 2024–2029* in August 2024, the country's second National Cybersecurity Strategy. The strategy has as its vision: "cyber resilience, digital trust," hoping to align this

[70] https://english.nctv.nl/topics/netherlands-cybersecurity-strategy-2022-2028/documents/publications/2022/12/06/the-netherlands-cybersecurity-strategy-2022-2028
[71] https://english.nctv.nl/topics/netherlands-cybersecurity-strategy-2022-2028/documents/publications/2022/12/06/the-netherlands-cybersecurity-strategy---action-plan
[72] https://hcss.nl/news/understanding-the-dutch-national-cyber-security-strategy-with-arthur-laudrain/

strategy with the goals set by the Vision 2050 program.[73] The strategy begins by recognizing ICT infrastructure and applications as a cornerstone of national economic growth. It emphasizes that ICT is "a key enabler for economic growth and social mobility and is expected to improve Rwandans' standard of living."[74] In order to support the country's economic development goals, the strategy highlights the importance of making infrastructure resilient and secure against cyber threats. In order to develop this strategy, the Ministry of ICT and Innovation collaborated with key national and international stakeholders in cyber security, especially the National Cyber Security Authority, sector regulators, critical information infrastructure owners, law enforcement agencies, and academia.

In addition to broad stakeholder consultations, the GoR conducted a comprehensive assessment of Rwanda's current cybersecurity landscape. This included identifying unaddressed threats, anticipating future risks, and reviewing existing policies and governance frameworks to guide the strategy's direction. The review examined several foundational documents such as the National ICT Strategy and Plan (2015)[75], Vision 2050 (2015)[76], and the Seven-Year Transformation Programme (2017)[77], to evaluate progress and pinpoint areas for improvement.

Drawing from this analysis and extensive consultation, the GoR established seven guiding principles to shape the NCS: national leadership; clear roles and responsibilities; public–private collaboration; risk-based management; alignment with Rwandan values; international cooperation; continuous improvement; and comprehensiveness.

[73] https://www.minecofin.gov.rw/fileadmin/user_upload/Minecofin/Publications/REPORTS/National_Development_Planning_and_Research/Vision_2050/English-Vision_2050_Abridged_version_WEB_Final.pdf

[74] https://cyber.gov.rw/index.php?eID=dumpFile&t=f&f=427&token=6375c4cab9b091a9747cd9f07f8dc616ba825245

[75] https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Rwanda%20NCSS%20NICI_III.pdf

[76] https://www.minecofin.gov.rw/fileadmin/user_upload/Minecofin/Publications/REPORTS/National_Development_Planning_and_Research/Vision_2050/English-Vision_2050_Abridged_version_WEB_Final.pdf

[77] https://www.greenpolicyplatform.org/sites/default/files/downloads/policy-database/NST1_7YGP_Final.pdf

Strategy

The *National Cybersecurity Strategy of the Republic of Rwanda 2024–2029* offers strategic guidance to strengthen Rwanda's resilience in cyberspace and to position the country as a trusted, secure digital hub.[78] The Strategy is structured around three strategic pillars[79]:

1. Promote Cyber Resilience and Trust
2. Build the Rwandan Cybersecurity Industry
3. Enhance Cooperation and Collaboration

Supporting these pillars are cross-cutting enablers that help anchor the strategy in sustainable practice and ensure coherence across sectors. These include capacity building, awareness and culture, governance and regulation, and public–private partnerships.[80] Beyond defining priorities, the strategy lays out practical and actionable recommendations for various actors:

- Critical infrastructure and essential service providers are asked to adopt baseline cybersecurity measures, comply with minimum standards, and embed security into operational planning.
- Regulators and sector agencies are tasked with refining governance, oversight, and enforcement mechanisms to align with the national framework.
- Public institutions, SMEs, and technology providers are encouraged to adopt risk management practices, engage in capacity building, and partner in innovation ecosystems.
- Education institutions, researchers, and training bodies are asked to integrate cybersecurity into curricula, support research and innovation, and develop relevant certifications and professional pathways.
- All citizens and users are recognized as part of the security chain, with calls for awareness, digital hygiene, reporting, and cooperation with national programs.

[78] https://cyber.gov.rw/index.php?eID=dumpFile&t=f&f=427&token=6375c4cab9b091a9747cd9f07f8dc616ba825245
[79] Ibid.
[80] Ibid.

This inclusive stakeholder framework mirrors the idea of shared responsibility in national cybersecurity, encouraging collaboration across sectors and society.

The strategy anchors itself in a dual vision of “cyber resilience, digital trust”, aiming to safeguard Rwanda’s digital transformation while building confidence in ICT systems. It aligns with Rwanda’s broader development goals under Vision 2050, seeking to integrate cybersecurity as an enabler of sustainable growth and social progress.

By focusing on resilience, industry development, and cooperation, Rwanda aims not only to defend its digital infrastructure, but also to catalyze its cybersecurity ecosystem, strengthen governance, and deepen international engagement.

Implementation and Accountability

To translate Rwanda’s *National Cybersecurity Strategy 2024–2029* from vision into practice, the strategy designates the National Cyber Security Authority (NCSA) as the central coordinating and oversight body.[81] The NCSA is charged with leading implementation, monitoring progress, and reporting to national leadership. The strategy will also be formally integrated into Rwanda’s national legal framework, giving it stronger enforceability and alignment with other laws and policies.[82]

NCSA’s coordinating role includes working with sector regulators, critical infrastructure operators, law enforcement, academia, and private sector participants to align sectoral plans and manage cross-cutting risks.[83] The structure allows NCSA to audit critical infrastructure, carry out cyber investigations (in cooperation with other organs), issue guidelines and standards, and coordinate threat intelligence sharing.

In order to ensure goals are met, the NCSA will establish Key Performance Indicators (KPIs) and a monitoring mechanism to track progress, ensure alignment with strategic goals, and periodically review performance.[84] The authority already has a mandate under Law No. 26/2017 to coordinate and implement national cybersecurity policy and to monitor national ICT security programs, giving it both legal grounding and functional legitimacy.[85]

[81] https://dig.watch/resource/national-cybersecurity-strategy-of-the-republic-of-rwanda-2024-2029
[82] https://dig.watch/resource/national-cybersecurity-strategy-of-the-republic-of-rwanda-2024-2029
[83] https://cyber.gov.rw/index.php?eID=dumpFile&t=f&f=427&token=6375c4cab9b091a9747cd9f07f8dc616ba825245
[84] https://dig.watch/resource/national-cybersecurity-strategy-of-the-republic-of-rwanda-2024-2029
[85] https://rwandalii.org/akn/rw/act/law/2017/26/eng@2017-07-03/source

Singapore

Strategy Development

Singapore has a long tradition of cybersecurity, launching its *Infocomm Security Masterplan* in 2005 and the formation of the Singapore Infocomm Technology Security Authority (SITSA) in 2009.[86] "In 2015, the Cyber Security Agency of Singapore (CSA)[87] was set up as the central agency to oversee and coordinate all aspects of cybersecurity for the nation."[88] CSA published the first Singapore Cybersecurity Strategy in 2016, which had its core objectives to: Build a resilient infrastructure; Create a safer cyberspace; Develop a vibrant cybersecurity ecosystem; and Strengthen international partnerships.[89] Before releasing an updated strategy, the Singaporean government identified 4 key shifts that led to the determination that a new strategy was necessary. The shifts include disruptive technologies, growing cyber-physical risks; ubiquitous digital connectivity; and increased geopolitical tensions in cyberspace.[90] The new strategy, developed in consultation with multiple stakeholders including industry and local and foreign academia was launched in 2021, laying out a plan to "strengthen the security and resilience of our digital infrastructure and enable a safer cyberspace to support our digital way of life."[91]

Strategy

The *Singapore Cybersecurity Strategy 2021* provides clear, actionable guidance for organizations and individuals on strengthening the security of both digital and physical systems. It is structured around three strategic pillars: Build Resilient Infrastructure, Enable a Safer Cyberspace, and Enhance International Cyber Cooperation. These pillars are supported by two cross-cutting enablers: Developing a vibrant cybersecurity ecosystem and growing a robust cyber talent pipeline.[92]

[86] https://isomer-user-content.by.gov.sg/36/6318c1f5-3257-4c99-80e5-27339cf41883/The-Singapore-Cybersecurity-Strategy-2021.pdf
[87] https://www.csa.gov.sg/
[88] https://isomer-user-content.by.gov.sg/36/6318c1f5-3257-4c99-80e5-27339cf41883/The-Singapore-Cybersecurity-Strategy-2021.pdf
[89] https://isomer-user-content.by.gov.sg/36/6318c1f5-3257-4c99-80e5-27339cf41883/The-Singapore-Cybersecurity-Strategy-2021.pdf
[90] https://isomer-user-content.by.gov.sg/36/6318c1f5-3257-4c99-80e5-27339cf41883/The-Singapore-Cybersecurity-Strategy-2021.pdf
[91] https://isomer-user-content.by.gov.sg/36/6318c1f5-3257-4c99-80e5-27339cf41883/The-Singapore-Cybersecurity-Strategy-2021.pdf
[92] https://isomer-user-content.by.gov.sg/36/6318c1f5-3257-4c99-80e5-27339cf41883/The-Singapore-Cybersecurity-Strategy-2021.pdf

Beyond outlining priorities, the strategy offers practical recommendations tailored to a wide range of stakeholders, including critical information infrastructure (CII) owners, technology vendors, enterprise leaders, cybersecurity professionals, researchers, students, and everyday users. By engaging all segments of society, Singapore frames cybersecurity as a shared responsibility and a collaborative national effort. Ultimately, the strategy seeks to achieve “a secure cyberspace [that] underpins our national security, powers a digital economy, and protects our digital way of life.”[93]

Implementation and Accountability

To ensure the Strategy moves from vision to execution, Singapore has established a robust accountability framework centered on the Cyber Security Agency of Singapore (CSA). CSA oversees national coordination, ensures compliance across sectors, and monitors progress through performance metrics, regular reviews, and public reporting. Beyond oversight, the government has launched targeted programmes to bolster implementation, such as the Operational Technology Cybersecurity Competency Framework (October 2021)[94], designed to upskill operational technology professionals and share best practices with CII owners.

In 2024, Singapore also amended its Cybersecurity Act to address new cyber risks and technological advancements, including covering a wider range of essential digital services beyond traditional CII, such as cloud service providers and managed security service providers. The amendments also enhanced incident reporting obligations and empowered the CSA with greater authority to investigate and respond to cyber threats to keep pace with the evolving digital landscape and increasingly sophisticated cyber threats.[95]

For regional accountability and capacity-building, Singapore committed $30 million over five years to establish the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE).[96] This centre delivers multi-disciplinary training, virtual cyber defence exercises, and CERT-to-CERT collaboration to strengthen ASEAN cyber resilience. Together, these layered governance mechanisms ensure clear responsibilities, oversight, capacity-building, and performance tracking, transforming the Cybersecurity Strategy into an actively enforced and measurable national effort.

[93] https://isomer-user-content.by.gov.sg/36/6318c1f5-3257-4c99-80e5-27339cf41883/The-Singapore-Cybersecurity-Strategy-2021.pdf

[94] https://www.csa.gov.sg/resources/publications/operational-technology-cybersecurity-competency-framework--otccf-

[95] https://sso.agc.gov.sg/Acts-Supp/19-2024/Published/20240704?DocDate=20240704

[96] https://www.csa.gov.sg/news-events/press-releases/singapore-deepens-commitment-to-a-secure-cyberspace-through-capacity-building

United Kingdom

Strategy Development

The United Kingdom's *National Cyber Strategy 2022*[97] built on the foundation laid by its 2016-2021 predecessor[98], aiming to expand on the success achieved during that period. The strategy placed science and technology at the center of the UK's approach, "ensuring that cyber continues to be a national economic and strategic asset, that [their] technology is more trustworthy and is better able to ward off a spectrum of cyber adversaries whose capabilities were, until recently, the sole preserve of nation states."[99] The former UK government pledged to spend £22 billion per year on research and development, and to put technology at the heart of plans for national security.[100] This included, among other initiatives, the creation of the National Cyber Force, a partnership between defense and intelligence, in 2021.[101] Although the strategy was published under a previous UK government and the new UK Government has announced plans to refresh it, it remains the current cybersecurity strategy in the UK.[102]

The strategy was developed with an understanding of both the achievements and the shortcomings of the previous plan. Similar to developing a new strategy with no predecessor, the most important action is determining what it seeks to accomplish. The UK's vision for the new strategy was straightforward: "cyber power in support of national goals."[103] By building upon relevant, established national goals related to digital technology and infrastructure, the national cyber strategy hoped to make the UK "one of the most secure and attractive digital economies to live, do business, and invest in."[104] The following national goals were used to guide the development of the strategy, with the vision that the

[97] https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022

[98] https://assets.publishing.service.gov.uk/media/5fbceaf08fa8f559e32b4cc1/6.6788_CO_National-Cyber-Security-Strategy-2016-2021_WEB3.pdf

[99] https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022#foreword

[100] https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022#foreword

[101] https://www.gov.uk/government/organisations/national-cyber-force

[102] https://www.gov.uk/government/publications/national-security-strategy-2025-security-for-the-british-people-in-a-dangerous-world/national-security-strategy-2025-security-for-the-british-people-in-a-dangerous-world-html#:~:text=This%20includes%20publishing%20a%20refreshed,and%20corruption%2C%20domestically%20and%20internationally

[103] https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022#foreword

[104] https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022#foreword

"UK in 2030 will continue to be a leading responsible and democratic cyber power, able to protect and promote our interests in and through cyberspace in support of national goals:

- a more secure and resilient nation, better prepared for evolving threats and risks and using our cyber capabilities to protect citizens against crime, fraud and state threats;
- an innovative, prosperous digital economy, with opportunity more evenly spread across the country and our diverse population;
- a Science and Tech Superpower, securely harnessing transformative technologies in support of a greener, healthier society; and
- a more influential and valued partner on the global stage, shaping the future frontiers of an open and stable international order while maintaining our freedom of action in cyberspace."[105]

In addition to guiding objectives, the strategy identified key shifts in the government's approach compared to the previous edition of the national cyber strategy. While the main goal was to enhance or expand previous efforts, the new strategy aimed to be more comprehensive. Mainly, it encompassed a whole-of-society approach, fostering a more proactive cybersecurity environment in the government, and strengthening the core effort to promote cybersecurity, with government leading the way.[106] As the foreword of the strategy noted: "Through this strategy, the government is doing more to protect UK citizens and companies, and its international partners – helping realise its vision of cyberspace as a reliable and resilient place for people and business to flourish."[107]

Strategy

The Strategy provided a vision that "the UK in 2030 will continue to be a leading responsible and democratic cyber power, able to protect and promote [its] interests in and through

[105] https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022#foreword

[106] https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022#part-1-strategy

[107] https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022#foreword

cyberspace in support of national goals."[108] It emphasized innovation, resilience, and shared responsibility among government, businesses, critical infrastructure, and citizens.

Cyber resilience was viewed through three lenses: understanding risk, defending systems, and preparing recovery. The approach provided was tiered: from basic protections for individuals and SMEs to advanced safeguards for national services. This was a whole-of-society strategy, supported by international cooperation.[109] The strategy establishes the foundational direction of the country's cyber governance. By using data-driven insights to identify risks, building capacity from the ground up, and encouraging accountability and shared responsibility across the government and private sector, the government hoped to achieve its goals. In order to improve upon their current cyber landscape, the strategy put forth the following pillars and accompanying objectives to guide their national cyber framework:

[108] https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022

[109] https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022#part-1-strategy

Pillars and objectives			
Pillar 1 **Strengthening the UK cyber ecosystem**	1. Strengthen the structures, partnerships and networks necessary to support a whole-of-society approach to cyber.	2. Enhance and expand the nation’s cyber skills at every level, including through a world class and diverse cyber profession that inspires and equips future talent.	3. Foster the growth of a sustainable, innovative and internationally competitive cyber and information security sector, delivering quality products and services, which meet the needs of government and the wider economy.

Pillar 2 **Building a resilient and prosperous digital UK**	1. Improve the understanding of cyber risk to drive more effective action on cyber security and resilience.	2. Prevent and resist cyber attacks more effectively by improving management of cyber risk within UK organisations, and providing greater protection to citizens.	3. Strengthen resilience at national and organisational level to prepare for, respond to and recover from cyber attacks.
Pillar 3 **Taking the lead in the technologies vital to cyber power**	1. Improve our ability to anticipate, assess and act on the science and technology developments most vital to our cyber power.	2. Foster and sustain sovereign and allied advantage in the security of technologies critical to cyberspace.	2a. Preserve a robust and resilient national Crypt-Key enterprise which meets the needs of HMG customers, our partners and allies, and has appropriately mitigated our most

	3. Secure the next generation of connected technologies and infrastructure, mitigating the cyber security risks of dependence on global markets and ensuring UK users have access to trustworthy and diverse supply.	4. Work with the multistakeholder community to shape the development of global digital technical standards in the priority areas that matter most for upholding our democratic values, ensuring our cyber security, and advancing UK strategic advantage through science and technology.	significant risks including the threat from our most capable of adversaries

Pillar 4 **Advancing UK global leadership and influence**	1. Strengthen the cyber security and resilience of international partners and increase collective action to disrupt and deter adversaries.	2. Shape global governance to promote a free, open, peaceful and secure cyberspace.	3. Leverage and export UK cyber capabilities and expertise to boost our strategic advantage and promote our broader foreign policy and prosperity interests.
Pillar 5 **Detecting, disrupting and deterring adversaries**	1. Detect, investigate and share information on state, criminal and other malicious cyber actors and activities in order to protect the UK, its interests and its citizens.	2. Deter and disrupt state, criminal and other malicious cyber actors and activities against the UK, its interests, and its citizens.	3. Take action in and through cyberspace to support our national security and the prevention and detection of serious crime.

Following the outlining of these pillars and objectives the strategy continued by providing detailed information for all relevant stakeholders. First, it provided a "Strategic Context", outlining the global cyber landscape and how the UK does, and intends to, fit in.[110] It provided context on definitions related to cyberspace, cyberpower and how the strategy intends to make the UK more resilient, and international leadership and influence. Next, the strategy focused on countering cyber threats and deterring adversaries.

In order to ensure relevant stakeholders understood what was at stake, the strategy outlined several case studies of recent cyber attacks, followed by drivers of change that were expected to radically change the cyber landscape over the coming years. The continued rapid expansion of data and digital connectivity, an increasingly complex landscape, evolving and diversifying cyber threats, global competition, and emerging technologies are just some of the factors that might lead to governments creating an NCS.

Finally, to support the vision of "a free, open, peaceful, and secure cyberspace", the strategy provided several guiding principles aimed at prioritizing a secure, open, and inclusive cyberspace that protects citizens' rights while supporting economic and democratic freedoms.[111]

Implementation and Accountability

In addition to outlining a comprehensive set of objectives, recommended actions, and relevant stakeholders, the implementation of the UK's National Cyber Strategy was grounded in a whole-of-society approach. Citizens, businesses, organizations, the cybersecurity sector, major technology companies, and the government must collaborate on the strategy's key issues to drive meaningful progress. Within the government, several major players would be crucial to success:

- First is the National Cyber Security Centre (NCSC)[112]. The NCSC was launched in 2017 to be the UK's national authority on the cybersecurity environment, sharing knowledge and addressing systemic vulnerabilities, while providing leadership on key national cybersecurity issues; in other words, the NCSC is the UK's Computer Security Incident Response Team (CSIRT), which is required under the NIS

[110] https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022#part-1-strategy:~:text=Part%201%3A%20Strategy-,Strategic%20Context,-Global%20Britain%20in

[111] https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022#part-1-strategy

[112] https://www.ncsc.gov.uk/

Regulations[113] passed in 2018 in accordance with the EU.[114] Under the strategy, the NCSC was tasked with the following:

  - Taking direct action to reduce cyber harms to the UK.
  - Supporting all parts of UK society to protect themselves.
  - Providing technical input to HMG policy and regulation on the issues of most importance for cyber security.
  - Providing UK sovereign capabilities.
  - Supporting growth in cyber skills and investment.

- The NCSC would also contribute to the evaluation of progress against the objectives of this national cyber strategy.
- Next is the National Cyber Force (NCF).[115] Established in 2020, the NCF is responsible for countering threats from criminals seeking to do harm to the UK; countering threats which disrupt the confidentiality, integrity, and availability of data and services in cyberspace; and contributing to the UK Defence operations.[116] The strategy supported the continuation of the NCF's work, including its operations which are used to "influence individuals and groups, disrupt online and communications systems," otherwise known as offensive cyber.[117]
- Finally, the Law Enforcement's National Cyber Crime Network was tasked with continuing to drive criminal justice responses to malicious activities in cyberspace. The network, composed of the National Crime Agency's National Cyber Crime Unit (NCCU), provides national leadership and coordination of the response in the UK.[118]

The Strategy provided detailed implementation guidance for each of its pillars. For every objective, it outlined background context, specific actions, intended outcomes, and the stakeholders responsible for execution and accountability. By clearly defining responsibilities and expected results, the strategy aimed to equip all stakeholders with the information they need to help the UK realize its vision of becoming a global leader in cybersecurity by 2030.

[113] https://www.legislation.gov.uk/uksi/2018/506/made

[114] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

[115] https://www.gov.uk/government/organisations/national-cyber-force

[116] https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022#pillar-1-uk-cyber-ecosystem:~:text=cyber%20assessments%20function.-,The%20National%20Cyber%20Force,-Established%20in%202020

[117] https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022#pillar-1-uk-cyber-ecosystem

[118] https://nationalcrimeagency.gov.uk/

Moving Forward

The UK government understands the importance of cybersecurity in addressing their nation's goals. While the 2022 National Cyber Strategy was comprehensive, it is important to understand that it is part of a greater ecosystem of strategies and regulations that all impact the cybersecurity ecosystem. Annex A of the strategy provided relevant information for how the following relate to cybersecurity: The Integrated Review[119], the National Data Strategy[120], the Plan for Digital Regulation[121], the National AI Strategy[122], the National Resilience Framework[123], the Net Zero Strategy[124], and the Beating Crime Plan.[125]

Following the publication of the National Cyber Strategy, the UK government published the *Government Cyber Security Strategy: Building a cyber resilient public sector*[126] (the government strategy) to provide insight into the government's plans to act on the objectives laid out in the former. "The strategy's vision is to ensure that core government functions are resilient to cyber attack, strengthening the UK as a sovereign nation and cementing its authority as a democratic and responsible cyber power."[127] In addition to providing additional context on the evolving cyber threat landscape, the government strategy provided actionable guidance to government agencies regarding managing cyber security risk, protecting against cyber attacks, detecting cyber security events, minimizing the impact of cyber security incidents, developing the right cyber security knowledge and culture, measuring success, and implementing the strategy.[128] The specific aim was for "Government's critical functions to be significantly hardened to cyber attack by 2025, with all government organisations across the whole public sector being resilient to known vulnerabilities and attack methods no later than 2030."[129]

The UK's National Cyber Strategy and subsequent Government Cyber Security Strategy lay out not only what needs to be achieved, but how and by whom. Success depends on the

[119] https://assets.publishing.service.gov.uk/media/641d72f45155a2000c6ad5d5/11857435_NS_IR_Refresh_2023_Supply_AllPages_Revision_7_WEB_PDF.pdf

[120] https://www.gov.uk/guidance/national-data-strategy

[121] https://www.gov.uk/government/publications/digital-regulation-driving-growth-and-unlocking-innovation

[122] https://www.gov.uk/government/publications/national-ai-strategy

[123] https://www.gov.uk/government/publications/the-uk-government-resilience-framework/the-uk-government-resilience-framework-html

[124] https://www.gov.uk/government/publications/net-zero-strategy

[125] https://www.gov.uk/government/publications/beating-crime-plan

[126] https://assets.publishing.service.gov.uk/media/61f0169de90e070375c230a8/government-cyber-security-strategy.pdf

[127] https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030

[128] https://assets.publishing.service.gov.uk/media/61f0169de90e070375c230a8/government-cyber-security-strategy.pdf

[129] https://assets.publishing.service.gov.uk/media/61f0169de90e070375c230a8/government-cyber-security-strategy.pdf

coordinated efforts of a broad ecosystem, from government agencies to private sector actors and individual citizens. With a clear structure for implementation and accountability, the strategy helped transform strategic visions into actionable steps. This comprehensive approach ensured that all parts of society were seen as playing a role in strengthening the UK's cyber resilience, ultimately positioning the country to meet evolving digital threats and to lead globally in cybersecurity by 2030.

United States

Strategy Development

The United States' most recent *National Cybersecurity Strategy*[130] was published in March 2023 with the vision of securing "the full benefits of a safe and secure digital ecosystem for all Americans."[131] To achieve this, it proposed a shift in how the United States allocates roles, responsibilities, and resources in cyberspace: by rebalancing the responsibility to defend cyberspace and realigning long-term investment incentives.[132] To develop the strategy, the government first sought to understand the strategic cybersecurity environment. Building off of the 2018 National Cyber Strategy, it identified emerging trends and the actions of malicious actors as the most critical factors to assess before formulating a strategic response.

The strategy notes that "emerging trends are creating both new opportunities for further advancement and new challenges to overcome."[133] The increasing complexity and interdependence of emerging technologies, the expansion of Internet-of-Things (IoT) devices in everyday life, and other technological shifts all contribute to the need for a more robust cybersecurity framework.

Next, it states that "malicious actors threaten our progress toward a digital ecosystem that is inclusive, equitable, promotes prosperity, and aligns with our democratic values."[134] Citing specific nation-state actors, it argues that new tools and services empower countries that previously lacked the technological capacity to inflict harm on U.S. interests to evolve

[130] https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
[131] https://bidenwhitehouse.archives.gov/oncd/national-cybersecurity-strategy/
[132] https://bidenwhitehouse.archives.gov/oncd/national-cybersecurity-strategy/
[133] https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
[134] https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

into sophisticated, organized crime syndicates.[135] These cyber threats endanger the "national security, public safety, and economic prosperity of the United States and its allies and partners."[136]

Both emerging trends and malicious actors, among many other factors, set the stage for the development of a new National Cybersecurity Strategy. In addition to incorporating lessons learned from the 2018 National Cybersecurity Strategy, the 2023 strategy was developed alongside the National Security Strategy and National Defense Strategy by a "broad interagency team."[137] Importantly, it was informed "through a months-long consultation process with the private sector and civil society."[138] The National Security Council (NSC) and the Office of the National Cyber Director (ONCD) led this effort in close collaboration with relevant public and private stakeholders, aiming to position the United States and its allies to build a digital ecosystem that is more defensible, resilient, and aligned with democratic values.[139]

Strategy

The government, following thorough interagency collaboration and private sector engagement, established a forward-looking vision to guide its national cybersecurity strategy:

> *"In this decisive decade, the United States will reimagine cyberspace as a tool to achieve our goals in a way that reflects our values: economic security and prosperity; respect for human rights and fundamental freedoms; trust in our democracy and democratic institutions; and an equitable and diverse society."*[140]

[135] https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

[136] https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

[137] https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

[138] https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

[139] https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

[140] https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

The 2023 strategy builds on the foundation of the 2018 strategy, stating that it "replaces the 2019 National Cyber Strategy but continues many of its priorities."[141] In addition to these continuities, the government introduced two "fundamental shifts in how the United States allocates roles, responsibilities, and resources in cyberspace."[142] The strategy recognizes that the federal government must use all instruments of national power—diplomatic, economic, military, intelligence, and law enforcement—in a coordinated manner to protect national security, public safety, and economic prosperity.[143] The overarching goals of the strategy are to ensure that the United States' digital ecosystem is:

- Defensible, where cyber defense is overwhelmingly easier, cheaper, and more effective;
- Resilient, where cyber incidents and errors have little widespread or lasting impact; and
- Values-aligned, where its most cherished values shape – and are in turn reinforced by – its digital world.[144]

To realize these goals, the strategy is organized around five strategic pillars:

1. Defend Critical Infrastructure
2. Disrupt and Dismantle Threat Actors
3. Shape Market Forces to Drive Security and Resilience
4. Invest in a Resilient Future
5. Forge International Partnerships to Pursue Shared Goals

Each pillar contains clearly defined objectives that support implementation. These objectives are deliberately interconnected, reflecting the complexity of modern digital infrastructure, cyber threats, and economic systems. By embedding specific outcomes within each pillar, the strategy provides a structured roadmap for aligning national resources and policy decisions toward shared cybersecurity goals.

[141] https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

[142] https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/

[143] https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/

[144] https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/

Two fundamental shifts underpin the strategy's implementation.[145] The first is a rebalancing of responsibility, moving the burden of cyber defense from individuals, small organizations, and under-resourced infrastructure operators to entities better equipped to manage cyber risk, such as the federal government and large technology and cybersecurity firms.[146] The second is a realignment of incentives to encourage long-term investment in secure technologies. The strategy outlines how the federal government will use its full range of authorities to reshape market forces and drive collaboration across sectors in a way that is equitable and mutually beneficial. These shifts aim to move beyond voluntary compliance, institutionalizing proactive defense through regulation, standards, public-private collaboration, and updated federal procurement practices.[147]

Finally, the strategy embraces a whole-of-nation approach, emphasizing coordinated action across federal, state, local, tribal, territorial, and private sector actors. By integrating cybersecurity into economic policy, law enforcement, and international diplomacy, the United States seeks not only to defend against cyber threats, but also to shape a global digital environment where resilience, security, and democratic values reinforce one another.

Implementation and Accountability

The U.S. National Cybersecurity Strategy builds on the foundation of previous strategies, offering actionable objectives while reinforcing the country's long-standing cybersecurity goals. Although it introduces a shift in how resources are allocated and investments are prioritized, its core vision remains aligned with previous national cybersecurity strategies. The strategy's five pillars serve as a springboard for future policymaking and program development. Designed to integrate into the broader national policy framework, it complements the National Security Strategy[148], relevant National Security Memoranda such as those regarding quantum computing[149] and critical infrastructure[150], Executive Orders on

[145] https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

[146] https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

[147] https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

[148] https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf

[149] https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

[150] https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/2021/jul/cs2021_0138.pdf

cybersecurity[151], and other related initiatives. It is also structured to accommodate future developments. For instance, the AI Action Plan released in July 2025 expands on the strategy by directing additional attention and resources to the protection of critical infrastructure and cybersecurity.[152]

To guide implementation, the Office of the National Cyber Director (ONCD) released the National Cybersecurity Strategy Implementation Plan (NCSIP) in 2023,[153] followed by an updated version in 2024.[154] The NCSIP is a roadmap for the effort outlined in the strategy. It describes more than 65 "high-impact initiatives requiring executive visibility and interagency coordination that the Federal government will carry out to achieve the Strategy's objectives."[155] Each initiative is directly linked to specific strategic objectives and identifies the lead federal agency, supporting entities, and an anticipated timeline for completion.

While federal agencies play a central role in executing these initiatives, the Strategy emphasizes that success depends on broad-based collaboration. Achieving its vision of reimagining cyberspace will "only succeed in implementing the National Cybersecurity Strategy through close collaboration with the private sector; civil society; state, local, Tribal, and territorial governments; international partners; and Congress."[156] Together, the Strategy and its Implementation Plan aim to unite all relevant stakeholders in advancing a more secure and resilient digital ecosystem.

International Conventions

African Union Convention on Cyber Security and Personal Data Protection (The Malabo Convention)

[151] https://www.whitehouse.gov/presidential-actions/2025/06/sustaining-select-efforts-to-strengthen-the-nations-cybersecurity-and-amending-executive-order-13694-and-executive-order-14144/

[152] https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf

[153] https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf

[154] https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/05/National-Cybersecurity-Strategy-Implementation-Plan-Version-2.pdf

[155] https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf

[156] https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf

The African Union (AU) Convention on Cyber Security and Personal Data Protection, commonly known as the Malabo Convention, was adopted in 2014 in Malabo, Equatorial Guinea.[157] According to Article 36, the Convention would enter into force once 15 member states had ratified it. In May 2023, Mauritania ratified the convention, bringing it into effect 30 days later, in June 2023.[158]

One of the key goals in ratifying the Malabo convention is to harmonize cybersecurity and data protection governance across the continent. By encouraging member states to align their national legal frameworks with continental objectives and standards, it promotes a consistent and elevated approach to digital governance.

The Convention encompasses four key areas: (1) Cybersecurity and cybercrime; (2) Personal data protection; (3) Electronic transactions; and (4) international cooperation.[159] As ratifying countries develop and revise their national cybersecurity strategies and legislation, the Convention provides a foundation to build off of. Its principles support the creation of interoperable policies that strengthen both national and regional cyber resilience.

Council of Europe Convention on Cybercrime (The Budapest Convention)

The Budapest Convention on Cybercrime, established in 2001 and entering into force in 2004, was the first major international treaty focused on combating cybercrime.[160] The treaty has three primary objectives: 1. Harmonizing national laws related to cyber crime, 2. Supporting the investigation of those crimes, and 3. Increasing international cooperation.[161] The treaty requires participating countries to criminalize specified cyber-related activities—such as illegal access, data interference, and computer-related fraud—and to adopt procedural rules for digital evidence gathering. This includes mechanisms such as the expedited preservation of stored data, real-time collection of traffic data, and enhanced powers for search and seizure of computer systems.[162]

[157] https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf
[158] https://www.diplomacy.edu/blog/what-is-the-malabo-convention/
[159] https://www.diplomacy.edu/blog/what-is-the-malabo-convention/
[160] https://rm.coe.int/1680081561
[161] https://www.crossborderdataforum.org/budapest-convention-what-is-it-and-how-is-it-being-updated/
[162] https://rm.coe.int/1680081561

Since the treaty's adoption, rapid technological change has expanded the range and sophistication of cyber threats. In response, the Cybercrime Convention Committee has recommended new measures, including the Second Additional Protocol (the first focused on racist and xenophobic acts). Adopted in 2022, the Second Additional Protocol addresses challenges in accessing electronic evidence across borders, particularly in relation to cloud computing, by streamlining procedures for cross-border data requests and improving safeguards.[163] As of now, at least 51 States have signed this protocol.[164]

For countries developing an NCS, aligning with the Budapest Convention provides a recognized international legal framework for combating cybercrime. It ensures national laws are interoperable with those of other States, facilitating cross-border investigations, which is critical in an environment where most cybercrime is transnational.

United Nations Convention on Cybercrime

The United Nations Convention against Cybercrime was adopted by the General Assembly of the United Nations (UN) in 2024 by resolution 79/243.[165] The treaty provides "States with a range of measures to be undertaken to prevent and combat cybercrime. It also aims to strengthen international cooperation in sharing electronic evidence for serious crimes."[166] It obliges states to criminalize offenses such as unauthorized access, data interference, fraud, and child exploitation, while creating mechanisms for expedited mutual legal assistance, cross-border evidence sharing, and extradition. The Convention's scope extends to emerging threats—including crimes involving crypto-assets and online grooming—and seeks to harmonize national laws and strengthen operational cooperation through designated contact networks. Its implementation will begin after a signing ceremony in Hanoi in October 2025 and requires ratification by forty states to enter into force.[167]

For countries developing National Cybersecurity Strategies, the Convention offers a ready-made framework for aligning domestic laws with international norms, building law enforcement capacity, and enabling faster transnational collaboration.

[163] https://www.coe.int/en/web/cybercrime/second-additional-protocol
[164] https://www.coe.int/en/web/cybercrime/second-additional-protocol
[165] https://docs.un.org/A/RES/79/243
[166] https://www.unodc.org/unodc/cybercrime/convention/home.html
[167] https://www.unodc.org/unodc/cybercrime/convention/home.html