Cybersecurity Strategy Scorecard

Dr. Fred Heiding
Alex O'Neill
Lachlan Price

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

Table of Contents

1. Foreword

For more than five decades, the Belfer Center has advanced policy-relevant research to help tackle some of the biggest security challenges of our time. This work has shaped policy discourse on arms control during the Cold War, counterterrorism strategy after September 11th, and the growing risks emerging from digital technologies today. The release of the 2025 Cybersecurity Strategy Scorecard continues this tradition.

While serving in the U.S. Department of Defense, I was fortunate to be involved in shaping and implementing American cybersecurity strategy as it became an increasingly urgent national security concern among policymakers and experts. Cyber threats—from state-backed hacking campaigns to ransomware attacks on private companies—are becoming more sophisticated, pushing governments to enhance their cybersecurity measures to safeguard citizens, critical infrastructure, and national economies.

Through past projects such as the 2022 National Cyber Power Index, the Belfer Center has helped shape policy debates around cybersecurity and digital strategy. This Cybersecurity Strategy Scorecard builds on the Belfer Center's prior research by offering a detailed cross-national assessment that incorporates qualitative and quantitative data, expert interviews, and country-specific evaluations. It provides a comparative framework for analyzing national cybersecurity strategies across major global players, identifying best practices and gaps in policy. By equipping policymakers with fact-based analysis and recommendations, this Scorecard provides policymakers with data-driven guidance for designing and implementing forward-looking cybersecurity policies.

Fred Heiding, Alex O'Neill, and Lachlan Price have done an outstanding job with this project. Their work will help future policy leaders make sense of cybersecurity strategies and navigate the complexities of managing cyber risks.

Eric Rosenbach
Director, Belfer Center's Defense, Emerging Technology, and Strategy Program
Former Chief of Staff and
Assistant Secretary for the U.S. Department of Defense

2. Acknowledgments & About the Authors

Acknowledgments

We wish to express our gratitude to the colleagues and policymakers whose contributions helped make this report possible. Above all, we are grateful to Eric Rosenbach for his essential role in conceptualizing this project and bringing it to life, as well as for supporting it over the last year through the Belfer Center's Defense, Emerging Technology, and Strategy (DETS) program. We also thank Dr. John Park for his advice and encouragement in the early phases of our research. Among the many colleagues who made valuable contributions, Dr. So Jeong Kim, Nikita Shah, and Julia Voo went above and beyond to share feedback on our research design as well as insight on specific country cases. We are indebted to many additional experts and researchers, including Manuel Atug, Tucker Bailey, Dr. Benjamin Bartlett, Jim Boehm, Ferdinand Gehringer, Juan Andres Guerrero Saade, Dr. Yaniv Harel, Jason Healey, Dr. Sven Herpig, Miriam Howe, Cam Shane, Dr. Sohyun Shin, and Dr. Valentin Weber. We are also deeply grateful to the officials who shared their perspectives with us, especially Yosi Aviram, Jessica Brooks, Matt Ferren, Hubert Han, Andre Jaworski, Wonjae Kim, Daniel Meltzian, Shin Yong-Seok, Maxi Sommerschuh, Ollie Whitehouse, Lauryn Williams, Yik Jiawei, Luise Zacharias, and a number of others who asked not to be named. A special thanks to the Belfer Comms office and the DETS program team, especially Emily O'Toole, Olivia Leiwant, and Ethan Lee, for their invaluable assistance, as well as to Andy Facini and Kimihiro Nakamura. All errors belong to the authors alone.

About the Authors

Dr. Fred Heiding is a research fellow at the Belfer Center's Defense, Emerging Technology, and Strategy (DETS) program at Harvard Kennedy School. His work focuses on computer security at the intersection of technical capabilities, business implications, and policy remediations. Fred is a member of the World Economic Forum's Cybercrime Center, a board member of DEFCON's misinformation village, a teaching fellow for the Generative AI course at Harvard Business School, and a member of the Responsible AI Institute. His work has been presented at leading conferences, including Black Hat (2023 and 2024), Defcon, BSides, and leading academic journals like IEEE Access and professional journals like Harvard Business Review. He has assisted in the discovery of more than 45 critical computer vulnerabilities (CVEs).

Alex O'Neill is a national security researcher who studies emerging technology, cyber threats, and illicit finance. He previously worked at the Belfer Center's Project on Managing the Atom and Korea Project, where he co-founded and led for three years the North Korea Cyber Working Group. Alex is the author of "Upholding North Korea Sanctions in the Age of Decentralised Finance" (Royal United Services Institute) and "Cybercriminal Statecraft: North Korean Hackers' Ties to the Global Underground" (Belfer Center). He received an MSc in Russian and East European Studies from the University of Oxford and a BA with distinction in History from Yale University.

Lachlan Price is a dual Master in Public Policy and Master of Business Administration candidate at Harvard Kennedy School and the MIT Sloan School of Management. Before attending graduate school he was a Digital Consultant at McKinsey and Company Australia, where he supported the development of the Australian 2023-2030 National Cybersecurity Strategy, the rollout strategy for Australia's Digital Identity system (myGovID), and several other digital initiatives across government and the private sector. Lachlan's research activities focus on strategy for public-private collaboration in emerging dual-use technologies, including AI, quantum, space, and autonomous systems. Lachlan holds an MEng in Aeronautical Engineering from Imperial College, London.

3. Executive Summary

This report analyzes the national cybersecurity strategies of seven leading powers—Australia, Germany, Japan, Singapore, South Korea, the United Kingdom, and the United States—to identify best practices and, we hope, inform future policymaking. We have benchmarked each strategy against a rubric of 70 criteria spanning five core categories: protecting people and infrastructure, generating capacity, building partnerships, codifying roles and responsibilities, and communicating clear policy. Our research highlights effective and innovative cybersecurity policy approaches that should inform global standards, as well as areas where the seven strategies fell short, aligned, or diverged significantly. Based on our findings, we offer commentary specific to each featured country's threat landscape and policy environment, as well as recommendations for future national cybersecurity strategists from any country.

Our results reveal that there is no universal blueprint for national cybersecurity strategy. Indeed, while certain technical best practices apply across the board, the most successful national policy approaches are tailored to the domestic context, that is, to the unique combination of threats, resource constraints, social and political dynamics, and other factors that distinguish each country from its peers. In other words, what works for Singapore or Germany may not always suit the United States or Japan. Nevertheless, the strategies share several recurring themes. Most countries prioritize developing the technical workforce, defending critical infrastructure, assigning cybersecurity responsibilities, and strengthening cooperation with industry and international partners, often through creative schemes. Fewer strategies adequately consider how to safeguard small- and medium-sized enterprises (SMEs) and vulnerable population groups or how to build a hospitable environment for the technical practitioners, entrepreneurs, and home-grown cybersecurity unicorns they usually envision cultivating. We have sought in our analysis to offer concrete recommendations for remediating those gaps and others, particularly improving cybersecurity governance, incentivizing private-sector investment in security, and preparing for emerging threats from AI and quantum technologies.

Key Assessments:

- **Australia, Singapore, the United Kingdom, and the United States' strategies stand out for their quality and creativity.** Each of those documents blends a competent policy baseline with at least a few signature initiatives worthy of global emulation, such as Australia's model for national threat sharing and the United States' vision for better aligning private sector incentives with security goals.

- **Germany, Japan, and South Korea's strategies outline weaker approaches.** Germany's is highly detailed but lacks a strong overarching vision and fails to address pre-existing holes in the national cybersecurity architecture. South Korea suffers from the reverse, presenting a coherent vision based on countering North Korean threats but supported by insufficiently detailed policy measures.

- **Nevertheless, several of the leading documents suffer from major flaws, while the less remarkable strategies still have lessons to offer.** The U.S. strategy, which received the highest marks of any strategy in our assessment, falls far short with respect to protecting individuals and their data. Despite its weaknesses, Japan's strategy's "Cybersecurity for All" theme lends itself to a strong focus on defending the whole of society, especially vulnerable groups that other strategies often overlook.

- **Common strengths across the strategies include private sector capacity-building, international partnerships, and critical infrastructure defense.** Most national cybersecurity strategies emphasize expanding technical education, upskilling programs, and workforce pipelines to address the

talent shortage. There is a widespread commitment to international and domestic cooperation, with particular emphasis on public-private partnerships and interagency coordination. Nearly all countries also prioritize critical infrastructure security, although their definitions of essential systems and defense strategies vary significantly.

- **Despite these strengths, several notable gaps persist, particularly in protecting SMEs and vulnerable populations.** Many strategies focus on large enterprises but devote little consideration to supporting smaller businesses, which often lack resources for cybersecurity. Investment in non-technical cyber workforces, such as legal and policy experts, remains insufficient, leaving critical gaps in governance and compliance. Approaches to regulating data privacy and assigning accountability for mitigating cyber risks are inconsistent, creating uncertainty for businesses and consumers. Furthermore, most strategies fail to think deeply about aligning incentives that would encourage the private sector to prioritize cybersecurity, which is likely to result in weak or fragmented implementation efforts.

- **Future challenges will require that cyber strategies more thoughtfully address accountability, risk quantification, and incentive structures.** Ensuring clear accountability and measurable outcomes for strategy implementation remains a key weakness, as many national policies lack enforcement mechanisms. Cyber risk quantification is still underdeveloped, making it difficult for policymakers and businesses to allocate resources effectively. In addition, governments must refine cybersecurity incentive structures to encourage the private sector to adopt meaningful security measures proactively rather than relying on reactive compliance.

This report proceeds in four main sections. The Introduction identifies key considerations for devising national cybersecurity strategy and takes stock of prior research on this topic. The following section outlines our research methodology, explains our approach's new contributions, and acknowledges a number of inevitable shortcomings for a project of this scope. The "Cybersecurity Strategy Scorecard" presents the results of our comparative evaluation of the seven strategies and individual scorecards for each country.[1] The subsequent "Analysis" section discusses our findings and offers practical takeaways for cyber policymakers. The report concludes with a broader consideration of future challenges and opportunities in the field of national cyber strategy.

1 The Appendix contains a more granular version of the evaluation scorecard as well as further details on the scoring methodology.

4. Introduction

The national cybersecurity strategy is the primary mechanism governments use to communicate a cybersecurity policy concept. These documents articulate guiding principles and outline the steps and actors required to achieve policymakers' cybersecurity vision.

Despite its importance today, national cybersecurity strategy is a nascent and rapidly evolving discipline. As of September 2024, nearly half of the 132 countries with a national cybersecurity strategy had drafted only a single strategy.[2] The earliest cybersecurity strategies appeared around two decades ago and have been updated just a handful of times in the intervening period.

Crafting and implementing a national cybersecurity strategy is a formidable challenge. The cyber domain touches many stakeholders and issues, crossing both local jurisdictions and national borders. Success requires policymakers to navigate complex government bureaucracies, allocate scarce resources, and win buy-in from heterogeneous members of the private sector and civil society. Understandably, it can be difficult to know where to start. Multinational organizations such as the United Nations International Telecommunications Union (ITU) and NATO have published guides for developing national cybersecurity strategies, which offer suggestions for organizing the documents and determining a suitable policy course.[3][4] However, the empirical data reveal there is no global standard approach. Only 85 of those 132 countries address critical infrastructure, lifecycle management, stakeholder engagement, and implementation.[1]

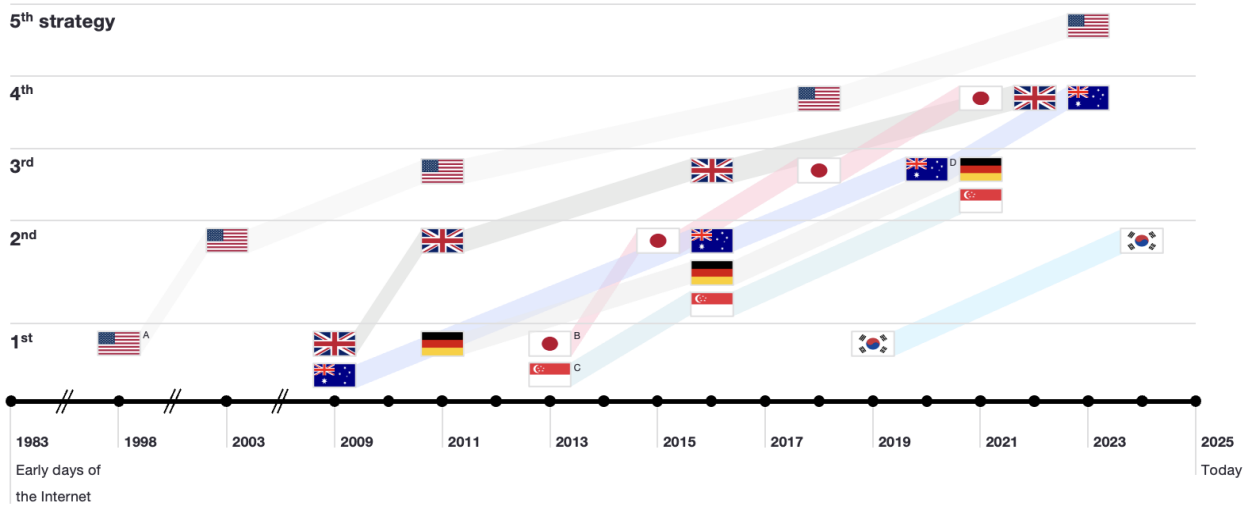
In drafting strategies, many countries look to perceived leaders such as the United States, the United Kingdom, Australia, and Singapore as sources of inspiration, aiming to copy the policies they assume to be the state of the art. Yet it is often unclear which practices are effective, whether they apply in foreign contexts, or if their success depends on conditions like economic or digital resources. Moreover, before even beginning to write a strategy, each government must determine the drafters, intended audience, and scope. We explore some of these issues next.

2 United Nations International Telecommunication Union, Global Cybersecurity Index 2024 (5th ed.), ITU, 2024, https://www.itu.int/dms_pub/itu-d/opb/hdb/d-hdb-gci.01-2024-pdf-e.pdf.

3 United Nations International Telecommunication Union, Guide to Developing a National Cybersecurity Strategy (2nd ed.), ITU, 2021, https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2021-national cybersecurity strategy-guide.pdf.

4 ATO CCD COE, National Cyber Security Strategy Guidelines, NATO, 2013, https://ccdcoe.org/library/publications/national-cyber-security-strategy-guidelines/.

Figure 1: Timeline of selected cybersecurity strategy releases



Notes: A. Refers to PDD 63, the first U.S. national cyber document; B. Ignores earlier acts and policy documents on information security strategy in 2000, 2006, 2009 and 2010; C. Ignores earlier 'Infocomm Security Masterplans' from 2005 and 2008; D. Ignores International Cyber Engagement Strategy documents in intervening years

Key Questions for National Cybersecurity Strategy Drafters

Who should participate in the drafting process?

The assignment of authorship roles carries major implications for the ultimate national cybersecurity strategy product. For a start, the entity responsible for drafting can set the tone and intent of the strategy, as well as determine which resources are prioritized. All else equal, a drafting process run by a military signals intelligence agency such as the U.S. National Security Agency (NSA) will yield a different outcome to the same process undertaken by a law enforcement agency like the Australian Federal Police (AFP), a digital ministry such as Singapore's Ministry of Communications and Information (MCI), or strategic advisory offices such as the U.S. Office of the National Cyber Director (ONCD). Further, today nearly every member of society has a stake in securing the cyber domain, not just the national authorities responsible for making policy. Large corporations, small businesses, government agencies with no cybersecurity remit, educational institutions, and everyday citizens ought to have their interests and perspectives taken into account, not only for the sake of fairness and protection but to ensure their roles as contributors to national cybersecurity are appropriately designed. Certainly, representatives of such groups stand to be consulted during the drafting process. Drafting by committee, however, risks fomenting conflict between stakeholders, promoting excessive compromise at the expense of substance, or ultimately producing a warped strategy that elevates certain drafters' priorities over what is best for the state overall.

Who is the intended audience?

The choice of the national cybersecurity strategy's audience is not as straightforward as it might seem. Among others, drafting authorities must decide whether a strategy is meant for consumption by government bodies or external stakeholders; specific domestic or international groups; society's most or least cybersecurity-capable members; or some blend thereof. These choices affect the direction, scope, and content of

the resulting document. A strategy written to guide interagency coordination may not merit a wide-reaching rollout campaign (or even public release) and is likely to employ large doses of specificity and technical or bureaucratic jargon. On the other hand, a strategy document designed to signal a broader policy vision – for instance, shifting cybersecurity accountability onto corporate service providers or taking a harder line against an adversary – is likely to be shorter, punchier, and less detailed. The latter approach implies a stronger reliance on distributed government agencies for guidance at the middle and granular levels of policymaking. The most comprehensive, visionary national cybersecurity strategy documents are typically intended for mixed audiences of government, non-government, domestic, and international consumers. We explore several countries' distinct audience selections in the Analysis section below.

What is the appropriate scope?

Cybersecurity is a broad domain that necessarily implicates a number of additional fields. The term "security convergence" refers to the fact that modern societies encompass assets in need of both digital and physical protection, from hospitals and nuclear power plants to data centers and individual personal computers. Emerging technologies like artificial intelligence present novel cyber risks and must themselves be secured. The cyber threat landscape also reflects the geopolitical environment, which most countries factor into their strategies. Policymakers may seek to shoehorn favored initiatives into their information security policy. Some governments use it to advance the green transition or market liberalization, while others use it to further censorship and mass surveillance. The domain is further complicated by the transnational and open architecture of the Internet. In short, developing a robust cybersecurity approach requires not only marshaling cross-disciplinary expertise but settling on a definition of "cybersecurity" itself.

National strategies often aim to be comprehensive and organize their content into several sections, commonly referred to as "focus areas," "pillars," or even "shields". The ITU's cyber strategy guide suggests considering seven focus areas: Governance, Risk Management in National Cybersecurity, Preparedness and Resilience, Critical Infrastructure and Essential Services, Capability and Capacity Building and Awareness Raising, Legislation and Regulation, and International Cooperation. Despite common themes, countries still organize their strategies in many different ways. The scope and organization of a strategy can affect how it is interpreted. For example, strategies that omit certain issues that other countries have addressed, such as protecting vulnerable populations, are a clue to the priorities of the policymakers who draft it. This is also true of syntax; placing issues earlier or later in a document can give some sense of relative priority. For this reason, we assess the scope, structure and language use of strategy documents in our analysis.

Which cyber policies should the strategy adopt?

Considering the many overlapping fields and technical complexity that characterize cybersecurity, it can be difficult to identify which policies actually work. For example, how do we know if requiring critical infrastructure companies to be listed on a national register deters attacks or improves response times? It is sometimes difficult or impossible to prove a given measure prevented a bad outcome from occurring. Moreover, when policies designed to deter or mitigate harm succeed, they reduce the amount of offensive data available to measure effectiveness. The vast number of exogenous factors that influence the number and type of cyber attacks also complicate the picture, making it virtually impossible to establish a causal relationship between cybersecurity policy and its impact.

Furthermore, political context can quickly make a cyber "best practice" infeasible since it may interfere with

established country-specific rights or norms. For example, the United States cannot implement a "Great Firewall" that blocks undesirable network traffic, regardless of how well such a system might prevent attacks in authoritarian countries. A similar phenomenon also occurs at the level of partisan politics; many national cybersecurity strategies reflect the political priorities of the governing party, which may not hold across international borders or even within the same country over time. Comparing cybersecurity strategies across nations is thus not always straightforward or fair.

Prior Analyses of National Cyber Policy

Existing benchmarks for evaluating national cyber posture include the ITU's Global Cyber Index[5], MIT's Cyber Defense Index[6], and the Belfer Center's National Cyber Power Index (see Table 1).[7] Each of those projects offers useful insights, but they share four overarching limitations, which we explore below.

Table 1: Summary of prior national cyber policy analyses, as well as this report.

Name	Rating system	Geographic scope	Collection mechanisms	Most recent date
National Cyber Power Index (Belfer Center)	Numerical score out of 100 and ranking, assessment of capabilities weighted by intent	30 major global states	Desk research covering national strategies and known cyber operations	2022
Cyber Defense Index (MIT)	Numerical score out of 10, weighted based on categories	20 major economies	Secondary data on digital technology adoption and regulatory policies and a global survey of 1000 senior executives	2023
Global Cybersecurity Index (UN ITU)	Numerical score out of 100	All UN member states	Self-reported questionnaire results based on best practices and desk research	2024
This report **Cybersecurity Strategy Scorecard** (Belfer Center)	Relative scores presented as leading, meeting the bar, or lagging	7 major cyber powers	Desk research covering national strategies and expert interviews	2025

Challenge 1: Building meaningful benchmarks

Several existing comparisons aggregate their country assessments into a single "score," which can be misleading for two reasons. First, quantitative assessments of best practices rely on arbitrary weightings. For example, they may rate critical infrastructure protections as more important or effective than cyber workforce

5 United Nations International Telecommunication Union, Global Cybersecurity Index 2024 (5th ed.), ITU, 2024, https://www.itu.int/dms_pub/itu-d/opb/hdb/d-hdb-gci.01-2024-pdf-e.pdf.

6 MIT Technology Review, Cyber Defense Index 2022/23, MIT, 2023, https://www.technologyreview.com/2022/11/15/1063189/the-cyber-defense-index-2022-23/.

7 Voo et al, National Cyber Power Index 2022, Belfer Center for Science and International Affairs, Harvard Kennedy School, 2022, https://www.belfercenter.org/publication/national-cyber-power-index-2022.

development, but such value judgments are highly subjective and hard to justify. Second, aggregating different cyber policy initiatives into a single score implies they are interchangeable. This approach creates uneven comparisons, such as combining the aforementioned critical infrastructure protections and workforce development initiatives, which are wholly different policy areas with distinct aims and impacts. Instead, effective benchmarks should recognize that there is no one-size-fits-all approach to cyber policy. What works in one context, like big enterprise, is seldom wholly transferable to another, like government agencies or small nonprofits.

Researchers often rely on arbitrary estimates of effectiveness when setting baselines for measuring cyber performance. For example, in the ITU's 2024 Global Cybersecurity Index, the United States scored 99.86 out of 100 points based on self-reported performance against the ITU's list of best practices. Of course, this near-perfect score does not imply that the United States can withstand almost any cyberattack or that it is inherently less vulnerable than countries with lower scores. While the score might suggest the United States has implemented all known national cybersecurity measures – a claim even U.S. policymakers would likely not make – the threat landscape evolves so quickly that these benchmarks require constant updates or quickly become meaningless. As a result, the United States' perfect score of 100 on the 2020 Global Cybersecurity Index is not at all comparable to its 99.86 score in 2024.

Challenge 2: Measuring outcomes rather than process or inputs

Many existing cybersecurity posture benchmarks measure process implementation and inputs rather than outcomes. They may count the implementation of best practices, progress toward achieving a list of pre-set goals, the size of the market, or the number of cybersecurity employees or students in a country. Yet measuring the implementation of cybersecurity processes or inputs is an analytical trap since many factors can prevent the intended effect from being realized. For example, having a process in place does not mean it is effective, and having more resources does not guarantee protection. On the contrary, the existence of processes may contribute to a false sense of security, and more digital assets represent a wider attack surface. It is also difficult to "weigh" the effectiveness of different processes or inputs in building effective cyber defense. As noted above, are critical infrastructure processes more important than educating large numbers of cyber experts? These issues can lead to arbitrary scoring.

Challenge 3: Providing robust, transparent justifications for evaluations

It is difficult enough to assess the quality and effectiveness of a given country's approach to cybersecurity by examining real-world indicators such as laws, spending, documented capabilities, and data-based metrics. In addition to the challenges associated with establishing causation described above, governments typically do not publish sufficient data to perform such analysis and classify sensitive information about their cyber intelligence and military capabilities that would shape any assessment. Statements of intent and survey results are particularly unreliable indicators of a given country's security posture. Governments may genuinely wish to implement certain decisions, like activating an offensive cyber force, but find themselves unable to do so or eventually change their minds. In other cases, governments inflate their accomplishments or capabilities in order to boost international prestige, cultivate domestic political support, or deter adversaries. Therefore, cyber posture comparisons that rely on such sources may lack a strong rationale for their results. Indeed, it is implausible that Bangladesh (96.96 out of 100) outperforms Australia (96.24 out of 100) or that Egypt (100 out of 100) exceeds Japan (97.58), as the ITU Index suggests.

Challenge 4: Moving beyond established best practices

Most existing benchmarks rely on lists of established best practices to evaluate countries' cyber postures. These best practices are often understood in measures of cyber performance assessed after an incident has occurred. Such measures include the annual net cost of cyberattacks or mean time to detect a vulnerability. While this approach is a useful starting point, the rapidly developing technical landscape requires policymakers to look ahead to the best practices of tomorrow rather than merely being satisfied with what works today. Thus, evaluating best practice adoption rates can provide a baseline measure of effective protection right now, but it fails to indicate which policies are most likely to be effective against future threats.

5. Methodology

In this section, we outline our methodology for assessing national cybersecurity strategies using a novel approach based on relative comparisons, qualitative assessments, and intent measurement. By assessing publicly available documents and testing our findings in interviews with experts and sitting officials, we have sought to ensure transparency, rigor, and a broad scope. We recognize the limitations associated with performing cross-country comparisons and restricting our evaluation to strategy documents rather than implementation results. However, our research is designed to maximize the utility of comparative benchmarking while preserving analytical rigor, which helps us highlight noteworthy policy innovations and illuminate key differences in strategic thinking. Thus, we firmly believe our report provides valuable insights for future cybersecurity strategy drafters.

Our evaluation classifies each country as "Leading," "Meeting the Bar," or "Lagging" against their six peers for the 70 elements of the framework. These designations are not mutually exclusive – in any given area, multiple countries may receive the same score, and every score does not need to be applied in every case. This provides a more reliable basis for evaluation than assigning absolute numerical scores[8], which can be arbitrary or misleading. To supplement our method, we provide an extensive written analysis that guides readers toward aspects of the evaluation that are especially interesting, for instance, policies that showcase innovation, reveal important policy gaps or otherwise merit further attention. In doing so, we aim to create a benchmarking tool to assist policymakers in drafting future national cybersecurity strategies.

Analyzing strategy documents

We analyzed seven countries' national cybersecurity strategy documents based on the evaluation framework presented in Figure 3 below. For each country, we also assessed a small number of supporting documents that relate directly to the national cybersecurity strategy. For example, our evaluation of the U.S. approach accounted for the National Cyber Workforce and Education Strategy, a core element of Washington's vision for workforce development mentioned explicitly in the main strategy document and without which consideration of the strategy's workforce development element would be incomplete. Since this project focuses on national cyber strategy, not the overall state of national cybersecurity, we deliberately excluded most strategy documents not directly related to the national strategy, as well as legal frameworks, regulations, executive orders, enforcement measures, and so on. It would be infeasible to assess every government document or

8 "Absolute" scoring refers to the common practice of assigning standalone numerical grades out of a given total before comparing with other scores, as opposed to assigning scores based on relative comparisons.

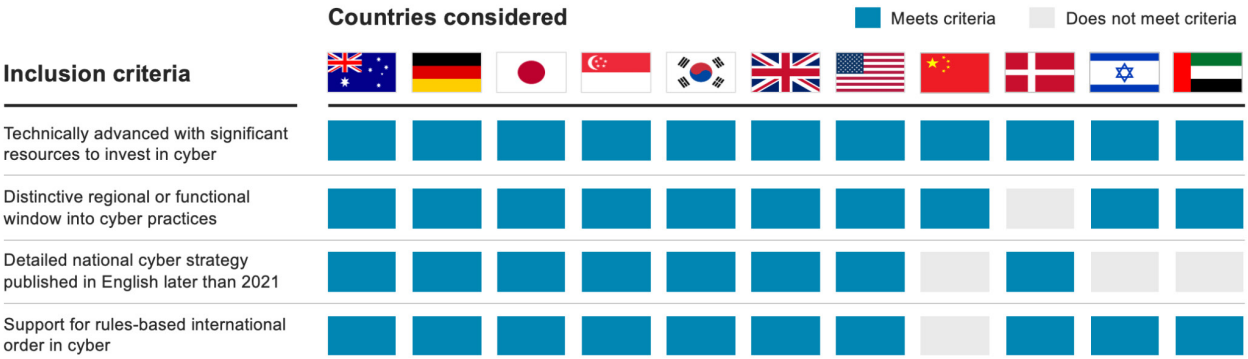
action with some relevance to national cyber policy. The one exception we made was for critical infrastructure, a particularly important area many countries address in standalone legislative or regulatory frameworks that the strategies typically reference but do not discuss in detail.

Inclusion criteria

We selected seven national strategies based on four key criteria. Specifically, each selected country:

- Is technically advanced and has considerable resources to invest in cybersecurity[9];
- Offers a distinctive window into particular functional or regional cybersecurity approaches;
- Has published, in English and no earlier than 2021, a national cybersecurity strategy of sufficient depth to evaluate in detail; and
- Supports and participates in the rules-based international order.

Figure 2: Evaluation of a subset of countries considered for this analysis against our inclusion criteria



The project assesses no more than two states from any major region, and the pairs that hail from the same neighborhood represent significantly different approaches. For instance, South Korea's strategy is oriented primarily around national security, while Japan's focuses on the economic aspects of cybersecurity. Germany's strategy sheds light on the broader EU cyber outlook, while the United Kingdom's resembles more of a blend with those of the United States and Australia. We had hoped to include at least one Middle Eastern country, such as Israel, Saudi Arabia, or the United Arab Emirates, but none met all the inclusion criteria, mainly because their national strategies lacked detail or were out of date.

Expert interviews

We supplemented the textual analysis with extensive interviews, including scholars and practitioners from all seven countries. Of the three dozen interviewees, most are current or former cyber policy officials, while a handful are private-sector or think-tank experts. After completing the initial assessment, we asked more than

9 Each selected country is classified as Tier 1 - Role Modeling in the ITU's 2024 Global Cybersecurity Index (see Annex, p. 24), is designated high-income by the World Bank, and has a top-30 GDP.

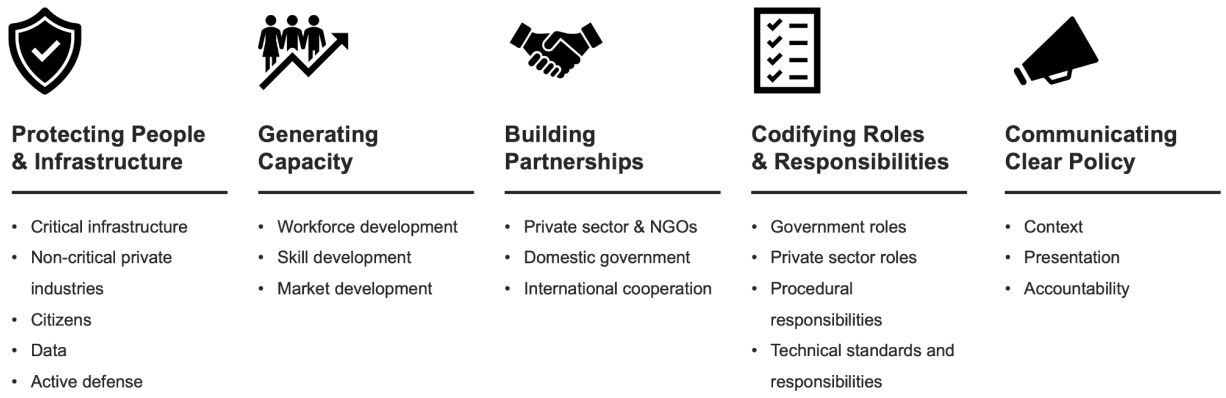
a dozen experts and officials, together representing each country included in the report, to perform a detailed review of the results. Belfer Center colleagues also provided in-depth feedback.

Evaluation Framework: The Cybersecurity Strategy Scorecard

Our assessment criteria are divided into five categories:

- **Protecting People and Infrastructure** assesses the strategies' plans for national cyber defense, accounting for components like critical infrastructure, personal data, supply chains, SMEs, and vulnerable populations.
- **Generating Capacity** analyzes each state's approach to developing people and institutions with the abilities required to contribute to national cybersecurity.
- **Building Partnerships** measures the strategies' plans for cooperation with domestic and international stakeholders.
- **Codifying Roles and Responsibilities** measures how clearly each country assigns duties and authority to its various cyber-relevant agencies and how clearly it establishes procedural and technical requirements, like incident reporting.
- **Communicating Clear Policy** takes stock of how well each country articulates its strategy and establishes systems of accountability and implementation.

Figure 3: The Cybersecurity Strategy Scorecard - categories and sub-categories



The five categories cumulatively contain 18 sub-categories and 70 subject elements, listed in full in the Appendix. For example, the "Codifying Roles and Responsibilities" category contains a "Government Roles" sub-category with elements like "Regulatory Agencies" and "Law Enforcement," which measure how well each country assigns cybersecurity responsibility to and empowers those entities. To reduce subjectivity, we created 268 binary criteria for determining a country's strategy's standalone performance in each element, which helped inform our comparison but is not presented in the report. Figure 4 in the next section presents our comparative evaluation at the sub-category level. The complete scorecard, with scores across all 70 elements, is presented in the Appendix.

Our Approach

Our novel method of comparing cybersecurity strategies addresses the limitations of prior evaluations, as outlined in the Background Section, by adopting three distinct features, namely:

1. **Relative comparisons** - We compare each country to the other six and adjust the scores based on their relative performance. This allows us to highlight leaders in policy innovation without having to rely on a rigid, presupposed definition of established best practices.

2. **Measuring intent** - We analyze the vision each strategy outlines, rather than attempting to measure implementation or outcomes. While this approach does not assess actual cybersecurity performance, it avoids the pitfalls of navigating confounding variables or assuming that successful implementation alone is a sufficient condition for success in a cyber strategy. It also places the focus on leading-edge innovation in cyber policy, which may be a leading indicator of cybersecurity performance, unlike lagging outcome indicators.

3. **Relying on publicly available documentation and expert interviews** - We have restricted ourselves to evaluating the publicly available documentation on cybersecurity strategy, supplemented with expert interviews. This approach enables us to justify our analysis robustly based on materials in the public domain and to avoid imprecise measures like surveys. The expert interviews helped ensure that our analysis treated each strategy fairly, accurately, and comprehensively.

Limitations

Evaluating and comparing national policy approaches introduces several problems. Even when restricting the analysis to high-income, technologically advanced states that support the rules-based international order, confounding variables like political structures, existing cyber postures, and national budgets make cross-country comparisons perilous. Should states with stronger civil liberties protections, like Germany and the United States, be penalized for envisioning less robust intelligence-gathering and threat-sharing programs than their more illiberal peers? Is it fair to compare the United States and Singapore's plans for research and development investment, considering that the former's GDP was almost 55 times greater in 2023?[10] Moreover, each country's strategy is rooted in its own lexicon, which may feature varied definitions of common terms and concepts. Certain states classify topics like data privacy or artificial intelligence governance as components of cybersecurity, while others view them as distinct fields and therefore do not address them in their strategies. As researchers at the German Council on Foreign Relations have found, official definitions of critical infrastructure also vary widely.[11] Should a country that publishes its AI security strategy as an external document or does not designate as essential its small manufacturing sector be penalized for insufficient comprehensiveness? Given the pace of change in the computer security field, strategies that seemed cutting-edge only a few years ago may now be outdated. Accordingly, our scores are unavoidably biased in favor of more recent strategies, whose authors have learned from earlier documents and better account for emerging risks like ransomware or generative AI. In future iterations of this exercise, the selected countries will have released new strategies, which will affect all relative scores.

10 World Bank Group, GDP in current USD, https://data.worldbank.org/indicator/NY.GDP.MKTP.CD.

11 For example, while nearly all countries designate energy systems as essential, only 45% treat national security systems as such: Dr. Valentin Weber et al, "Mapping the World's Critical Infrastructure Sectors," German Council on Foreign Relations, November 2023, https://dgap.org/en/research/publications/mapping-worlds-critical-infrastructure-sectors.

Capacity constraints and limited information availability have compounded these challenges. As noted above, we restricted the project's scope to core cybersecurity strategy documents and closely related materials for the sake of feasibility. Furthermore, our research analyzes the national cybersecurity strategy, not the operational state of national cybersecurity. These restrictions result in non-trivial information loss, both because the out-of-scope materials are significant and cyber policymaking is a dynamic endeavor that changes between the publication of one strategy and its successor. In addition, much cyber policy information, particularly related to offensive capabilities, is not publicly available and, if factored into our analysis, might have led to different conclusions or higher scores. This consideration is especially relevant for South Korea, whose strategy is organized principally around developing stronger offensive cyber capabilities. As practitioners from multiple countries reminded us, the available materials are political in nature and often express aspirations or fragments rather than on-the-ground realities. Researchers possess a limited capacity to read between the lines or judge a country's true intent based on its strategy alone.

Relative scoring comes with its own challenges. While it helps emphasize standout performers even when all selected countries perform similarly, the relative-scoring method does not distinguish between close calls or wide gaps, except where highlighted manually. Nor does it capture differences with the same precision of a numerical system. Of course, there is still room for human bias during the scoring and implementation, but we believe the advantages of relative scoring far outweigh its drawbacks.

We acknowledge these potential shortcomings in the spirit of forthrightness, not because we believe the conclusions that follow are unsound. This report is the product of thousands of hours of rigorous analysis, several dozen interviews with experts and practitioners, and a review process incorporating internal and external scrutiny. We are confident in its robustness and usefulness as a tool for future strategists and researchers.

6. The Cybersecurity Strategy Scorecard

This section contains our evaluation of the seven national cybersecurity strategies. First, we present findings across the five categories, identifying areas where national strategists tended to excel, fall short, innovate, or diverge. The overall trends indicate a strong performance in building partnerships with industry and foreign partners, as well as in assigning clear cybersecurity roles and responsibilities. Common shortcomings involved devoting insufficient attention to protecting vulnerable populations, building sub-national capacity, developing the workforce, and incentivizing private-sector investment in cybersecurity. We then present individual scorecards for each country, offering more detailed commentary and highlighting elements that stand out as positive, negative, or worthy of emulation. The Appendix displays a more granular version of the scorecard that assesses each country against 70 elements contained within the sub-categories, totaling 490 scores.

Figure 4: The Cybersecurity Strategy Scorecard evaluates the seven countries across five categories, which include 18 sub-categories in total. The Appendix includes an even more detailed version of the scorecard, including several elements for each subcategory.

Category	Sub Category	Australia (2023)	Germany (2021)	Japan (2021)	Singapore (2021)	South Korea (2024)	UK (2022)	US (2023)
Protecting People and Infrastructure	Critical infrastructure	Leading	Meeting the bar	Meeting the bar	Leading	Meeting the bar	Meeting the bar	Leading
	Non-critical private industries	Leading	Meeting the bar	Meeting the bar	Leading	Lagging	Leading	Leading
	Citizens	Leading	Meeting the bar	Leading	Leading	Lagging	Meeting the bar	Lagging
	Data	Leading	Leading	Meeting the bar	Meeting the bar	Meeting the bar	Leading	Lagging
	Active defense	Meeting the bar	Meeting the bar	Meeting the bar	Meeting the bar	Leading	Meeting the bar	Leading
Generating Capacity	Workforce development	Meeting the bar	Lagging	Meeting the bar	Meeting the bar	Lagging	Meeting the bar	Meeting the bar
	Skill development	Leading	Meeting the bar	Leading	Leading	Meeting the bar	Leading	Meeting the bar
	Market development	Meeting the bar	Meeting the bar	Leading	Meeting the bar	Meeting the bar	Leading	Leading
Building Partnerships	Private sector & NGOs	Meeting the bar	Leading	Leading	Leading	Meeting the bar	Meeting the bar	Leading
	Domestic government	Lagging	Meeting the bar	Leading	Meeting the bar	Meeting the bar	Leading	Meeting the bar
	International cooperation	Meeting the bar	Meeting the bar	Meeting the bar	Leading	Leading	Meeting the bar	Leading
Codifying Roles and Responsibilities	Government roles	Leading	Meeting the bar	Meeting the bar	Leading	Meeting the bar	Meeting the bar	Leading
	Private sector roles	Meeting the bar	Meeting the bar	Meeting the bar	Meeting the bar	Meeting the bar	Meeting the bar	Leading
	Procedural responsibilities	Leading	Meeting the bar	Meeting the bar	Leading	Meeting the bar	Leading	Leading
	Technical standards and responsibilities	Meeting the bar	Meeting the bar	Meeting the bar	Meeting the bar	Meeting the bar	Meeting the bar	Leading
Communicating Clear Policy	Context	Meeting the bar	Leading	Meeting the bar	Meeting the bar	Leading	Leading	Leading
	Presentation	Leading	Meeting the bar	Meeting the bar	Meeting the bar	Meeting the bar	Meeting the bar	Leading
	Accountability	Meeting the bar	Meeting the bar	Meeting the bar	Meeting the bar	Meeting the bar	Meeting the bar	Leading

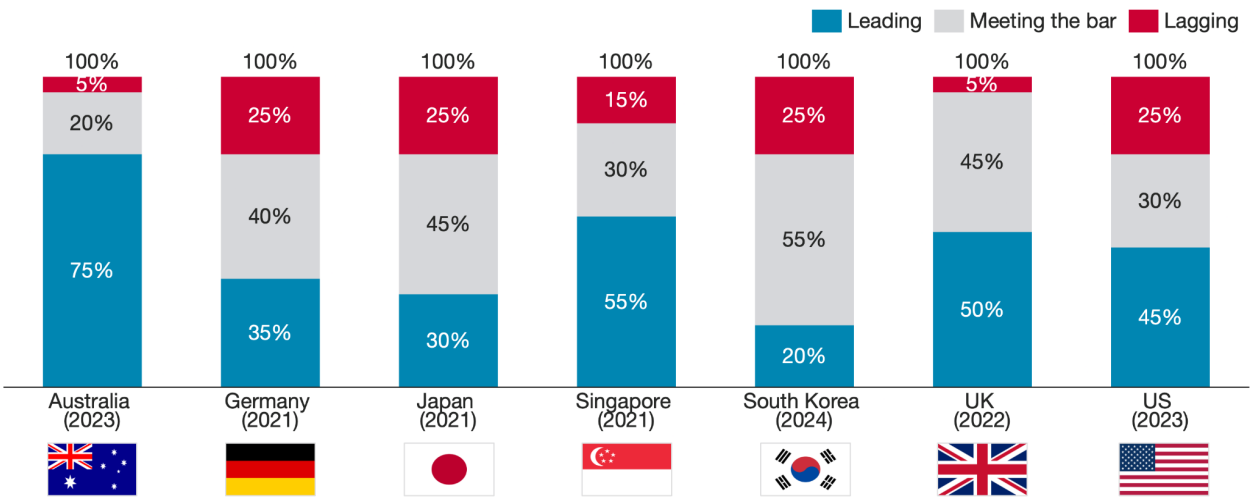
6.1 Global Trends by Category

Protecting People and Infrastructure

All strategies in our sample prioritize protecting both people and infrastructure, but their focuses diverge sharply. The proportion of leading scores in this category was the second lowest across the five in our framework, and the proportion of lagging scores was the second highest. Still, even though most countries received average scores, a few stood out with strong visions. Some countries, such as the United States, focus on securing critical infrastructure, while others, such as Japan, focus on protecting individuals, and many leave gaps exposing entire sectors or population groups, like the elderly. Thus, it is important to scrutinize who cybersecurity policies choose to protect and who they are leaving behind. All strategies from our sample have a strong focus on protecting large private enterprises. Most build on critical infrastructure security policy with comprehensive cybersecurity legislation, such as Singapore's Cybersecurity Act, Australia's Security of

Critical Infrastructure Act (SOCI), and the United Kingdom's strategy for the telecommunications sector. The strategies consistently focus on building resilience through initiatives such as modernizing IT infrastructure, replacing legacy systems, adopting zero-trust architectures, and enforcing multi-factor authentication. Some strategies, such as Singapore's, also include initiatives to make it easier for governments to launch investigations of insecure infrastructure. Government systems and communication technologies are best addressed, while other infrastructure systems, such as critical manufacturing and health services, are often neglected. The strategies also devote much attention to leveraging private sector capacity for government cybersecurity work. However, small and medium-sized enterprises receive far less attention than larger corporations.

Figure 5: Each country's performance in Protecting People and Infrastructure. The blue, gray, and red bars denote the percentage of element-level scores that are "Leading," "Meeting the bar," and "Lagging" compared to the other countries.



The strategies devote considerable thought and attention to protecting people, but their approaches differ. Private citizens are often mentioned, including various schemes to protect end users and shift the liability from users to organizations, but vulnerable population groups and civil society organizations are largely neglected. The United States' strategy centers around a top-down approach to protecting individuals by incentivizing major providers to invest in security and streamline regulations, hoping this will affect all users positively. In contrast, the European countries in our sample opt for a more regulation-driven approach, which contrasts the U.S. emphasis on streamlining regulation but leads to fewer gaps. For instance, the development and adoption of GDPR led to Germany and the United Kingdom receiving strong scores for personal data protection, while the United States has no nationwide equivalent. Other countries adopt more bottom-up approaches to protecting individuals. For example, Australia's strategy emphasizes victim support services rather than regulations. Japan's strategy champions individual protection via its "Cybersecurity for All" initiative. This approach elevates protections for individuals and SMEs, promotes digital literacy, and shields institutions with limited cybersecurity capabilities, such as universities. Singapore employs a hybrid top-down and bottom-up approach, combining zero-trust architecture regulations with the direct provision of data protection services for SMEs. Thus, we see that while top-down and bottom-up approaches to individual protections are not mutually exclusive, most strategies lean one way or the other. The results invite one to ask how countries can balance robust protection of major sectors with the needs of niche and vulnerable parts of society.

Table 2: Summary of common strengths in Protecting People and Infrastructure

Strength	Notable Examples
Securing key critical infrastructure sectors, especially IT and telecommunications	**Australia** - SOCI Act **UK** - Telecommunications sector cybersecurity strategy
Protecting the private sector, especially large-scale enterprises	**Australia** - Cyber Wardens program **UK and Singapore** - Cyber Essentials program
Protecting the general population	**Singapore** - Safer Cyberspace Masterplan **Australia** - Victim support services **Japan** - Theme of Cybersecurity for All

Table 3: Summary of common weaknesses in Protecting People and Infrastructure

Weakness	Explanation
Updating supporting documentation	Many countries have updated their strategies but not the supporting documentation. A notable example is Germany's critical infrastructure protection plan, which was last updated in 2009.
Engaging civil society and addressing the needs of vulnerable populations	Most countries discuss protecting businesses and citizens but neglect to consider how the needs of civil society organizations and vulnerable populations (such as the young, elderly, or minorities) might differ or require extra resources. There are some notable exceptions to this, including Japan and Australia.
Protecting specific CI segments, like critical manufacturing	While critical infrastructure is well covered, we observe that many countries do not consider distinct protections for niche sectors like critical manufacturing.
Building centralized approaches to data privacy	When they are addressed, data privacy standards are often scattered and insufficient, except for the notable emphasis on GDPR in Germany and the UK.
Advocating for security best practices	The strategies typically do not address security best practices, often lacking detail on technical standards, system modernization, and how the population should be made aware of these.

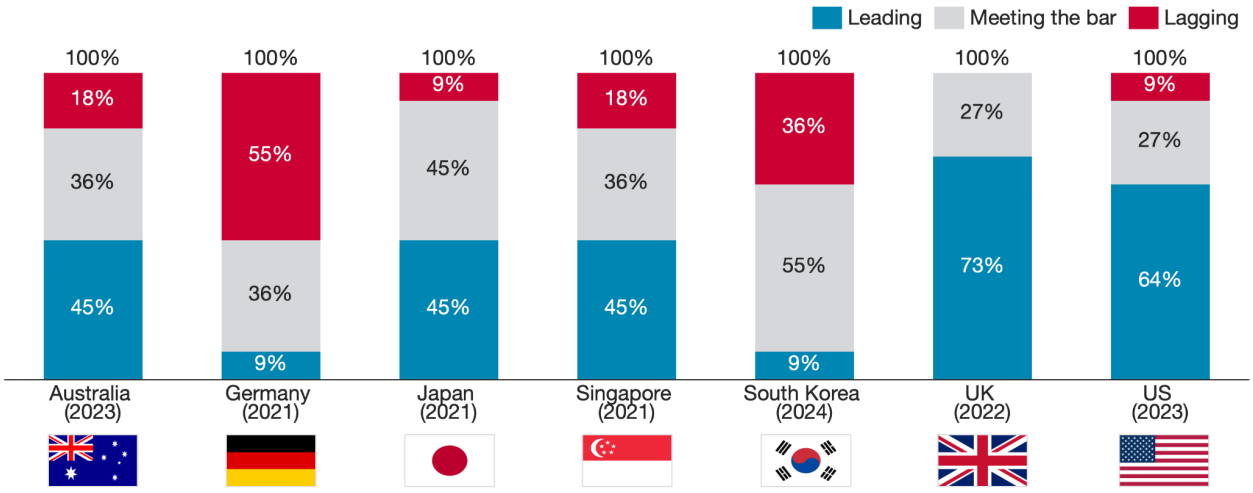
Generating Capacity

Generating Capacity was the worst performing category, receiving the highest proportion of lagging scores and the lowest proportion of leading scores. However, the results were skewed by strongly lagging results from Germany, which largely neglects capacity generation in its strategy. Aside from Germany, most countries demonstrate a strong commitment to growing their technical cybersecurity workforce, both within the government and the private sector. Even so, countries generally neglect to consider how to generate capacity for non-technical practitioners, such as cyber-specialized lawyers and policymakers. This knowledge deficiency

can lead to regulatory gaps, ineffective policies, legal vulnerabilities, inefficient cross-sector collaboration, and missed opportunities in international cyber diplomacy.

Initiatives targeting education and awareness-building, such as the UK's CyberFirst initiative and Australia's publicly available cyber awareness platforms, are common, demonstrating positive trends in raising public and industry-wide cyber competence. Australia's strategy exhibits a noteworthy bottom-up initiative to foster cyber literacy by empowering community organizations to deliver tailored cyber awareness campaigns to diverse groups. This is a rare, strong example of leveraging community knowledge to improve the reach and impact of cyber awareness campaigns. This approach ensures that education is tailored to the needs of different communities, both culturally and linguistically. However, although most strategies mention similar awareness-raising initiatives and ambitions, it is uncertain whether these programs are likely to be used or if they will be useful in practice, raising the question of whether countries aspire to genuinely raise public awareness or merely pay lip service to the issue.

Figure 6: Country performances for Generating Capacity.



The strategies propose many ways to strengthen the cyber workforce, including supporting education, research, and emerging technology firms. For example, the US CyberCorps program supports students who pursue cybersecurity degrees and later serve in federal, state, local, or tribal government roles, the UK's CyberFirst Girls Competition aims to inspire girls interested in technology to pursue a career in cybersecurity, and Singapore offers a program to support youth, women, and mid-career professionals to pursue a career in cybersecurity. Research institutions and emerging technology firms are often highlighted as mechanisms for market development. Germany stands out in this regard by creating an agency for cybersecurity innovation. Many strategies outline funding proposals for emerging technology firms, like the UK's Cyber Runway Program, providing access to funding, expertise, and mentorship to startups and innovators or many countries' research initiatives to support post-quantum cryptography innovation. All countries seek to grow the workforce, but approaches differ. Japan's strategy emphasizes upskilling of the existing workforce through training programs. Australia's strategy, on the other hand, highlights immigration as a mechanism to build capacity. South Korea, on the other hand, proposes building military cyber capabilities and alludes to establishing a military-to-industry cyber pipeline that resembles the Israeli model. Most countries discuss developing national cybersecurity industries, but it is not clear how countries with smaller economies would support the creation of internationally competitive cybersecurity firms. Singapore thus prioritizes verifications

and certifications, perhaps implicitly recognizing that it's unlikely to compete with the U.S. private sector. Few strategies focus adequately on developing the general technology workforce.

Table 4: Summary of Common Strengths in Generating Capacity

Strength	Notable Examples
Expanding the technical workforce, including professional upskilling and training programs	**Australia** - Building a peak body for cyber professionals **USA** - National Cyber Workforce and Education Strategy
Building education and awareness	**Australia** - cyber.gov.au awareness website **UK** - CyberFirst **Singapore** - SG Cyber Talent initiative
Developing emerging technology firms	**UK** - AI and quantum innovation hubs; focus on dual-use technology and embedded cybersecurity **Japan** - Effectiveness verification platform; specific provisions for AI and quantum **Australia** - Safe use of emerging tech (AI, quantum); standards for post-quantum cryptography
Supporting institutional cyber research	**Germany** - Agentur für Innovation in der Cybersicherheit GmbH (Agency for Innovation in Cybersecurity) **UK -** NCSC Applied Research Hub **USA -** Federal Cybersecurity Research & Development Strategic Plan, including ongoing funding Federally Funded Research & Development Centers (FFRDCs) in cyber research such as the NSF and DOE National Laboratories

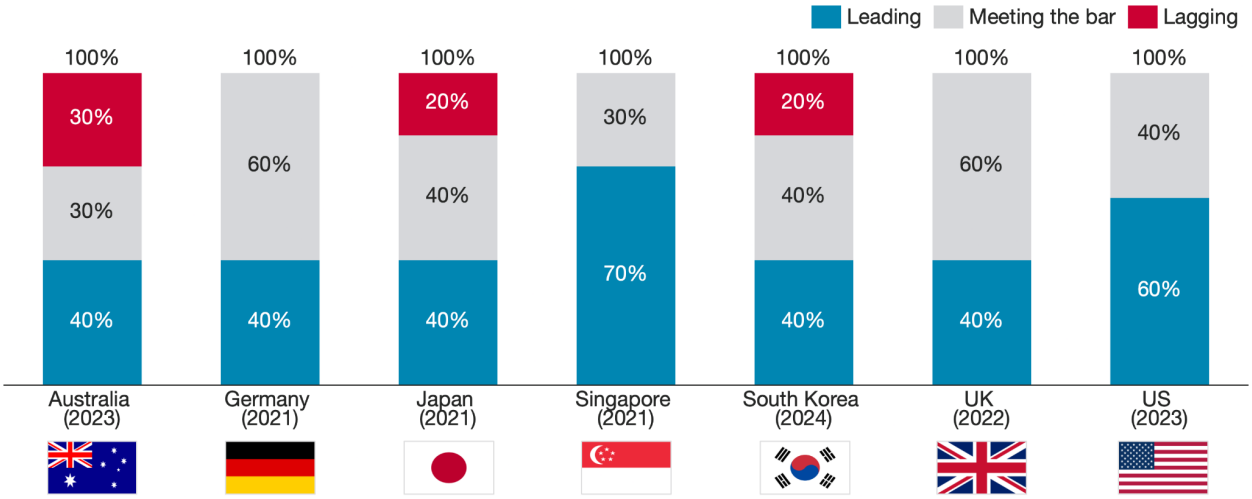
Table 5: Summary of Common Weaknesses in Generating Capacity

Weakness	Explanation
Developing the non-technical cyber workforce, including lawyers and policymakers	Most countries discuss how to build general cyber awareness and deepen education pipelines for technical cyber specialists but do not discuss how non-technical expertise in cyber law and policy should be developed further
Building skills across the general tech workforce	Many countries fail to consider how technical cybersecurity education should feature in software engineering and computer science courses in general (outside of cybersecurity specialties)
Generating local and regional law enforcement capabilities	Most countries do not discuss how law enforcement capabilities related to cybercrime will be uplifted at the local and regional level, e.g., through earmarked funds or personnel rotations through different levels of law enforcement

Building Partnerships

Partnerships are a core focus of all strategies. This category received the second highest proportion of leading scores and second lowest proportion of lagging scores across all countries, equal to the Communicating Clear Policy category. The main themes across all countries are building domestic non-government partnerships with private companies and research institutes. Common mechanisms to foster collaborations include reducing bureaucracy and increasing communication. For example, the UK's Industry 100 scheme and the US's Joint Cyber Defense Collaborative (JCDC) initiatives aim to facilitate information sharing between industry experts and government practitioners by removing information barriers, such as by granting selected individuals from government security clearance requirements when contributing to state cyber initiatives. Domestic cooperation across government bodies is also a common focus. Some countries, like the United States and Germany, aim to follow a distributed model of cyber authority, where multiple agencies share responsibilities across different sectors. The U.S. strategy highlights collaboration between the Department of Homeland Security, the Department of Defense, the FBI, and intelligence agencies to achieve a multi-agency approach to cyber threats at the national level. Germany's strategy emphasizes cooperation between federal and state authorities, with specific agencies like the BSI (Federal Office for Information Security) playing a pivotal role. However, the distribution of authority can affect the ability to execute cyber policy. Germany, for instance, experiences a significant power imbalance. The federal government lacks authority to enforce cyber laws, policies, and regulations in the states, hampering efforts at building a coherent and unified approach to national cybersecurity strategy.

Figure 7: Country performances for Building Partnerships.



On the other hand, countries like Singapore and Japan have adopted top-down, centrally coordinated models, where central agencies hold significant control. Singapore's Cyber Security Agency (CSA) directly manages policy implementation and coordination with the private sector. The centralized structure allows for more direct control and faster decision-making, though it relies heavily on the agency's capacity to manage a wide range of sectors. Regardless of the model, each country's strategy underscores the importance of continuous improvement in interagency collaboration to ensure quick incident response, effective resource allocation, and a coherent cyber defense.

The strategies also strongly emphasize international collaboration, with a wide range of successful examples

including international homogenous collaborations such as Five Eyes, regional partnerships sometimes coordinated through agencies such as ENISA, and international heterogeneous collaborations like the Budapest Convention to Fight Cybercrime. However, the type of partnership prioritized differs across countries. For example, Australia's strategy has a clear focus on regional and international partnerships, but only mentions local- and state-government partnerships in passing, whereas Germany discusses state-government partnerships in some detail. Few countries devote attention to partnerships with civil society organizations and local governments despite calling for initiatives like workforce development and awareness-raising that require grassroots involvement. While it is pragmatic to first prioritize industry and governmental partnerships, the lack of local government engagement and insufficient collaboration with civil society and local law enforcement are causes for concern. Local partnerships are crucial for achieving swift incident response, especially with respect to incidents targeting vulnerable populations and SMEs, and without them, national cybersecurity efforts risk being top-heavy and incomplete.

Table 6: Summary of common strengths in Building Partnerships

Strength	Notable Examples
Collaborating between government, industry, and research institutes	**Singapore** - National Cybersecurity R&D Programme (NCRP) **Australia** - Investments in enterprise-level cybersecurity innovation
Cooperating at the level of national cyber agencies	**USA** - Joint Ransomware Task Force (CISA and FBI)
Cooperating to build expertise at the regional level	**Singapore -** ASEAN cyber vision via exchange programs and collaborative CERT networks **Germany -** ENISA, plus plans for contributions to EU and NATO cyber initiatives
Combating cybercrime at the global level	**USA, UK, Singapore, and Australia -** Counter Ransomware Initiative **USA, UK, and Australia** - Five Eyes **Australia, USA, UK, Germany, Japan, and Korea** - Budapest Convention

Table 7: Summary of common weaknesses in Building Partnerships

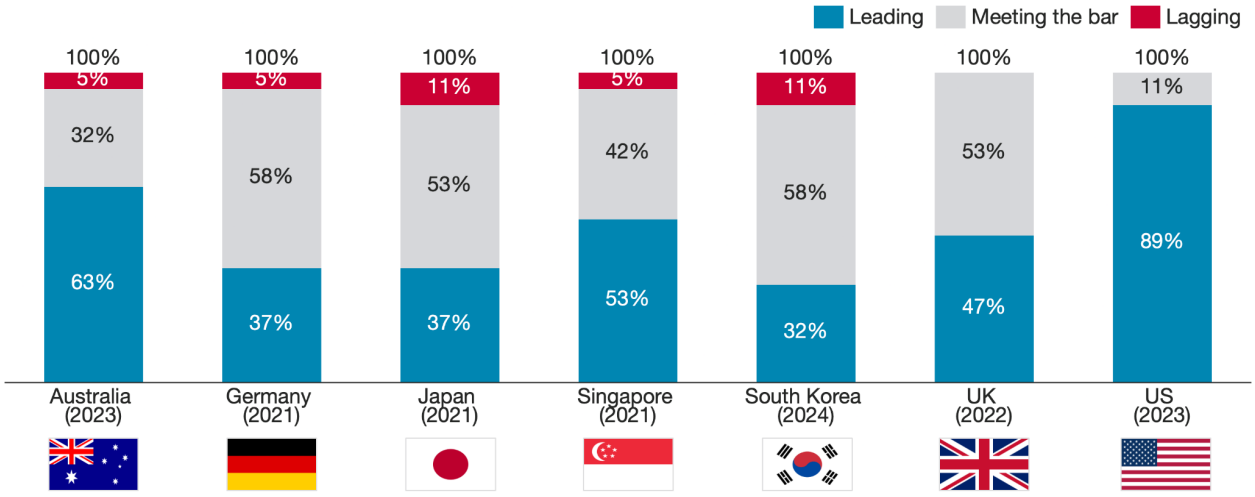
Weakness	Explanation
Partnering with civil society	Most countries fail to discuss how partnerships with civil society, including NGOs, could be leveraged for national security purposes
Cooperating with state and local government	Local governmental partnerships are often mentioned in the passing but generally lack meaningful detail, implementation plans, or a discussion of responsibilities
Building international technical standards	Few strategies address how to work with the international community to improve technical standards

Codifying Roles and Responsibilities

Codifying Roles and Responsibilities was the category that received the highest proportion of leading scores and the lowest proportion of lagging scores. The strategies tend to thoroughly discuss the appointment of national cyber coordinators and envision strong, dedicated cybersecurity agencies. Most emphasize the role of foreign ministries, highlighting an understanding of the need for international partnerships, protection of shared resources like the Internet, and global information sharing. Some countries call for appointing cyber ambassadors and dedicate entire sections of their strategies to international cyber policy. The strategies also acknowledge that cybersecurity agencies have been forced to grow rapidly in recent years, driven by the increasing complexity of cyber threats, society's technical dependency, and the need for quick, decisive action. The high scores throughout this category reflect in part the effective structure of many cyber agencies, several of which operate with the mindset of startups within the government to avoid being slowed by bureaucracy.

There is a consensus among both strategy documents and experts that cybersecurity agencies need to continue to mature, but it's not certain how they should do so. Many were born during periods of crisis and immediately faced trial by fire – CISA became a full agency less than two years before the 2020 U.S. election – but as they look beyond initialization and urgent response, they face the challenge of defining their long-term roles and responsibilities. The increasing sophistication of cyber threats and the rise of new technologies like AI and quantum computing indicates a need for continuous adaptation, complicating these discussions further. Some agencies might move towards a more centralized top-down authority model, where a single cyber agency oversees national cybersecurity efforts with clear mandates to facilitate rapid and unified response to complex threats. For example, the UK's National Cyber Security Centre (NCSC) provides a single point of authority for national cyber defense. Alternatively, countries might choose a distributed or sectoral approach to allow agencies to focus on areas of expertise, such as critical infrastructure, and add domain-specific defense plans. Germany follows this path with its Bundesamt für Sicherheit in der Informationstechnik (BSI), which works alongside sector-specific regulators to enforce cybersecurity policies tailored to different industries. Yet another approach is to double down on industry collaboration and facilitate private-public information sharing and collaboration. Most countries include elements of this approach, like Singapore's plan to enhance national cyber resilience in partnership with private companies through the Cyber Security Agency (CSA) and its Cybersecurity Labelling Scheme. Similarly, the United States prioritizes regulatory harmonization and private-sector engagement through ONCD-led initiatives. Australia's Protective Security Policy Framework also underscores the importance of industry collaboration, with the government actively promoting a zero-trust culture and ASD's "Essential 8" cybersecurity best practices to guide both public and private entities.

Figure 8: Country performances for the Codifying Roles & Responsibilities category.



Many countries struggle to incentivize organizations to report cyber incidents. Potential legal repercussions, costs, and reputation losses may make it more attractive to solve the incident internally rather than involving the state, to the detriment of the end users, society, and the organization itself. Some strategies offer clever ways to counter this by separating cybersecurity responsibilities among different agencies. For example, Singapore structures incident response teams under the Ministry of Digital Development and Information rather than traditional security or defense ministries, allowing security teams to focus on prevention and response without overlapping regulatory pressures. Australia has tackled the issue by ensuring that the Australian Signals Directorate has no legal enforcement power and that there is an "All Hazards Incident Response" protocol where critical infrastructure companies aren't held liable for consumer negligence when they are responding to an incident. Still, reporting obligations remain challenging across the board. Counter-ransomware responsibilities are often only mentioned in passing. However, the lack of counter-ransomware initiatives in the strategies is sometimes explained by the early publication date of many strategies in our analysis, considering ransomware has only recently risen to the level of a national security priority in most countries.

Table 8: Summary of Common Strengths in Codifying Roles and Responsibilities

Strength	Notable Examples
Assigning government roles and responsibilities	**Singapore -** CSA is the central agency for all cyber-related topics **USA** - Differentiated responsibilities between CISA, NSA, FBI **Australia** - ACSC, Australian Federal Police, and regulator responsibilities, including limited use obligations for de-conflicting incident response and law enforcement
Outlining the role of the Foreign Ministry in cyber	**Australia** - National Cyber Ambassador, Department of Foreign Affairs and Trade regional cyber crisis response team **USA -** State Department's Bureau of Cyberspace and Digital Policy; International Cyberspace and Digital Policy strategy

Defining how private-sector roles fit into national cybersecurity	**Japan** - Focus on cybersecurity as emergent from private sector collective action **Singapore** - Positioning the cybersecurity industry as a growth engine for the economy **South Korea** - Expanding the utilization of private sector capabilities for national cyber crisis response **UK** - Accreditation for private sector cyber incident response service providers
Crafting incident response procedures	**Australia -** ASD All-Hazards Incidence Response capability for critical infrastructure; Small Business Cyber Resilience Service **Japan** - Development of CERT/CSIRT incident response frameworks **Singapore** - Cyber Fusion Platform and National Cyber Security Command Center **USA** - Cyber Safety Review Board

Table 9: Summary of Common Weaknesses in Codifying Roles and Responsibilities

Weakness	Explanation
Aligning incentives throughout the private sector	Most strategies mention the need to better align incentives but fail to provide detailed and accountable plans to this end, especially beyond the development of certifications.
Improving quantitative methods for risk assessment (e.g., cost estimates or other enablers of the insurance market)	Few strategies provide a plan for improving quantitative estimates of cyber risk and costs. A notable exception is Singapore's Cyber Risk Management (CyRiM) project, which aims to develop tools and datasets to help facilitate insurance market development.
Building procedures to respond effectively to ransomware attacks	Details on counter-ransomware roles, responsibilities, and procedures lack depth and detail in several strategies (such as those of Germany, Japan, and Singapore), as they were written before ransomware was widely considered a serious national security concern. This contrasts newer strategies like those of the U.S. and Australia, which provide robust frameworks for tackling ransomware.

Communicating Clear Policy

Communicating Clear Policy received the second-highest proportion of leading scores across all categories, equalling the Building Partnerships category, and only had a few lagging scores. Most strategies communicate their objectives clearly and cover a broad range of issues, using accessible language and well-organized sections. They typically offer a contextual assessment of each country's unique threat landscape, shaping the rationale behind key focus areas. For example, South Korea offers a detailed assessment of the North Korean threat and emphasizes international cooperation, highlighting its shift toward offensive cybersecurity. However, South Korea, as well as several other strategies (especially the shorter ones), seems to focus more on signaling than laying out specific plans. They often fail to provide concrete action items and use non-specific language such as "The Government will..." rather than assigning tasks to specific offices, deadlines, and

budgets. We explore this problem in more detail in the Analysis section.

The U.S. strategy stands out with a clear layout of accountable agencies in its implementation plan, although some initiatives (such as data privacy objectives) lack detailed follow-through. Specific initiatives like the FBI's coordination with the Joint Ransomware Task Force provide a model for how multiple agencies can share responsibility for cybersecurity goals. Australia also provides specific timelines, clear department accountability, and a strong sense of direction. This contrasts with strategies such as Singapore's, which fails to commit to detailed timelines, with only vague mentions of plans to operationalize through Government Cybersecurity Operations, though we note that this may not have been included in Singapore's case due to the intended audience of the document.

Figure 9: Country performances for the Communicating Clear Policy category.

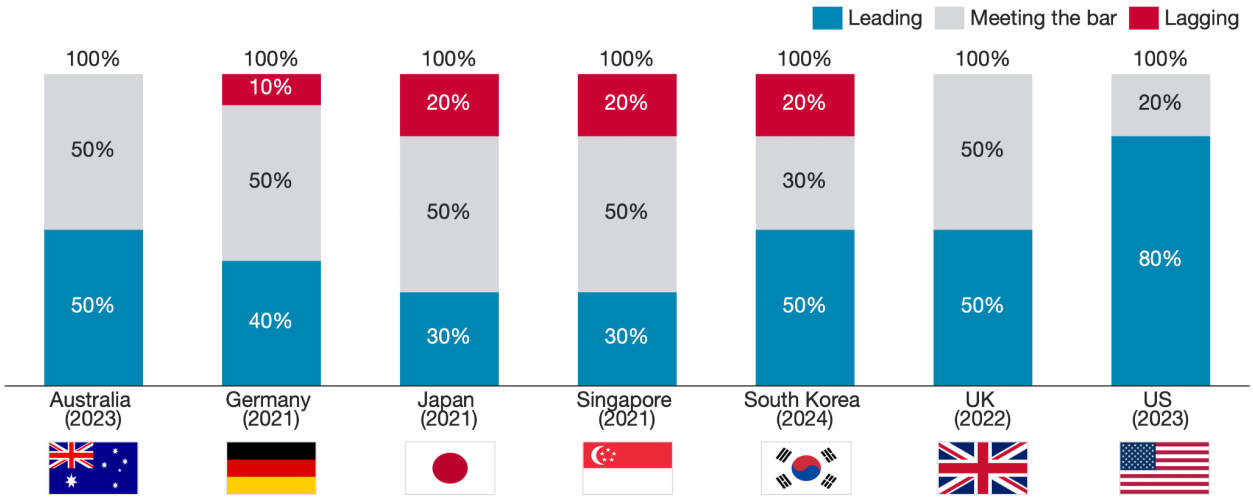


Table 10: Summary of Common Strengths in Communicating Clear Policy

Strength	Notable Examples
Structuring the strategy	**Australia** - "Shields" framework supported by uniquely numbered initiatives and actions. **Singapore** - "Pillars and enablers" framework.
Assessing the threat landscape	**South Korea** - North Korean threat assessment. **USA** - Russian and Chinese threat assessment.
Scoping the strategy	**USA** - The scope of the "Pillars" framework is, in many ways, the template for other nations.

Table 11: Summary of Common Weaknesses in Communicating Clear Policy

Weakness	Explanation
Including quantitative measures of performance	Most strategies fail to describe how they will quantify progress against their strategic aims (e.g., through reductions in the number and impact of attacks) other than measuring progress through the roll-out of their planned initiatives.
Detailing timelines	Many strategies lack timelines for rolling out specific initiatives; those that do present timelines are vague about how milestone achievement is defined and who is responsible for establishing that the milestone has been reached.
Committing to concrete actions	The strategies we studied made frequent use of ambiguous language such as "We will work with…" and "We will improve…" when describing their initiatives without committing to specific, measurable actions.

6.2 Country Scorecards

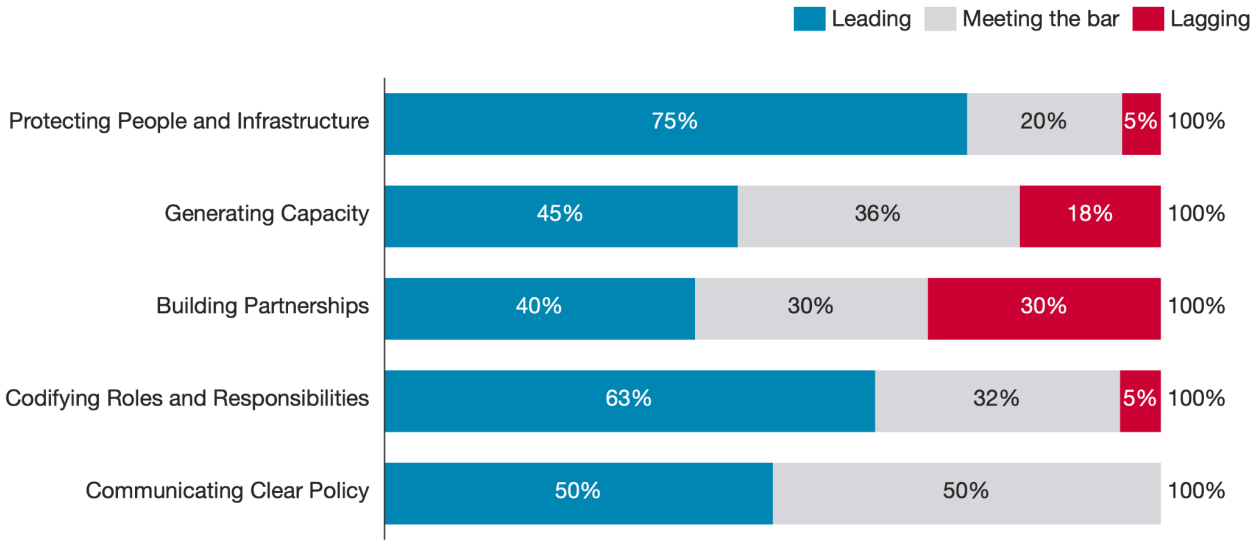
The following individual country scorecards analyze each national strategy in depth. The first passage of each individual scorecard discusses the country's performance in the evaluation. The second passage highlights elements of the national strategy that constitute international benchmarks and considers whether high-scoring policies would be effective in other contexts.

These assessments reveal clear leaders, especially the United States, Australia, the United Kingdom, and Singapore, all of which received leading marks on at least 50% of the 70 elements for which they were scored. Germany and Japan, with two of the oldest strategies considered in this assessment, received 23 and 25 leading scores, respectively, and more than 30 meeting the bar scores each, reflecting documents that are largely comprehensive and competent but, by late 2024, do not stand out much in terms of excellence or innovation. South Korea's new strategy received the lowest marks, leading in only 20 areas and lagging in nearly a quarter. While the South Korean strategy is undoubtedly lacking, its performance may be partly attributed to its purpose, which is rooted more in signaling a shift toward a confrontational cybersecurity posture than in conveying nuanced policy determinations. Interestingly, the score distribution was not uniform: the United Kingdom received only one lagging score, five fewer than the United States' next-lowest six lagging scores, despite coming a rather distant third in leading scores (36, tied with Singapore and 11 behind the United States).

Australia

Australia's 2023 strategy received the second-most leading scores and third-fewest lagging scores of the strategies assessed in this report. It consistently performed well across four categories, especially in Codifying Roles and Responsibilities and Protecting People and Infrastructure, where its critical infrastructure defense concept, underpinned by the landmark SOCI Act[12], sets a standard worthy of emulation. The strategy received positive scores in Generating Capacity for elements of the workforce development and cyber awareness programs it envisions, as well as in Communicating Clear Policy for its organization, clarity, and breadth. The Australian strategy received middling marks only in Building Partnerships, due to its lesser consideration of civil society or state- and local-level bodies. The Australian strategy's weaknesses are minor compared to those of most other strategy documents. Its only lagging scores involved plans for conducting counter-influence operations, developing the non-technical cyber and local law enforcement workforce, building partnerships with local and state government and civil society organizations, and conducting system hardening. The relatively small number of lagging scores indicates that the Australian strategy performs well across most aspects of national cyber strategy.

Figure 10: The Australian strategy's performance across the five evaluation categories.



The Australian strategy should be treated as a model for upper-middle tier powers seeking to develop incident response and reporting procedures, public-private partnerships, critical infrastructure resilience, and a strong global cybersecurity presence. Its vision for developing a whole-of-economy threat-sharing network and the accompanying threat-blocking scheme is particularly impressive for the granularity of detail it provides. The strategy document closely resembles in structure and content its U.S. and UK equivalents, which may be considered nearly as predecessors. Australia has also released a comprehensive and specific implementation plan that provides a clear roadmap for achieving the strategy's vision through 2025.

12 Australian Government Department of Home Affairs, Security of Critical Infrastructure (SOCI) Act 2018, https://www.cisc.gov.au/legislation-regulation-and-compliance/soci-act-2018.

Table 12: The Australian strategy's key strengths.

Strength	Details
Incident reporting	The "one-stop shop" portal Australia envisions is a model for streamlining the flow of information from victims to government cyber authorities (see strategic objective 6.1 on p. 25).
Threat sharing	Australia's strategy outlines detailed plans, including funding strategies, for establishing a "whole-of-economy" threat intelligence network built on public-private partnerships involving ASD and industry ISACs (see strategic objective 11 on pp. 35-6).
Technical workforce development	The strategy takes a thorough approach to cultivating a stronger and more diverse cyber workforce through upskilling, migration reforms, and initiatives for recruitment and professionalization (see strategic objective 17 on pp. 47-9).
Protecting SMEs and vulnerable populations	The strategy devotes more attention and resources to protecting small- and medium-sized enterprises (SMEs) and vulnerable populations than do most others (see strategic objective 1 on pp. 18-9, strategic objective 2.2 on p. 20, and strategic objective 18.1 on p. 50).
Critical infrastructure security	The strategy builds on the SOCI Act with strong measures for enhancing critical infrastructure security through initiatives like the "Systems of National Significance" scheme and for streamlining regulation (see strategic objective 13 on pp. 40-1).
Implementation plan	The accompanying "Action Plan" assigns tasks to specific agencies and provides a detailed roadmap for achieving most initiatives.
Organization	The strategy is exceptionally clear and well-structured, with lots of detail but a sensible and digestible format.

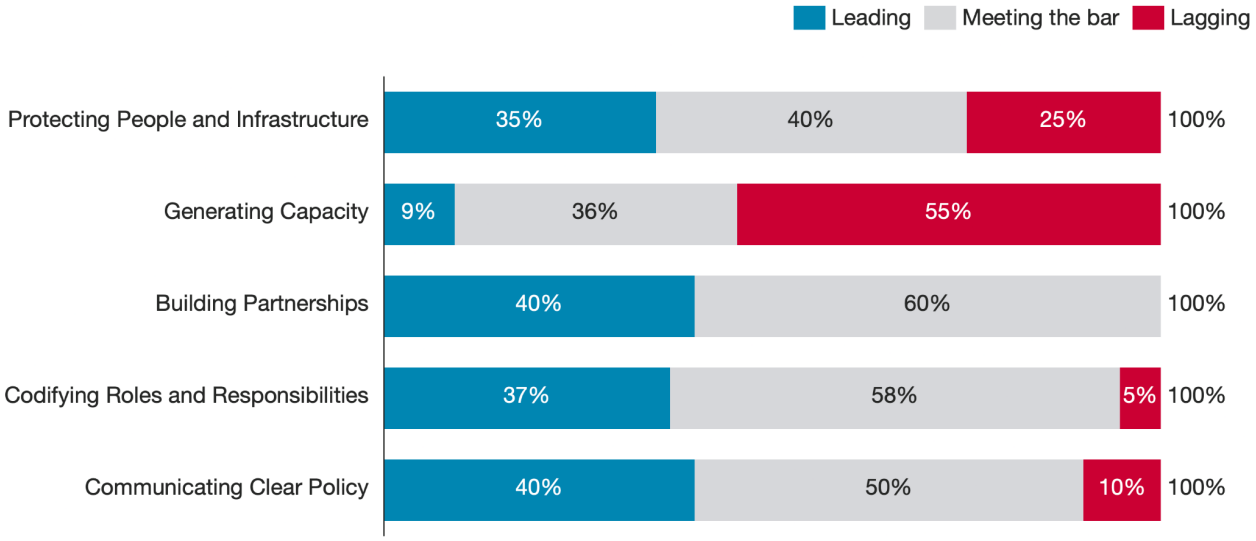
Table 13: The Australian strategy's key weaknesses.

Weakness	Details
Non-technical workforce development	Like most other strategies, the Australian cyber workforce development plan devotes less attention to important non-technical roles like cyber-qualified lawyers, law enforcement, and businesspeople.
Sub-national cyber capacity building	The strategy appears to underinvest in building sub-national cyber capacity, mentioning "local" stakeholders a number of times but rarely in substantive ways, often as beneficiaries of sectoral investment through vehicles like the National Reconstruction Fund (see strategic objective 18 on pp. 50-1).
Cybersecurity market development	The strategy mentions several investment and incentive schemes to cultivate a stronger domestic cybersecurity market, but many of the plans listed pre-date the strategy's publication and are either small-scale or only partly related to the cybersecurity industry (see strategic objective 18.1 on pp. 50-1).

Germany

Germany's 2021 strategy received the second-lowest number of leading scores and the second-most lagging scores of the strategies assessed in this report. It earned high marks in Building Partnerships for envisioning a defined prominent role in shaping EU and NATO cyber policy and an important supporting role in international settings. The German strategy also performed reasonably well in Codifying Roles and Responsibilities, despite the miscalibrated distribution of federal and state-level cyber authorities and the complex web of agencies whose remit touches German cybersecurity.[13] In Communicating Clear Policy, Germany received strong marks for the strategy's breadth and discussion of how it builds on the country's existing cybersecurity posture, but it performed worse with respect to accountability. Germany also received lower scores in Generating Capacity for having less detailed cybersecurity workforce and market development concepts than other countries. The strategy's Protecting People and Infrastructure evaluation was strikingly mixed, reflecting the contrast between its thoughtful plans for securing government IT systems and citizens' personal data and its weak discussion of critical infrastructure, which is centered around an outdated document from 2009. These scores indicate a divergence between Germany's 2021 strategy and day-to-day policymaking, which has prioritized implementing the robust KRITIS framework to comply with the EU's NIS2 cybersecurity requirements.[14]

Figure 11: The German strategy's performance across the five evaluation categories.



The German strategy provides a useful template in some areas – particularly cybersecurity leadership in regional institutions, safeguarding personal data, and leveraging research institutions and civil society – but several factors unique to the German context make it relatively unsuitable for international benchmarking. The strategy acknowledges the complexity of interagency and federal-state cooperation under Germany's constitutional structure, which circumscribes the Federal Office for Information Security (BSI) and other national agencies' cyber jurisdiction and often subordinates them to less-capable regional actors. The

13 For more details on the many domestic and international bodies that play a role in German cybersecurity, see Sven Herpig and Frederic Dutke, "Germany's Cybersecurity Architecture", Stiftung Neue Verantwortung, October 2023, https://www.interface-eu.org/storage/files_for_publications/2023/231019_cyber_architecture/11thed_cybersecurityarchitecture.pdf.

14 For more details on the KRITIS framework and NIS2 implementation plan, see OpenKRITIS, NIS2 in Germany, 2024, https://www.openkritis.de/eu/eu-nis-2-germany.html.

German strategy proposes an array of concrete steps for strengthening existing coordination mechanisms, but they mostly resemble patches rather than long-term solutions, assuming they are implemented at all. Other factors have reduced the strategy's relevance since publication, including deteriorating relations with Russia and the fact that it was adopted just before a national election that elevated a new party into power.

Table 14: The German strategy's key strengths.

Strength	Details
Regional cybersecurity leadership	The strategy outlines a vision for shaping European cyber policy and being a major contributor to NATO policy and global behavioral standards (see 8.1.4 and Action Area 4, especially 8.4.1, 8.4.2, 8.4.5, and 8.4.7).
Data protection and digital identity	The strategy lays out detailed plans for raising standards to safeguard citizens' data even beyond GDPR, especially for electronic identities and financial information (see 8.1.5, 8.1.6, and 8.2.5).
Certification schemes	The strategy leans into Germany's strength in cybersecurity certification for technologies like 5G networks, cloud service providers, and Internet of Things (IoT) devices, committing to promoting them in the EU and globally (see 8.1.4, 8.2.7, 8.2.10, and 8.2.12)
Protecting against emerging threats	The strategy anticipates threats from emerging technologies like AI and quantum in-depth, advocating for verifiable security and risk-based frameworks, which is noteworthy because the strategy came out in 2021 (see 8.1.10, 8.2.9).
Leveraging research institutions and civil society	Building on the April 2021 National Pact on Cyber Security, the strategy outlines plans for providing targeted funding to IT security research institutions and accelerating the commercial availability of cybersecurity innovations (see 8.2.2 and 8.2.7).[15]
Delegation of cybersecurity responsibilities among federal agencies	The strategy clearly distributes responsibility among federal-level actors with cyber functions, starting with the BSI and including the domestic intelligence agency BfV, the federal police BKA, the Cyber-AZ coordinating council, and other agencies (see pp. 19-21).
Safeguarding government systems and public services	The strategy offers plans for enhancing the security of government networks, adding federal administration information security officers, and safely digitalizing election processes, among other initiatives (see Action Area 3, especially 8.3.1, 8.3.3, 8.3.4, 8.3.5, and 8.3.6).

15 For more information on the National Pact, see this Interior Ministry document (in German): Bundesministerium des Innern und für Heimat, Nationaler Pakt Cybersicherheit: Gesamtgesellschaftliche Erklärung vorgestellt, 23 Apr 2021, https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2021/04/nationaler-pakt-cybersicherheit.html.

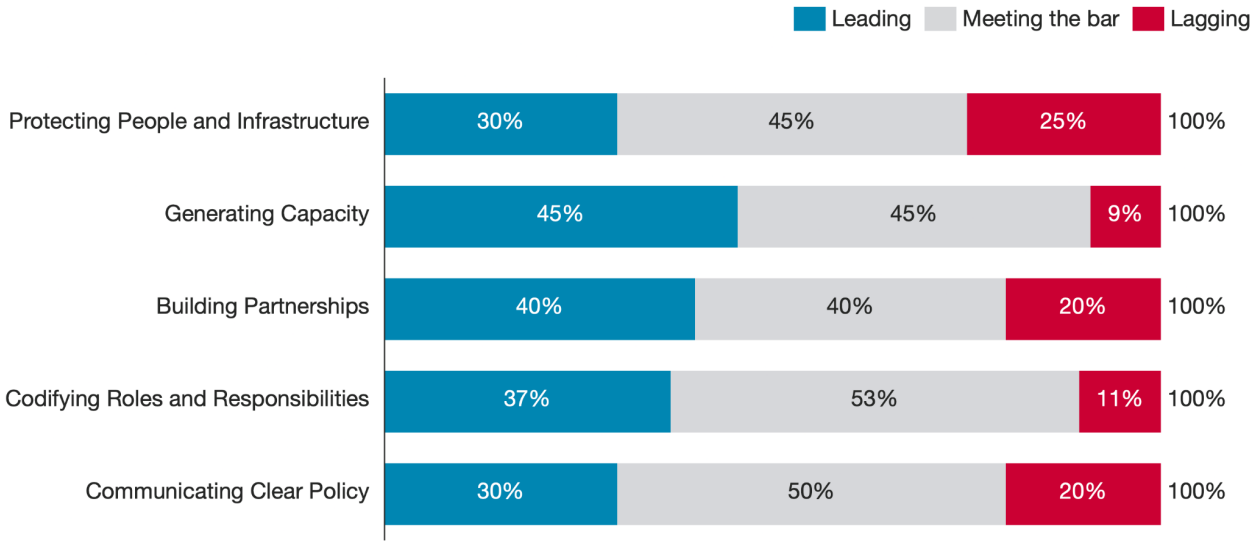
Table 15: The German strategy's key weaknesses.

Weakness	Details
Critical infrastructure protection	The strategy's main critical infrastructure provisions rely on the 2009 National Strategy for Critical Infrastructure Protection, which is outdated and often vague (see 8.2.11).
Addressing miscalibrated federal-state powers in cyberspace	To its credit, the strategy acknowledges this problem and proposes several measures to remediate it, but they mostly address symptoms (for example, dysfunctional coordination mechanisms) rather than the root problem of under-empowering otherwise capable federal agencies. The calls for legislative change are not sufficiently specific (see Action Area 3, especially 8.3.1, 8.3.3, 8.3.5, 8.3.7, 8.3.8, and 8.3.12).
Forward defense	The strategy does not mention forward defense or offensive cyber capabilities, except for a brief reference in the definitions section (see p. 125). Of course, this may have been a deliberate choice rather than an oversight.
Workforce development	The strategy acknowledges that "top-class IT security research and well-trained IT security professionals are key to ensuring cyber security provision in the long term" (p. 49) but offers few substantive measures for developing the cybersecurity workforce or industry.
Accountability	The strategy does not systematically assign the initiatives it lays out to government actors or establish deadlines by which they are to be completed.
Assessment	Though each initiative concludes with a "How will we measure this?" section, most assessment criteria are vague and tied to process rather than outcomes.

Japan

Japan's 2021 strategy received a solid assessment, covering lots of ground but excelling in only a few areas. It tied for the second-fewest leading scores and received the third-most lagging scores. The Japanese strategy received polarized marks in Protecting People and Infrastructure, faring poorly on critical infrastructure defense but quite well for its commendable focus on safeguarding individual users and their data, vulnerable groups, and SMEs under the banner of "Cybersecurity for All." It received generally positive scores in Building Partnerships, where it devotes welcome attention to international and local-level engagement, and in Codifying Roles and Responsibilities, where its consideration of technical standards surpassed its establishment of policy and procedural responsibilities. The strategy's best performance came in Generating Capacity in recognition of the strategy's emphasis on education, training, and awareness as part of a broader campaign to accelerate a secure digital transformation. Even in that category, though, Japan received middling grades because its plans for workforce and market development tend to lack detail compared with those of peer countries. The strategy received lower marks in Communicating Clear Policy for its relatively poor organization and vague prescriptions.

Figure 12: The Japanese strategy's performance across the five evaluation categories.



Japan's strategy exemplifies how quickly the field of cybersecurity policy has changed in a short period of time. The strategy is unique for considering cybersecurity through the lens of the economy and ongoing digital transformation more so than as a national security issue. Just three years after the release of the strategy, Japan announced its intention to pivot sharply toward a national security orientation, recognizing harsh geopolitical realities like looming cyber threats from Russia, China, and North Korea and announcing new core policies like "Active Cyber Defense" that do not feature in the 2021 concept. In its next strategy, Japanese policymakers will likely also need to reconsider their approach to dealing with industry, as the current cyber governance regime is significantly weaker than in most other countries.

Table 16: The Japanese strategy's key strengths.

Strength	Details
"Cybersecurity for All" theme	Japan's strategy takes a unique whole-of-society approach to cybersecurity, placing special emphasis on protecting vulnerable population groups and SMEs.
Data management	The strategy devotes extensive attention to data management, obligating the government to clarify the definition of the term, establish frameworks for managing risks in specific use cases, and evaluate differences between Japanese and external data management standards with an eye toward harmonizing the frameworks (see objectives 4.1.3[2] and 4.2.1[1i]).
Supply chain security	The Japanese strategy includes a detailed discussion of supply chain threats and several semi-concrete initiatives for securing cyber supply chains, such as a scheme for registering and recommending IT services for SMEs (see sub-sections 3.2 and 3.3 and objectives 4.1.3 and 4.2.1[1i]).
Preparing for emerging threats	The strategy flags and discusses at length a number of emerging technology threats, especially quantum computing. More broadly, it is impressively devoted to advancing R&D with respect to cyber-relevant technologies, though as with the rest of the document, it would benefit from some additional specificity (see 4.4.1[2], especially passage iv).
Promoting digital literacy and cybersecurity awareness	The strategy outlines several initiatives designed to improve digital and security literacy across the board, "with no one left behind." In keeping with the document's relative emphasis on society and the economy, rather than national security, its proposals cover not just cyber hygiene but everyday uses of ICT in order to advance digitalization and grow the economy (see objectives 4.1.4 and 4.2, especially 4.2.1).

Table 17: The Japanese strategy's key weaknesses.

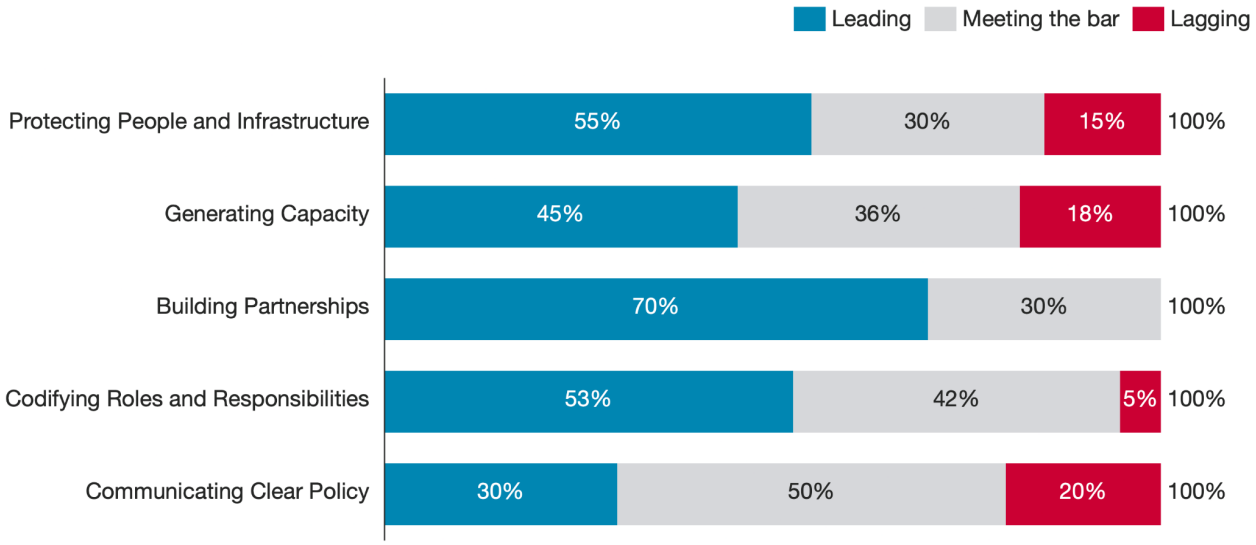
Weakness	Details
Workforce development	The workforce development plan focuses on upskilling, promoting digital literacy, and supporting existing workers rather than cultivating a much-needed larger workforce.
Specificity	The strategy is lengthy and detailed but not especially specific, especially in issuing prescriptions. In general, the document is more successful at identifying threats and desired outcomes than the specific steps required to achieve them. The document uses the phrase "etc." 77 times, according to keyword search analysis.
Accountability	The document includes a brief implementation plan at the end and an appendix that assigns policy responsibility to various agencies. The appendix is an important first step toward accountability, but it fails to assign responsibility at the level of specific policy tasks and outcomes. For example, primary responsibility for "Addressing cyber crimes" falls to five agencies, with two more secondarily responsible (see p. 62).
Organization	The strategy is less well-organized than peer documents, which tend to center around more clearly delineated thematic pillars.

Singapore

Singapore's 2021 strategy received a favorable evaluation in most areas, tying for the third-most leading scores. That performance is a noteworthy achievement given that the strategy was published more than three years ago and that Singapore's GDP is significantly lower than those of the other countries included in this report. The strategy performed particularly well in Codifying Roles and Responsibilities, Protecting People and Systems, and Building Partnerships. It presents advanced concepts for defending its critical infrastructure and data environment, such as establishing Singapore as a trusted Testing, Inspection, and Certification (TIC) hub and developing a coordinated approach to national cybersecurity with Critical Information Infrastructures (CIIs) at its core, remaining impressive even in comparison with richer and larger countries. The strategy largely neglects emerging threats like ransomware, AI-enhanced capabilities, and quantum, an understandable weakness considering the strategy's age. Singapore also pioneers cyber cost and risk estimations via the Cyber Risk Management Project (CYRiM). The program provides a structured approach to quantifying cyber risks and associated costs, enabling organizations to make more informed decisions about their cybersecurity investments. By offering a common framework for assessing cyber risk, CYRiM helps to standardize risk evaluation across different sectors, facilitating better understanding and communication of cyber threats. It allows companies to get a more accurate estimate of potential financial losses from cyber incidents to facilitate and motivate cybersecurity investments.

Singapore received less impressive scores for Generating Capacity, though still mostly favorable. Its plan to develop a "vibrant cybersecurity ecosystem" lacks the same level of detail as its plans for building resilience and user safety. The strategy is generally clear and well structured, but it lags behind other countries regarding accountability and performance review.

Figure 13: The Singaporean strategy's performance across the five evaluation categories.



The Singaporean strategy should serve as a benchmark for many cyber policy areas. Singapore punches above its weight in international engagement; it plays a leading role in the Association of Southeast Asian Nations (ASEAN) and exerts a strong influence over global cyber policymaking. While Singapore's strategy document does not mention ransomware, the government's extensive involvement in the Counter Ransomware Initiative and other major counter-cybercrime efforts flows directly from the foundation laid in the strategy, which is itself a product of a longer national trend toward global policy engagement. Singapore's visions for incident

response, critical infrastructure defense, and protection of small and vulnerable entities are all worth emulating. However, a number of factors could make it difficult for other countries to transpose Singapore's policy concepts successfully. Among others, Singapore benefits from a less hostile geopolitical environment than perhaps any other major country, a small geographic area to defend and coordinate across, a highly advanced economy, and a national culture that enables strong law enforcement and technological surveillance.

Table 18: The Singaporean strategy's key strengths.

Strength	Details
Hardening government systems	The strategy contains a clear, advanced plan for modernizing government network security according to zero-trust principles and assigns duties to organizations like the Smart National and Digital Government Group (SNDGG) and Government Cybersecurity Operations Centre (GCSOC) (see p. 18).
Regional cyber leadership	Singapore's strategy outlines plans for building on its exemplary regional leadership, especially through ASEAN. The approach encompasses not only capacity building but areas like norm promotion (see Chapter 3, especially pp. 35 and 39-40).
International cyber leadership	The strategy envisions a major role for Singapore in international cyber policymaking. The passages concerning mutual recognition of security labeling schemes and fighting cybercrime are particularly notable (see pp. 37 and 39). However, certain aspects, such as the call for establishing stronger behavioral norms in cyberspace, would benefit from a more specific discussion of goals.
Protecting vulnerable groups and SMEs	Singapore devotes sustained attention to protecting vulnerable groups such as youth and seniors, as well as to protecting SMEs through novel programs like government-provided data protection as a service (DPAAS) (see p. 25).
Separating incident response and enforcement	The strategy emphasizes the independence of the Cyber Security Agency (CSA), which performs capacity building, incident response, and other key functions separately from law enforcement agencies (see p. 17). This division incentivizes victims to seek help and report cyber incidents.

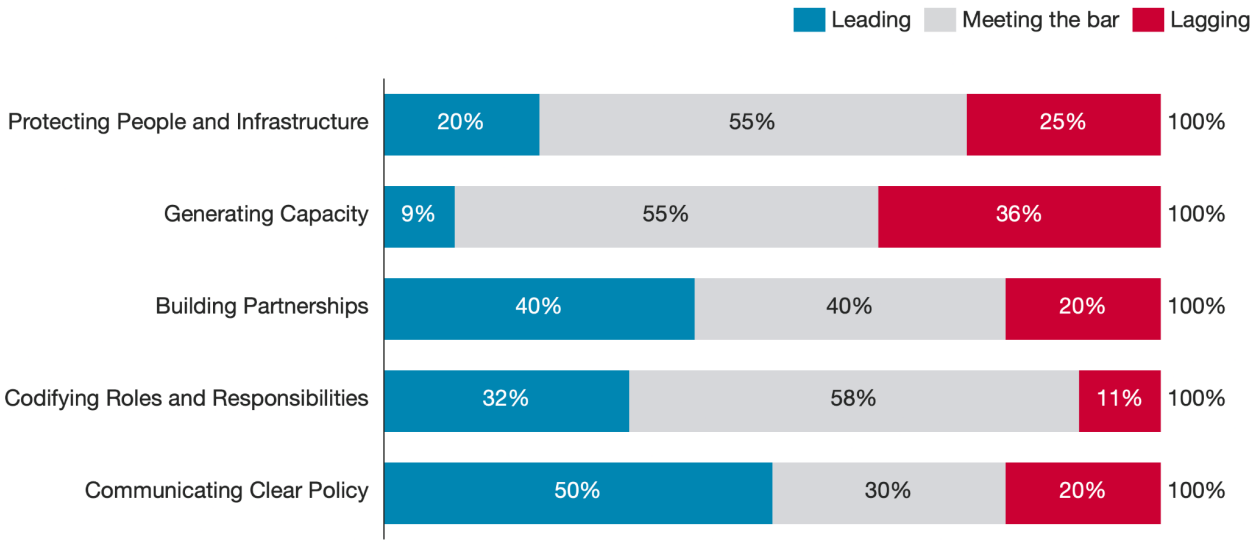
Table 19: The Singaporean strategy's key weaknesses.

Weakness	Details
Market development	The strategy's vision for cultivating domestic cybersecurity firms and entrepreneurs is much less concrete than its aspects designed to promote talent and research (see Chapter 4, "Develop a Vibrant Cybersecurity Ecosystem").
Preventive intelligence gathering and threat sharing	The strategy offers little detail on plans for gathering and sharing intelligence, especially for cooperating with multinational industry partners with valuable capabilities.
Emerging threats	The strategy pays little attention to ransomware, AI, quantum, or other emerging threat areas, an understandable shortcoming considering it was published in 2021.
Accountability	The strategy lacks specifics on accountable parties and deadlines, often declaring simply that "The government will…"

South Korea

The 2024 strategy represents a marked change from the cybersecurity concept South Korea adopted in 2019. The new strategy reflects a transformed political context in which a president with hawkish views on North Korea reversed the course set by his dovish predecessor. The result is a document whose organizing principle is to aggressively counter North Korean cyber threats. Unlike many other national strategies, which offer a lengthy overview of the country's cyber policy toolkit and a long list of to-dos, South Korea's is a short statement of key priorities that deliberately eschews comprehensiveness and specificity, though the Basic Plan fills in some gaps with respect to implementation. Despite being the most recently published document analyzed in this report, South Korea's 2024 strategy received the lowest evaluation scores. The strategy performed best at deepening partnerships with global allies and on issues related to cyberspace norms. It generally calls for harnessing industry for certain tasks, like developing and securing critical technologies, but does not mention civil society or local governments, key players in any national cybersecurity plan. South Korea has long been a global leader in securing data and ICT infrastructure, so it is perhaps understandable that the pillar devoted to "Enhancing Cyber Resilience of Critical Infrastructure" offers little depth or new vision. The strategy does not pay much attention to Generating Capacity beyond disruption and deterrence, which are treated with inconsistent specificity. Its limited focus on technical workforce development is a notable contrast to most other national approaches, which tend to outline more substantive policy measures for cultivating talent. The South Korean strategy received solid marks in Codifying Roles and Responsibilities for relatively clearly delegating tasks to responsible agencies, especially the National Intelligence Service. It says little about strengthening procedural responsibilities and industry regulations, except with respect to incident response. The strategy document is written clearly and situates itself within the existing South Korean cybersecurity policy environment, but it lags behind peers regarding accountability and progress assessment.

Figure 14: The South Korean strategy's performance across the five evaluation categories.



The South Korean strategy is noteworthy for its unique design but is ultimately less worthy of global emulation than most other strategies considered in this report. Its main limitation is the consistent lack of detail, which weakens its treatment of standard cybersecurity policies and holds back proposals that might otherwise have been impactful. For example, the aspects that involve cultivating a stronger military-to-industry

cybersecurity talent pipeline, establishing governance and security frameworks for digital government platforms, and pursuing "strategic industrialization" of critical technologies would likely have received leading scores if they had been fleshed out further. The Basic Plan provides some further detail but does not measure up to the U.S. implementation plan. South Korea's is also a blatantly political document; one section is entitled "Achievements of the Yoon Suk Yeol Administration in the Past Two Years and Future Direction." In terms of value to international cyber strategists, the South Korean concept is likely most valuable to countries with similar security situations, like Israel and Ukraine, where external signaling to adversaries and allies may take precedence over conveying truly substantive policy goals.

Table 20: The South Korean strategy's key strengths.

Strength	Details
Clarity of vision	The strategy clearly establishes North Korean cyber threats as its primary concern and offensive capabilities as the primary means of countering them (see Pillar 1, especially sections A and D).
International partnerships	The strategy outlines specific goals for important international relationships, such as working with Japan and the United States to counter North Korean cybercrime and sharing threat information with NATO and Indo-Pacific regional partners (see section 2.A, especially tasks 2, 3, 4, 5, 6, and 8, as well as section 2.C).
International cyber norms	The discussion of international cyber norms and confidence-building measures is among the strategy's more detailed passages, with some clear goals related to the applicability of international law in cyberspace (see section 2.B, especially tasks 2 and 3).
Leveraging industry capacity	The strategy calls for partnering with industry in several areas, including international capacity building, conducting technical research, industrializing core strategic technologies, responding to cyber incidents, and, to some extent, cultivating a stronger workforce (see section 2.C, especially tasks 1 and 2; section 4.A and task 4.B.2; section 5.C; and section 5.D). The Basic Plan provides a more detailed roadmap for leveraging the private sector for incident response (see pp. 39-41).
Developing threat response capabilities	Besides explicitly focusing on North Korean threats, the strategy's greatest shift is toward emphasizing "offensive cyber defense and response." It calls for enhancing capabilities in several areas – among them preventive intelligence gathering, attribution, and threat sharing – though there is less mention of actual offensive or disruptive capabilities than might be expected (see pillar 1, especially sections A, B, and D).
Promoting resilience	Pillar 3 on critical infrastructure is not especially detailed or groundbreaking, but its focus on building resilience across essential ICT systems, government platforms, and supply chains is to be commended (see Pillar 3).

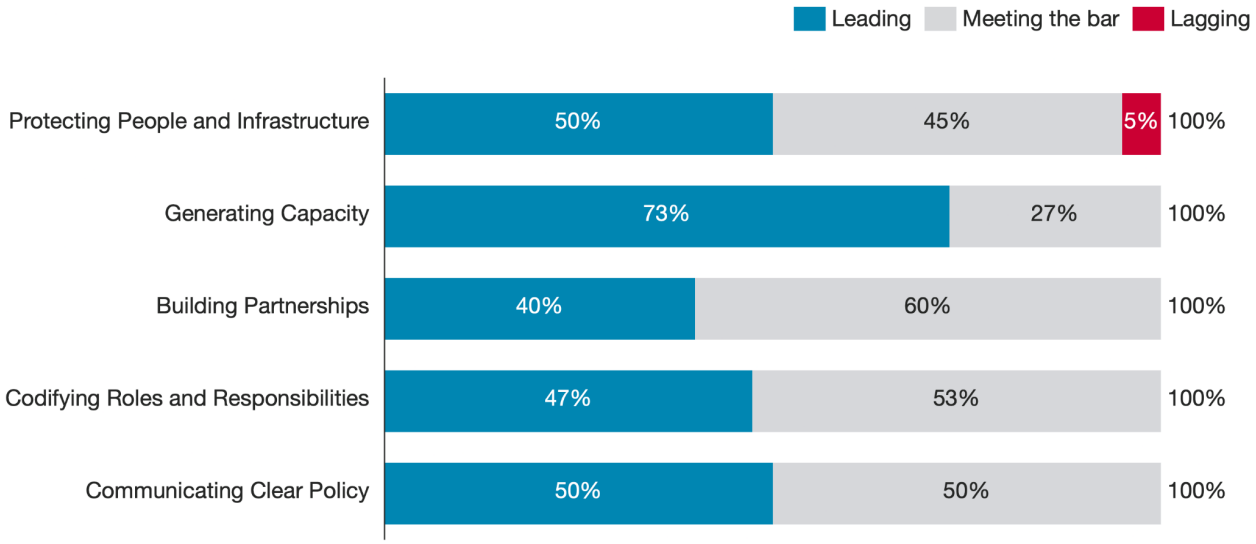
Table 21: The South Korean strategy's key weaknesses.

Weakness	Details
Comprehensiveness	The strategy's scope is much more limited than in peer documents. Allowing that the drafters seem to have focused purposely on a few key themes, it is still a major shortcoming to leave unaddressed core elements of national cybersecurity, such as workforce development, data protection, industry cybersecurity incentives, and sub-national cyber coordination, even if South Korea already performs well in some of those areas.
Depth	The "Strategic Tasks" section consists of one-sentence passages that articulate key objectives but cannot capture them in detail and are often quite vague. The Basic Plan offers significantly more depth in several areas, particularly defending critical infrastructure and control systems, but remains insufficiently specific. For example, it calls for developing a "Korean-style zero-trust technology model" without providing any further information as to what that might entail or require (see p. 32).
Workforce Development	In general, the strategy charts a course for enhancing South Korea's cybersecurity capacity through technical innovation and procurement, especially harnessing AI, rather than workforce development. To be sure, the Basic Plan devotes around a page to "Developing and Retaining Skilled Personnel" and makes a few short references to developing human capital (see pp. 40-41, 22, and 27). These passages, however, lag behind their counterparts in peer strategies in terms of detail and expression of concrete goals. In addition, the South Korean strategy does not convey any intent, let alone plans, to broaden women's participation in the cybersecurity workforce, a dually important topic for promoting gender equality and building capacity.
Protecting SMEs and vulnerable populations	The strategy does not mention SMEs or vulnerable groups such as the elderly. The Basic Plan makes two brief references to SMEs: one lists an earlier plan to offer reduced fees for certifying information technology products, while the other calls for providing SMEs with incident response and recovery support (see pp. 35 and 36).
Setting procedural responsibilities	The strategy does not mention key procedural areas like incident reporting requirements, identifying lessons learned, or regulatory harmonization, which are core focuses of other national cybersecurity strategies. The South Korean strategy extensively discusses incident response (see sections 1.A, 1.D, 3.C, and 5.A).
Accountability	The strategy does not systematically assign the initiatives it lays out to government actors or establish deadlines by which they are to be completed.
Assessment	The strategy mentions assessment only once, in its final sentence, and offers no detail other than to assign the task to the Office of National Security (see p. 43).

United Kingdom

The United Kingdom's 2022 strategy performed well across the evaluation, receiving the fewest outright lagging scores of any country. The strategy received its strongest marks for Generating Capacity, particularly with respect to developing cyber skills and digital literacy. It contains impressive plans for Building Partnerships with capable actors outside government, exemplified by schemes like the Industry 100 (i100) and National Cyber Advisory Board, though the "Global Leadership" section is the shortest and perhaps least concrete of the strategy's five pillars. The distribution of cybersecurity roles and responsibilities is clear, and the strategy highlights lingering gaps in law enforcement authorities under the Computer Misuse Act. It received mostly favorable scores with respect to Protecting People and Infrastructure, led by discussions on strengthening the UK cyber ecosystem and defending the most critical infrastructure sectors. The strategy stands out for the accessibility, comprehensiveness, and clarity with which it describes the broader operating environment, especially the current threat landscape and the role of cyber within the government's broader agenda. While the UK strategy provides for self-assessment, it lags behind the United States and Australia with respect to delegating specific tasks and setting clear deadlines.

Figure 15: The United Kingdom strategy's performance across the five evaluation categories.



The UK strategy has a number of elements that should be considered global benchmarks. Its vision for engaging industry and civil society partners was among the strongest of the seven countries assessed in this report. The strategy outlines plans to develop two key initiatives: Cyber Essentials and Active Cyber Defence (ACD). The Cyber Essentials scheme is a great example of strategizing organizational security and has been adopted worldwide, including in advanced cybersecurity states like Singapore. The UK's approach to cybersecurity workforce development is also impressive, including the Cyber Security Skills and Cyber First programs. The "Cyber Reserves" initiative envisions leveraging the technical workforce to support national defense capabilities in times of need. In some ways, though, the UK strategy is less notable for its content than for what is not present. Substantial gaps remain in the UK cyber regulatory regime, especially outside the designated critical sectors, and government cyber actors lack some of the authority to defend forward and disrupt threats that counterparts in other countries enjoy. A growing contingent in the United Kingdom has also voiced concerns that the design of UK cybersecurity bodies is outdated and needs revitalization. While the strategy nods to the urgent need for a review of the Computer Misuse Act 1990 – which the government has since completed,

revealing a number of necessary revisions – it would have been valuable to conceptualize and set in motion those changes in the strategy document.[16]

Table 22: The United Kingdom strategy's key strengths.

Strength	Details
Protecting SMEs	The United Kingdom's Cyber Essentials scheme presents a simple and effective framework for protecting businesses and inspired the Singaporean scheme of the same name. The UK strategy additionally mentions support available to businesses through the cyber PROTECT network, the Economic Crime Victims Care unit, and regional Cyber Resilience Centers (see Pillar 2, Objective 2, especially items 103 and 117).
Engaging the private sector	The NCSC's Industry 100 (i100) scheme and GCHQ/MoD's Joint Cyber Reserve Force both exist to break down barriers to public-private cooperation in national cybersecurity. The UK's National Cyber Advisory Board also provides a mouthpiece for private sector cybersecurity experts to articulate their perspectives to government, and the UK Cyber Cluster Collaboration (UKC3) networks the UK cyber industry with government and NGOs.
Data privacy	Building on GDPR, the UK strategy calls for a stronger data protection framework, in line with the previous National Data Strategy. The call for legislative action to enhance protections for data has paved the way for the 2024 designation of data centers as Critical National Infrastructure (see Pillar Two, Objective Two, especially items 111, 112, and 115).[17]
Domestic government partnerships	The UK strategy focuses on enabling coordination and collaboration between domestic government entities well beyond the ambition of the other cybersecurity strategies studied. Highlights include the establishment of a Government Cyber Coordination Center to enable all levels of the UK government to "defend as one," as well as the development of Regional Cybercrime Units for each of the UK's nine law enforcement regions and coordination of national responses to cybercrime via the National Cybercrime Unit at the National Crime Agency (see, for example, Pillar 1, Objective 1, item 68 and Pillar 2, Objective 1, item 99).

16 United Kingdom Home Office, Computer Misuse Act 1990: Call for Consultation, May 11, 2021, https://www.gov.uk/government/consultations/computer-misuse-act-1990-call-for-information; United Kingdom Home Office, Review of the Computer Misuse Act 1990, February 7, 2023, https://www.gov.uk/government/consultations/review-of-the-computer-misuse-act-1990.

17 See UK Department for Science, Innovation and Technology, "Data Centres to Be Given Massive Boost and Protections from Cyber Criminals and IT Blackouts," September 12, 2024 https://www.gov.uk/government/news/data-centres-to-be-given-massive-boost-and-protections-from-cyber-criminals-and-it-blackouts.

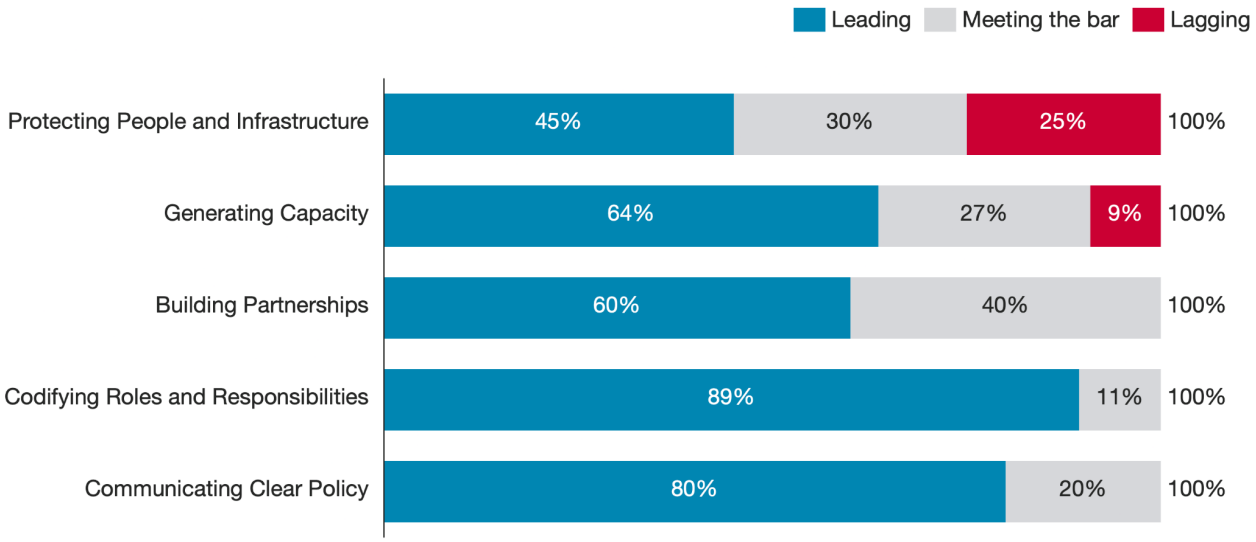
Table 23: The United Kingdom strategy's key weaknesses.

Weakness	Details
Active defense, especially disruption operations	While the UK strategy discusses preventive intelligence gathering and proposes some changes to outdated legislation to support disrupting cybercrime, it does not adequately address threat actors or develop clear concepts for combating the full spectrum of cybercrime, especially disinformation campaigns and ransomware.
Protecting critical infrastructure, especially especially outside designated essential sectors	Defending critical infrastructure is an obvious priority, but the strategy does not fully address the emerging challenges it warns of. Doubling down on the sector-based approach to designating entities for protection — to be sure, a common approach worldwide — does not respond to the stated concern that "critical infrastructures will become much more distributed and diffuse and this fundamentally changes how regulation will impact the security of the critical functions and services we rely on" (see "Drivers of Change," item 34). Moreover, the sectoral approach results in the exclusion of certain important entities, such as manufacturers of key products outside the designated fields.
Incentivizing investments in cybersecurity	The strategy abstractly notes the need for stronger market incentives to invest in cybersecurity but does not offer a detailed vision for improvement, let alone a roadmap for getting there. During interviews, experts consistently felt that the current incentive structure has failed to get board-level leadership of critical infrastructure entities to devote sufficient attention to cybersecurity.

United States

The United States' 2023 strategy received the most leading scores and second fewest lagging scores of the countries assessed. The strategy tends to assign cybersecurity roles and responsibilities clearly, though the overlapping functions of CISA, ONCD, the National Security Council, and certain other bodies raise questions about whether a more streamlined model might have been possible. The U.S. strategy outlines a thoughtful vision for harnessing its private sector and research capabilities toward advancing cybersecurity. It also received high scores in Building Partnerships and Generating Capacity, though plans for building sub-national authorities' cyber capacity are notably lacking. The document is sensibly structured to Communicate Clear Policy, thorough, and paired with a detailed implementation plan that assigns deadline-driven accountability to specific government actors. The U.S. strategy received mixed scores in Protecting People and Infrastructure, where insufficient consideration of SMEs and vulnerable population groups undermined one of the strongest national concepts for enhancing critical infrastructure security and conducting active defense. The strategy acknowledges the need for a national data management framework but does not propose concrete steps for developing one, a lingering weakness compared with most other countries.

Figure 16: The United States strategy's performance across the five evaluation categories.



Many aspects of the U.S. strategy are already seen as global benchmarks. The strategy features useful concepts for harmonizing disparate industry regulations, upgrading government systems, securing digital supply chains, and investing in cybersecurity research and innovation. In interviews, international practitioners lauded the U.S. approach to building resilience and accelerating recovery, citing initiatives like the Cyber Safety Review Board (CSRB) as particularly well-crafted. In some ways, though, one of the U.S. strategy's key strengths – that it is tailored to the country's unique capabilities – makes it less transferable to foreign contexts than other strategy documents. The size of the U.S. market affords Washington a special ability to influence private sector behavior, namely, with respect to shifting accountability and promoting secure-by-design principles. The United States also wields singular influence on the international stage, putting it in a particularly strong position to build coalitions, distribute global resources, and shape cyberspace norms. It would make less sense for governments with more limited global influence or private sector sway to transpose these aspects of the U.S. strategy without alteration.

Table 24: The United States strategy's key strengths.

Strength	Details
Shaping cybersecurity incentives	The goal of transferring accountability to the most capable actors is an important shift in narrative and policy. An array of specific initiatives support this vision across software, IoT, insurance, and other fields (see Pillar Three, especially Implementation Initiatives 3.2.2, 3.3.1, 3.3.2, 3.3.3, 3.5.1, 3.5.2, and 3.6.1).
Regulatory harmonization	The strategy calls for "modern and nimble regulatory frameworks… tailored for each sector's risk profile, harmonized to reduce duplication, complementary to public-private collaboration, and cognizant of the cost of implementation," and the implementation plan lays out a roadmap for advancement (see Strategic Objective 1.1 and Implementation Initiatives 1.1.1, 1.1.3, and 5.5.1).
International engagement	The strategy discusses plans for marshaling global coalitions, setting technical standards and behavioral norms in cyberspace, strengthening partnerships, and helping raise global cybersecurity capacity (see Pillar Five, Strategic Objective 4.1, and Implementation Initiatives 5.1.3, 5.2.2, 5.3.1, 5.5.1, 5.5.3, and 5.5.4).
Active defense	The strategy prioritizes enhancing preventive and disruptive capabilities, streamlining interagency processes, and organizing international policy forums to combat malign cyber activity, such as the Counter-Ransomware Initiative (see Strategic Objectives 2.1, 2.2, 2.4, 2.5, 5.1, and 5.2).
Critical infrastructure security and resilience	Improving critical infrastructure security is one of the strategy's primary focuses, to be accomplished through sector-specific regulation, public-private partnerships, and federal action building on Executive Order 14028 (see Pillar One and corresponding Implementation Initiatives, especially 1.1.2, 1.2.2, 1.2.4, 1.2.5, 1.3, 1.4, and 1.5).[18]
Incident response and recovery	The passages concerning federal incident response processes reflect a strong understanding of cyberattack victims' perspectives and needs. It outlines specific goals for leveraging the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) and the CSRB, as well as for holding wide-reaching preparatory exercises (see Strategic Objective 1.4 and corresponding Implementation Initiatives).
Accountability	The implementation plan names a single responsible agency for every initiative, as well as contributing entities and deadlines.

18 CISA, Executive Order on Improving the Nation's Cybersecurity, 2021, https://www.cisa.gov/topics/cybersecurity-best-practices/executive-order-improving-nations-cybersecurity.

Table 25: The United States strategy's key weaknesses.

Weakness	Details
Protecting SMEs and vulnerable populations	The strategy mentions society's most vulnerable members a few times (see the introduction to Pillar Three) but does not contain tailored measures for protecting them. While those groups would benefit from a more secure digital ecosystem overall, other national strategies more substantively address small businesses and population groups like the elderly.
Sub-national capacity building	Like most of its peers, the U.S. strategy does little beyond calling for closer incident response coordination with state, local, Tribal, and territorial (SLTT) agencies (see the introduction to Pillar One and Implementation Initiative 2.5.4).
Data management	The strategy expresses support for legislative efforts to create a "robust, clear" U.S. data privacy framework but offers no corresponding implementation initiatives (see Strategic Objective 3.1).
Regional cybersecurity leadership	The strategy makes limited mention of engaging regional partners. The implementation plan contains a few early-stage initiatives, but overall, the U.S. concept lags behind its Singaporean and Australian peers in this area (see Strategic Objective 5.2 and Implementation Initiatives 5.1.1 and 5.1.4).

7. Analysis

This section discusses the results of the Cybersecurity Strategy Scorecard. Above all, our evaluation reveals that in developing national cyber strategies, no one size fits all. The seven countries represent widely varied political, economic, digital, and threat environments, each of which demands a bespoke approach built on cybersecurity best practices and lessons learned. The strategies that received the best scores leaned into national strengths and sought to decisively address outstanding weaknesses, while those that performed worse often either failed to account sufficiently for their unique attributes or ignored them outright.

Based on the trends we observed, we offer a series of specific policy recommendations that apply to multiple countries and the field of cybersecurity strategy in general. In particular, we suggest pathways for incentivizing the private sector to invest in cybersecurity, enhancing public-private cooperation, better protecting vulnerable and underserved populations, developing and diversifying the global cyber workforce, and holding governments more accountable for strategic initiatives.

Observations: No One Size Fits All

Cyber Strategies Serve Varying Purposes and Target Audiences

Considering the widespread acceptance of technical best practices like zero-trust architecture, the seven strategies revealed more variance than expected. They use similar language with keywords like "resilience," "digital ecosystem," and "stakeholder engagement" and are made up of essentially interchangeable strategic sections (often called pillars or shields). The strategies also often embrace similar broad goals on topics like securing critical infrastructure and enhancing threat-disruption capabilities. Yet they demonstrate significant differences in their intended audiences and purpose. This might be explained by the strategies' political nature; they reflect each government's unique circumstances, including its resources, constraints, strategic priorities, and prior cybersecurity posture. The differences show that common strategic cybersecurity issues, such as designing cyber-relevant institutions, setting a policy agenda, and allocating scarce resources, are far from settled. Moreover, approaches that work in certain countries are not guaranteed to be efficient elsewhere. With these considerations in mind, we can also use national cybersecurity strategies to learn more about digital policymaking and new concepts that yield actionable lessons for other contexts.

Even before deciding on policy substance, practitioners make key decisions about their strategy's purpose, intended audience, themes, and scope. Five countries in this assessment viewed publishing a strategy as an opportunity to enumerate a comprehensive list of tasks and plans for accomplishing them beyond merely articulating an overall policy direction. This approach, designed for consumption by both internal government and external audiences, typically produces longer and more granular documents that assign operational duties to specific bodies and at least gesture toward accountability in the form of assessment metrics and outcome goals. Germany's strategy, which runs over 130 pages, represents an extreme version of this approach, declining to express a grand vision in favor of four comparatively narrow action areas, each with roughly a dozen specific objectives. Singapore and South Korea, on the other hand, have released far shorter strategies made up of less dense text supported by abundant graphics. Rather than guiding operational cybersecurity activities, strategies such as these serve mainly to communicate messages to allies and adversaries, such as to signal a stronger willingness to confront North Korea in cyberspace. While most strategy documents are written in the language of national security, Japan's stands out for devoting two of its three

pillars to softer themes like "enhancing socio-economic vitality and sustainable development" and "realizing a digital society where people can live with a sense of safety and security," though recent policy announcements indicate that Japan's cybersecurity posture is rapidly shifting to align with peers' defense-oriented approaches.[19] The seven strategies also delimit the scope of cybersecurity in multiple ways. Nearly all discuss cyber risks posed by quantum and AI technologies, Singapore's 2021 strategy being the lone exception, while others tie in other key national priorities, like the clean energy transition in the United States or "strategic industrialization" of critical and emerging technologies in South Korea.[20]

National cybersecurity strategies also reflect the political power structures that generate them. They are born from unique processes of internal negotiation and thus emerge as much from bureaucratic competition as from actual cybersecurity planning. For example, South Korea's National Intelligence Service (NIS) owns or shares responsibility for over a third of all implementation tasks, more than any other body. This authority likely reflects its institutional power more than a considered determination that responsibilities for crisis management and incident response should belong to an intelligence agency with a history of insularity and politicization.[21] The atypical design of the U.S. cybersecurity apparatus, in which CISA, ONCD, and elements of the National Security Council exercise overlapping remits, stems from contrasting visions in Congress and the White House.[22] Moreover, all strategies reflect the political orientation of the government that published them, albeit to varying degrees. It is not a coincidence that the first tactical objective presented in Australia's 2023 strategy, generated by a center-left Labor government, is to "support small and medium businesses to strengthen their cyber security" or that South Korea's hawkish government explicitly designates North Korea the focus of its 2024 strategy, a marked shift from the dovish Moon administration's 2019 strategy that did not name Pyongyang once.[23] Five strategies begin with a foreword from the head of state or cabinet minister responsible for cybersecurity.[24] Other political aspects are more subtle, such as the use of coded jargon like "decisive decade" and "Global Britain" in the U.S. and UK strategies, respectively.[25] Even where political influence seems less pervasive, as in the cases of Singapore, Germany, and Japan, national strategies should be viewed as tools for expressing aspirations and geopolitical signals rather than purely reasoned descriptions of current realities or future expectations.

Success Requires Tailoring to National Contexts, Not Just Copy-Pasting

The strongest cyber strategies tailor core policies to their national context. For example, the most notable feature of the U.S. strategy, the third pillar that proposes to "shape market forces to drive security and resilience," is something only the United States is especially well suited to execute. As officials from multiple

19 Prime Minister's Office of Japan, Expert Panel toward Improving Response Capabilities in the Field of Cybersecurity, June 7, 2024, https://japan.kantei.go.jp/101_kishida/actions/202406/07cyber.html.

20 See Strategic Objective 4.4 ("Secure Our Clean Energy Future") on pp. 25-6 of the U.S. strategy and Strategic Task 4.A ("Strategic Industrialization of Core Technologies") on pp. 35-6 of the South Korean strategy.

21 See Strategic Task 5.A.4 on p. 38 of the South Korean strategy, which proposes to "Designate the National Intelligence Service as the lead agency for cyber crisis management, overseeing the sharing of threat information, issuing alerts, and coordinating incident responses across all levels of government." See also the task assignment chart in the "National Cybersecurity Basic Plan Executive Summary."

22 For more, see: Ellen Nakashima, "Tension Grows Between Congress and the Administration over How White House Cyber Policy Should Be Run," *Washington Post,* February 18, 2021, https://www.washingtonpost.com/national-security/biden-cybersecurity-policy-congress-tension/2021/02/18/7f9d7398-6c9b-11eb-ba56-d7e2c8defa31_story.html?_pml=1.

23 See Objective 1.1 ("Support Small and Medium Businesses to Strengthen their Cyber Security") on pp. 18-9 of the Australian strategy and p. 11 of the South Korean strategy's "Background" section. The South Korean National Cybersecurity Basic Plan devotes seven pages to discussing the "Achievements of the Yoon Suk Yeol Administration in the Past Two Years and Future Direction" (see pp. 18-24).

24 Germany and Japan's strategies have no political introduction.

25 See p. 1 of the U.S. strategy's "Introduction" and "Global Britain in a Competitive Age" under "Strategic Context" on p. 17 of the UK strategy.

countries' cyber agencies noted in interviews, the United States' strong market power allows it to enforce stricter private sector accountability, to the extent it wishes to do so. In other words, while other governments risk alienating companies if they attempt to hold stewards of data accountable or shift liability for insecure software products, companies will generally adapt to new requirements rather than withdraw from the U.S. market. For countries like Singapore and Japan, which rely heavily on the digital services of multinational corporations typically based in the West, it is more difficult to shape private sector behavior. Moreover, countries aiming to develop their cybersecurity industries may be cautious about implementing major structural changes such as strict software liability requirements too soon, which could discourage businesses from entering or remaining in the market.[26] In short, considerations related to market size and maturity, to say nothing of other areas, often lead states to opposite policy conclusions that are both correct in context.

The most thoughtful workforce development strategies are also designed to align with the unique characteristics of the national environment. Allowing that all such plans share baseline similarities, like commitments to expanding cybersecurity education and reducing obstacles to hiring and retention, three distinct approaches stand out. Australia's strategy places immigration at the center of its workforce development plan in the hope that "a new global outreach capability and re-energized local outreach network will allow us to access critical talent pools and put Australia back in competition with other countries for the highly skilled migrants we need."[27] By contrast, Japan, which historically has taken a restrictive stance on immigration, prioritizes upskilling the current IT workforce and elevating the appeal of the cybersecurity profession with an eye toward creating "a virtuous cycle that attracts talented human resources who will lead the next generation."[28] The strategy outlines complementary programs such as "Plus Security," which aims to equip non-technical professionals like business executives with stronger digital familiarity, and various IT literacy schemes. Finally, while the U.S. cyber workforce strategy endorses both upskilling and immigration, its primary focus, by far, is expanding the cybersecurity labor pool through education and other investments.[29] Nearly all strategies express strong commitments of varying substance to increasing diversity in the cybersecurity field, both as a moral imperative and as a means of expanding the labor force.[30]

Local conditions have contributed to interesting contrasts in the countries' approaches to cyber intelligence gathering and threat mitigation. The Germany scorecard above notes the borderline-incomprehensible web of government agencies with some level of responsibility for cybersecurity. Moreover, Germany's federal system devolves exceptional power to the 16 states, each of which has its own cyber authority and unique strategy. As the national strategy acknowledges, the fact that the states exercise default jurisdiction over most cyber incidents "means that the Federation itself cannot take threat prevention action even in case of major, complex and/or international cyber threat situations that call for a solution at a national level and

26 See, for example, "Develop Advanced Capabilities for Economic Growth and National Security" on p. 44 of the Singaporean strategy.

27 See p. 48 of the Australian strategy under Shield Five, objective 17.

28 See "Recruitment, development, and active use of human resources" (4.4.2) on pp. 54-5 of the Japanese strategy. Indeed, Japan expresses on p. 20 a desire to avoid "a situation in which Japan must rely excessively on foreign sources for products, services, and technology related to cybersecurity," though that description unfortunately seems to correspond to the country's current reality.

29 See 3.3.5 ("Develop immigration policies to welcome and retain foreign-born talent into the nation's cyber workforce") on p. 31 of the U.S. workforce development strategy.

30 See, for example, Strategic Objective 4.2 ("Attract and Hire a Qualified and Diverse Federal Cyber Workforce") in the U.S. workforce development strategy; "Support youths, women, and mid-career professionals to pursue a cybersecurity career" and "attract diverse talent" in Chapter five of the Singaporean strategy (pp. 53-4); Objective 2 ("Enhance and expand the nation's cyber skills at ever level, including through a world class and diverse cyber security profession that inspires and equips future talent") of the UK strategy; and "Improve the diversity of the cyber workforce" under initiative 17 of Australia's strategy (p. 49).

often also require international coordination."[31] Accordingly, German law enforcement faces a mismatch in empowerment, where less-capable local authorities exercise wider remits in terms of intelligence gathering and disruption activities than better-resourced federal agencies. Even though the German national strategy proposes several mitigation measures, cybersecurity policy and efficiency drives alone are insufficient to remediate the disadvantages of structurally decentralized authority.[32]

Contrastingly, in the United States, federal authorities dominate but face stiff restrictions on certain forms of intelligence gathering, especially domestic surveillance. This norm has contributed to the scattered distribution of cybersecurity responsibilities: CISA sits under the Department of Homeland Security, apart from law enforcement agencies like the FBI and intelligence organizations like the National Security Agency, which is responsible not only for signals intelligence collection but for safeguarding U.S. national security systems. Other countries have imposed fewer restrictions on their intelligence and cyber agencies, often deliberately promoting their integration. The Australian Cyber Security Centre (ACSC) and UK National Cyber Security Centre (NCSC), for example, sit under their respective signals intelligence agencies, which are empowered to work "across the full spectrum of cyber operations."[33] As noted above, in South Korea the NIS is "the lead agency for cybersecurity" and bears responsibility for more cybersecurity tasks than any other body.[34] Interviews with officials from those countries suggest the integrative arrangement facilitates valuable synergies between offensive and defensive complements in areas such as surveillance or pursuing threat actors. Of course, that structure raises questions about civil liberty protections and cooperation across the wider interagency. Singapore and Japan exemplify yet another approach in which the centralized cybersecurity agency sits under a digital ministry and reports to the cabinet, centering its mission around civil initiatives like economic growth and secure digitalization rather than national security per se.

Recommendations

1. Improve incentives for private-sector cybersecurity

Robust private sector incentive structures should be a core part of national cybersecurity. The private sector's cybersecurity efforts are hampered by misaligned incentives and outdated, reactive approaches characterized by meeting minimum requirements and minimizing costs. Most countries mention an ambition to improve cybersecurity incentives for the private sector and encourage more proactive protections but fail to provide practical solutions for how to do so. The U.S. strategy is a notable exception, which leads the way with clear examples and pragmatic action plans for incentive alignment. For example, its secure-by-design plan to shift liability to organizations penalizes insecure products, thus incentivizing the additional cost required to create and develop secure products. Initiatives like the U.S. Cybersecurity Apprenticeship Program foster partnerships between government, academia, and the private sector to address the skill gap in cybersecurity, incentivizing organizations to invest in developing a skilled workforce while supporting broader national

31 See 8.3.1 "Improving the options available to the Federal Government for threat prevention in case of cyberattacks" on p. 79 of the German strategy. Full text: "The Federation only has special jurisdiction over threat prevention in certain areas, such as national self-protection, international terrorism, border protection," and railways. "In all other cases, the federal states have jurisdiction over threat prevention, which means that the Federation itself cannot take threat prevention action even in case of major, complex and/or international cyber threat situations that call for a solution at national level and often also require international coordination. This assignment of responsibilities is not appropriate for the current threat situation in the cyber domain… It is not possible to effectively counter cyber threats in Germany in this way in the long term."

32 See 8.3.1, 8.3.3, 8.3.7, and 8.3.12 of the German strategy.

33 See "Why Australia has an opportunity to lead" on p. 13 of the Australian strategy.

34 See South Korea's National Cybersecurity Basic Plan, p. 14.

security and economic goals.

Despite the strong example from the United States, most governments struggle to adequately incentivize private sector protections, haphazardly adopting a mix of "carrot" and "stick" policy tools, including regulation, legislation, subsidies, grants, and direct service provision. There is an especially pressing lack of data-driven approaches that clearly show how and why certain policy interventions are useful for organizations. The collective failure to secure private sector digital systems and products is a negative economic externality. Proceeding on this basis, we make several suggestions for how countries can focus and enhance their efforts to improve private-sector cybersecurity incentives below.

1.A Invest in making cyber risk assessment more transparent and measurable

To address the negative externality of insecure products and systems, we first need accurate tools to measure it. All countries we analyzed, with the notable exception of Singapore, fail to address this. Consequently, most governments implement various regulatory and subsidy schemes without a strategic-level quantification of their expected impact. Furthermore, it is often unclear how much companies should spend to upgrade their cybersecurity and how these upgrades relate to the company's growth and profitability. The cyber insurance market will hopefully provide a better understanding of cybersecurity costs equations and risks in the coming years, but it is still a nascent field with many uncertainties. Thus, governments cannot currently rely on the private sector to spend an adequate amount on cybersecurity without policy intervention.

We suggest countries initiate efforts to better measure the costs of cyber risk and returns on cybersecurity investments across the economy. Singapore has made progress in this direction by estimating the costs of cybersecurity attacks through its Cyber Risk Management (CyRiM) project, initiated in 2016. This was a partnership led by the Nanyang Technological University, drawing on contributions from the government (specifically the Monetary Authority of Singapore), industry, and broader academia. The project generated a series of reports on the costs of various attacks, as well as a pricing tool for calculating insurance premiums.[35] More governments should work on this issue and consider metrics such as the speed at which enterprises detect and eject threat actors, the turnover rate of exploited vulnerabilities, and shifts in cyber insurance claims.[36] While any attempts at measuring externalities are by their nature fraught, the ideas mentioned above provide more actionable insights into whether government policies are meaningfully reducing systemic cyber risks. We strongly encourage more governments to attempt to do so. Furthermore, this is an excellent area for global collaboration, as many cost examples will generalize across different geopolitical contexts and technical infrastructures without requiring stakeholders to share sensitive data.

1.B Avoid overreliance on certifications

Cybersecurity certification schemes are very common, but overreliance on certifications can generate several problems. The idea that certifications facilitate more secure markets has led to their widespread adoption. For example, Germany, and the European Union's ENISA, issue and expand cybersecurity certifications for IoT and other technical products and services. The UK's strategy utilizes the widely successful Cyber Essentials certification scheme, first promoted in the UK's 2016 strategy, to create board-level incentives

35 Nanyang Technological University Singapore, Cyber Risk Management Project, 2016, https://www.ntu.edu.sg/irfrc/research/cyrim.

36 Prof. Jason Healey has developed this proposal in more detail in "Measuring Policy Effectiveness of Cyber Defensibility and Deterrence," *Lawfare*, September 10, 2024, https://www.lawfaremedia.org/article/measuring-policy-effectiveness-of-cyber-defensibility-and-deterrence.

for cyber risk management. Japan offers a similar strategy to raise executive awareness of cybersecurity, and Singapore is focused on "innovating to build world-class products and services" through their National Integrated Centre for Evaluation (NICE), including a robust certification scheme to validate products with adequate cybersecurity. Their strategy refers to the country's excellent cybersecurity certification guide, introduced by Singapore's Cybersecurity Certification Center, and includes convenient services such as a QR code that leads to a list of all certified products. Singapore has also developed the Singapore Common Criteria Scheme (SCCS), a continuation of the globally recognized Common Criteria (CC) standard for certifications (ISO/IEC 15408).

Despite their popularity, certifications are no panacea. They rapidly become outdated in the modern technical environment, can incentivize optimizing for compliance rather than actual security, and can cause regulatory capture when unaffordable for smaller companies. No strategy mentions how to mitigate these drawbacks. When governments are looking to implement certification schemes, we suggest they also consider how their strategy will address their shortcomings. For example, combining certification schemes with subsidies for SMEs could limit regulatory capture. Guidelines for periodic review and adjustment of certification standards could help ensure certifications remain relevant and effective. Governments should also ensure that certifications go beyond product- and service-specific technical requirements, extending into an examination of company culture and promoting proactive stances to secure products and systems. In doing so, they have a better chance of avoiding incentives to not exceed a low and static bar for cybersecurity.

1.C Expand private-sector cybersecurity assistance beyond financial aid

Most countries aim to reduce cybersecurity costs facing private companies, especially SMEs. However, the strategies often lack thoughtful consideration of how this will impact the companies' cybersecurity outcomes beyond just reducing the cost to implement basic protections. There are many examples of financial assistance earmarked for SMEs. For example, Singapore and Japan offer pre-approved cybersecurity solutions subsidized for small and medium sized enterprises. Germany offers financial support for SMEs to improve their IT security, encouraging cybersecurity adoption at scale through programs like *go-digital* and *Digital Jetzt*. Australia offers an inverted approach by limiting regulatory burdens for small businesses, and Japan's strategy discusses reduced cyber insurance premiums for small businesses.[37]

While these financial incentives are valuable, they cannot stand alone as the primary tool for strengthening private-sector cybersecurity. The delivery of many of these initiatives lacks consideration of the nuanced or secondary impacts they are likely to have on firms' actual cybersecurity posture. For example, Singapore's approach of providing SMEs with subsidized, pre-approved cybersecurity solutions risks creating a one-size-fits-all scenario where the solutions may not fully meet the diverse needs of all businesses. This can lead to a false sense of security if the products do not address specific vulnerabilities unique to certain businesses. Other proposed subsidy programs like Germany's *go-digital* and *Digital Jetzt* offer no guidance on what the application process will look like. Overly complex or bureaucratic application processes could impose costs and deter the very SMEs they aim to help. On the other hand, overly lax requirements can lead to wasted resources, dependency on government support, and a failure to foster genuine, self-sustained cybersecurity improvements.

37 However, as of November 2024, there is no publicly available information indicating that the Japanese government has implemented a strategy to reduce cyber insurance premiums specifically for small businesses. Despite this, the cyber insurance market in Japan is experiencing significant growth, driven by increased awareness of cyber risks and the adoption of digital platforms across various industries. The market is projected to grow at a compound annual rate of 20.8% during 2024-2032 (see https://www.imarcgroup.com/japan-cyber-insurance-market).

To ensure financial support leads to meaningful security improvements, governments should complement subsidies with broader measures that actively build long-term cybersecurity capacity. This includes targeted training programs, hands-on security audits, and other incentives for the private sector, and especially for SMEs, to adopt industry best practices rather than just baseline compliance. Countries should also balance the financial incentives with stronger accountability mechanisms to ensure that the security improvements are measurable and sustainable rather than one-time fixes. We also propose that governments provide clearer guidance on how SMEs can access public cybersecurity assistance, such as subsidies and services, as well as clear measures of success for these initiatives that consider the long-term cybersecurity impact on the companies they aim to help.

Financial assistance, when implemented effectively, can serve as a powerful catalyst to foster mature private-sector cybersecurity. However, it should be integrated into a broader strategy that includes education, guidance, and adaptable security frameworks. Governments should not just fund cybersecurity improvements but actively shape how businesses build lasting resilience against cyber threats. To that end, it is reasonable for governments to offer financial assistance for cybersecurity, especially to SMEs, and if it is done correctly, it can help them create a sustainable security culture early on. However, financial assistance alone will not be sufficient unless it is widely accessible and directed towards dynamic and robust system-level cybersecurity improvements.

2. Foster trust between public and private sectors in incident response

Another central concern of governments ought to be how to incentivize information sharing between the public and private sectors. Threat information sharing is often hindered by excessive bureaucracy and national security concerns. Organizations are disincentivized to report cyber incidents due to potential legal repercussions (e.g., arising from compliance breaches), reputational damage, or additional costs. It is also not always clear how and to whom cyber incidents should be reported. Many countries have proposed initiatives to address this. We have noted the most promising approaches in the paragraphs below.

The UK's Industry 100 (i100) initiative, the United States Joint Cyber Defense Collaborative (JCDC), and Australia's robust threat intelligence and blocking program are excellent examples of how governments can improve real-time threat intelligence and knowledge sharing between the public and private sectors. The Industry 100 initiative temporarily embeds industry experts within the NCSC while remaining on the payroll of their company to preserve their independence. In this scheme, the NCSC benefits from the latest industry trends and technical solutions, while industry participants gain exposure to government cybersecurity strategies, best practices, and threat intelligence. This expedites collaboration and enables quicker response times to cybersecurity challenges. Australia's model aims to create a hub-and-spoke system linking ISACs, industries, and companies, enhancing actionable threat intelligence sharing on a larger scale. Embedding private sector experts in government discussions (as seen in i100) and broader threat intelligence sharing programs (as seen in Australia) are both best-practice approaches to fostering more efficient public-private collaboration. Governments can also encourage global third-party actors, like the World Economic Forum and the United Nations, to foster industry information-sharing initiatives between organizations worldwide.

Australia and Singapore have separated their national entities responsible for law enforcement and cyber incident response in an effort to promote faster and more effective crisis mitigation. Their governmental cybersecurity incident response teams have adopted "firefighter-like" postures where they aim to quickly help the affected organization without having the authority to penalize them. For example, the incident response team in Singapore is part of the Digital Ministry rather than law enforcement, creating liability

protection for companies that report breaches. Australia's "all-hazards" cyber incident response capability is owned by the Australian Signals Directorate (ASD). Since ASD is part of the Department of Defense and not a law enforcement organization they lack the authority to prosecute critical infrastructure providers during responses to major attacks. In addition to making it safer to report cyber incidents, governments must make it easier to report them, especially for small and medium-sized organizations and private individuals. Australia's single-service incident reporting portal is a great example of an access-enabling initiative to that end. It is further complemented by extensive guidance on reporting obligations and official Federal-level response protocols.

3. Emphasize the cyber needs of vulnerable populations

As mentioned throughout this report, the protection of vulnerable population groups and SMEs is often neglected. For example, we found little or insufficient mention of specific protections for minorities, the elderly, or young people in the German, South Korean, U.S., and UK strategies. The following paragraphs highlight examples of strategies that prioritize protecting their whole societies in cyberspace.

In Singapore, the "Data Protection as a Service" initiative offers accessible, managed solutions to SMEs, enabling them to protect sensitive information without significant internal resources, reinforcing digital safety across smaller businesses. Singapore also tailors cybersecurity programs for seniors and youth, addressing specific demographic vulnerabilities and fostering cyber awareness in each age group.

Japan's whole-of-society approach to cybersecurity uses several noteworthy cybersecurity measures to protect vulnerable groups like the elderly, children, and rural communities. The strategy emphasizes a mix of public outreach, education, and resilience-building programs. Japan's cybersecurity strategy also emphasizes the importance of public awareness and training initiatives to address low cyber literacy among older citizens, who are often targeted by digital scams. This approach is part of a comprehensive effort to increase resilience among all population segments, particularly those most susceptible to cyber threats.[38] To protect young people online, Japan has developed targeted educational programs that focus on digital safety and online security awareness. These programs align with Japan's broader strategy, which aims to incorporate a whole-of-society approach to cybersecurity, encouraging collaboration among civil society, local organizations, and government bodies to foster cyber resilience.[39]

Australia promotes culturally inclusive and tailored cybersecurity education and recognizes that vulnerable groups, including First Nations communities, culturally and linguistically diverse populations, people with disabilities, seniors, and young people, often face unique challenges and barriers in accessing cyber support and resources. To address this, the strategy highlights several interesting initiatives to make cybersecurity awareness and education more accessible and relevant to these groups. First, a community grant program empowers local community leaders to design and implement cyber awareness campaigns that are culturally and linguistically tailored to the specific needs of diverse groups. This increases the reach of campaigns and ensures they are delivered in a culturally resonant way. Australia's approach also includes the "Cyber Wardens" program, which trains individuals within businesses and communities to act as primary contacts for cybersecurity concerns, promoting knowledge-sharing and proactive security measures at the grassroots level.

---

38 Asia Society, "High Risk Japan — How Vulnerable is Japan to Cyber Attacks?", May 25, 2023, https://asiasociety.org/video/high-risk-japan-how-vulnerable-japan-cyber-attacks.

39 Christine, Debora and Thinyane, Mamello, "Cyber Resilience in Asia-Pacific: A Review of National Cybersecurity Strategies," United Nations University, 2020, https://collections.unu.edu/view/UNU:7760.

These strategies reflect a growing recognition that cybersecurity must adapt to diverse needs, as different population segments and business sizes face unique risks. However, we encourage more research on how and when to tailor cybersecurity programs to different demographics, such as tracking engagement patterns, data-driven methods to customize training to specific populations, and interviews or participatory approaches to understand user needs and develop solutions together with target communities. Lastly, we encourage all governments to prioritize digital literacy, which is a necessary precondition for cyber hygiene and awareness, and recognize that this is especially critical for vulnerable groups who may lack the resources to become digitally literate without government intervention.

4. Cultivate a stronger cybersecurity workforce

Many strategies discuss expanding the workforce through diversity but most fail to produce tangible and meaningful plans to address it. For example, the Australian strategy outlines several workforce development initiatives, including some to support underrepresented groups, but does not back these with specific, actionable implementation plans. The strategy mentions initiatives to attract and retain diverse talent but fails to provide targeted support or measurable goals for increasing women's representation in the sector. Without concrete programs or benchmarks focusing on gender diversity, the plans are unlikely to produce meaningful change. Similarly, Singapore's strategy emphasizes workforce development through partnerships with educational institutions and professional programs that include youths, women, and mid-career professionals. While it explicitly mentions women as a target group, the strategy does not offer specific programs or support systems uniquely tailored to women's challenges in entering or advancing in cybersecurity roles. The emphasis remains on general upskilling and pipeline development, which, though beneficial, is unlikely to address the systemic issues that prevent women and minorities from joining or staying in cybersecurity roles.

The U.S. and UK strategies have made contrastingly strong contributions to promoting diversity in cybersecurity. The U.S. National Cyber Workforce and Education Strategy lays out the most comprehensive plan for boosting the cyber workforce, improving technical education outcomes, and reaching groups that are often underrepresented in the field. The UK's CyberFirst program, in particular, stands out as an example of how countries can foster excitement for careers in cybersecurity for a diverse group of young people. The program is specifically targeted at students in secondary and tertiary education, offering events and financial support for those pursuing cybersecurity qualifications.[40] Importantly, the CyberFirst Girls competition - a nationwide, Year 8 level, girls-only competition to develop cybersecurity solutions - is the flagship of the CyberFirst program.[41] Beyond directly providing inspiration and support for young women interested in cybersecurity, the prominence of the CyberFirst Girls competition is a strong signal of the UK's commitment to building a more inclusive environment for women in cybersecurity. The UK government also actively supports a community of organizations dedicated to advancing diversity in cybersecurity, including several NGOs.[42] Other countries could heed this example and build similarly prominent programs for young women interested in the field.

40 UK National Cyber Security Centre, CyberFirst overview, https://www.ncsc.gov.uk/cyberfirst/overview.

41 UK National Cyber Security Centre, CyberFirst Girls Competition,, https://www.ncsc.gov.uk/cyberfirst/girls-competition.

42 See, for example, the Cyber Girls First initiative at https://cybergirlsfirst.com/ . This NGO is an example of a successful initiative inspiring women to take up careers in technology. Since its launch, the initiative has helped improve uptake of computer science and IT subjects at the General Certificate of Secondary Education level amongst girls, often leading to apprenticeships and related university courses. The initiative hosts events that introduce girls aged 11-14 to coding, IT, and cybersecurity.

5. Specify accountabilities and establish clear metrics for implementation

Many countries have published implementation plans to complement their national cybersecurity strategies, and while we commend this effort, we have found that there is substantial room for improvement in assigning accountabilities for implementation. The Accountability subcategory in our scorecard had some of the fewest leading ratings overall, with developing outcome-oriented goals being the *only* element in our scoring matrix for which there were *zero* leading ratings. This is a product of hazy accountabilities and unclear measures of success, with many countries specifying that they will merely make further plans under certain initiatives. Take, for example, U.S. Strategic Objective 1.3.1. "Assess and improve Federal Cybersecurity Centers' and related cyber centers' capabilities and plans necessary for collaboration at speed and scale," for which the accompanying text prescription reads as follows: "ONCD will lead the Administration's efforts to enhance the integration of centers such as these, identify gaps in capabilities, and develop an implementation plan to enable collaboration at speed and scale." This is effectively a plan for a plan, with no clear measure of success or even a definition for "speed" or "scale." This problem is not unique to the United States; all countries have used similarly vague planning language in their strategies.

To make progress on implementation, we recommend that countries adopt much more specific, measurable, and, therefore, transparent accountabilities. For example, every initiative should have a specific, individual owner (i.e., a position title, not an agency name) who is ultimately responsible for successful delivery by a clear deadline. What counts as successful delivery should also be measurable - taking the above U.S. example, this would mean that improvements in speed and scale would be defined, for example, in terms of the percentage improvement in initial system response time to an incident or number of reports shared. We acknowledge that many measurements of cybersecurity performance are fraught, and we encourage policymakers to consider how this problem can be tackled strategically. One promising proposal from Prof. Jason Healey is to develop baseline and directional indicators for nationwide cybersecurity performance tied to impact, threat, and vulnerability levels, similar to economic indicators like the CPI. Policymakers could also assess factors such as the mean time to detect and eject adversaries, the frequency of systemic cyber incidents, and the financial impact of major breaches over time.[43] By embedding such measures into national strategies, governments can transition from broad policy aspirations to tangible benchmarks that track progress in cybersecurity effectiveness. Whether adopting these suggestions or otherwise, we strongly encourage policymakers to make measurable outcomes a focus of their ongoing efforts to build robust national cybersecurity strategies.

43 Prof. Healey has developed this proposal in more detail in "Measuring Policy Effectiveness of Cyber Defensibility and Deterrence," *Lawfare*, September 20, 2024, https://www.lawfaremedia.org/article/measuring-policy-effectiveness-of-cyber-defensibility-and-deterrence.

8. Conclusion

As nations grapple with an increasingly complex digital landscape, the importance of robust, well-crafted cybersecurity strategy is only growing. Cyber policymakers must navigate deepening geopolitical tensions, rapid technological change, and evolving security threats, to name just a few challenges. At the same time, the changing context presents opportunities to leverage emerging technologies and international partnerships to enhance national cybersecurity postures.

This report is intended to help cybersecurity policymakers develop effective strategy in the face of those evolving circumstances. It has analyzed the cybersecurity strategies of seven leading nations, providing insights into their current approaches and identifying best practices. Our comparative evaluation reveals plenty of commonalities but a surprising number of major differences in how countries address cybersecurity challenges. While some nations excel in certain areas, there is no perfect or universally applicable strategy. Each country's approach reflects its unique geopolitical context, technological capabilities, and national priorities. However, several key themes have emerged that are likely to shape the future of national cyber strategy.

The most effective strategies demonstrate a holistic approach, recognizing that cybersecurity is not merely a technical issue but one that intersects with economic, diplomatic, and national security concerns. Successful concepts integrate cybersecurity considerations across all sectors of government and society, fostering a whole-of-nation approach. Furthermore, strategies need to incorporate mechanisms for regular reviews and updates to remain effective. Successful strategies must also prioritize partnerships. The global, interconnected nature of modern information technology renders international and domestic cooperation essential to every country's cybersecurity approach. The most forward-thinking strategies emphasize the importance of cross-border and cross-sector collaboration, information sharing, and joint capacity-building efforts. Lastly, security must be balanced with other priorities, such as innovation, economic growth, and privacy. Strategies need to address these trade-offs explicitly, ideally grounded in quantitative considerations of cost and risk, and propose balanced solutions.

We found common areas for improvement across all seven cyber strategies we analyzed and offered recommendations for future cybersecurity policymakers to address them. Specifically, we suggest approaches for strengthening private sector cybersecurity, enhancing public-private cooperation, better protecting vulnerable populations, taking a more expansive view of workforce development, and making government implementation accountabilities more specific and measurable. We also highlight examples of policies from countries that perform well against these common pitfalls to serve as models for other national cybersecurity strategies.

We hope that our comparative analysis offers valuable lessons for policymakers worldwide. By learning from the strengths and weaknesses of existing strategies, nations can better prepare themselves for the cyber challenges of tomorrow. As we conclude this year-long endeavor, we are both humbled by the complexity of the challenges ahead and inspired by the collective wisdom and innovation demonstrated by nations striving to secure our shared digital future.

9. Appendix: The Full Cybersecurity Strategy Scorecard

Category	Sub Category	Element	Australia (2023)	Germany (2021)	Japan (2021)	Singapore (2021)	South Korea (2024)	UK (2022)	US (2023)
Protecting People and Infrastructure	**Critical infrastructure**	Critical manufacturing & production	Meeting the bar	Meeting the bar	Lagging	Meeting the bar	Meeting the bar	Lagging	Leading
		Financial	Leading	Meeting the bar	Lagging	Leading	Meeting the bar	Leading	Meeting the bar
		Government systems & public services	Leading	Leading	Meeting the bar	Leading	Meeting the bar	Meeting the bar	Leading
		Health services	Leading	Lagging	Lagging	Leading	Meeting the bar	Meeting the bar	Meeting the bar
		IT and communications	Leading	Meeting the bar	Meeting the bar	Leading	Meeting the bar	Leading	Leading
		Transport	Leading	Lagging	Meeting the bar	Leading	Meeting the bar	Meeting the bar	Meeting the bar
		Utilities	Leading	Lagging	Meeting the bar	Leading	Meeting the bar	Meeting the bar	Leading
	Non-critical private industries	Large corporations	Leading	Meeting the bar	Meeting the bar	Leading	Meeting the bar	Leading	Leading
		Small-to-medium sized organizations	Leading	Leading	Leading	Leading	Lagging	Leading	Lagging
		Shared global systems	Leading	Lagging	Lagging	Leading	Lagging	Meeting the bar	Leading
	Citizens	General population	Leading	Leading	Leading	Leading	Meeting the bar	Leading	Meeting the bar
		Vulnerable populations	Leading	Meeting the bar	Leading	Leading	Lagging	Meeting the bar	Lagging
		Civil society	Meeting the bar	Meeting the bar	Leading	Meeting the bar	Lagging	Meeting the bar	Lagging
	Data	Data privacy standards	Meeting the bar	Leading	Meeting the bar	Meeting the bar	Meeting the bar	Leading	Lagging
		Data management standards	Leading	Leading	Leading	Meeting the bar	Meeting the bar	Leading	Lagging
		Digital ID	Leading	Leading	Lagging	Lagging	Lagging	Leading	Meeting the bar
	Active defense	Disruptive activities	Leading	Lagging	Meeting the bar	Meeting the bar	Leading	Meeting the bar	Leading
		Counter-influence operations	Lagging	Meeting the bar	Meeting the bar	Lagging	Leading	Meeting the bar	Meeting the bar
		Preventive intelligence gathering	Meeting the bar	Leading	Meeting the bar	Lagging	Leading	Leading	Leading
		Threat sharing	Leading	Meeting the bar	Leading	Meeting the bar	Leading	Leading	Leading
Generating Capacity	**Workforce development**	Technical government cyber practitioners	Leading	Lagging	Leading	Leading	Meeting the bar	Leading	Leading
		Non-technical government cyber professionals (e.g	Lagging	Lagging	Meeting the bar	Lagging	Lagging	Meeting the bar	Meeting the bar
		Local and regional law enforcement	Lagging	Lagging	Meeting the bar	Meeting the bar	Lagging	Meeting the bar	Lagging
		Private cybersecurity workforce	Leading	Lagging	Meeting the bar	Leading	Meeting the bar	Leading	Leading
		General technology workforce	Leading	Lagging	Meeting the bar	Meeting the bar	Lagging	Meeting the bar	Meeting the bar
		Entrepreneurs	Meeting the bar	Meeting the bar	Lagging	Meeting the bar	Lagging	Leading	Leading
	Skill development	Education and training	Leading	Meeting the bar	Leading	Leading	Meeting the bar	Leading	Leading
		Awareness	Leading	Meeting the bar	Leading	Leading	Meeting the bar	Leading	Meeting the bar
	Market development	Cybersecurity firms	Meeting the bar	Lagging	Meeting the bar	Meeting the bar	Meeting the bar	Leading	Leading
		Emerging technology firms	Meeting the bar	Meeting the bar	Leading	Lagging	Leading	Leading	Leading
		Research institutions	Meeting the bar	Leading	Leading	Leading	Meeting the bar	Leading	Leading
Building Partnerships	**Private sector & NGOs**	Private companies	Leading	Meeting the bar	Leading	Leading	Leading	Leading	Leading
		Research institutions	Meeting the bar	Leading	Leading	Leading	Meeting the bar	Meeting the bar	Leading
		Civil society organizations	Lagging	Leading	Lagging	Meeting the bar	Meeting the bar	Meeting the bar	Meeting the bar
	Domestic government	Local government	Lagging	Meeting the bar	Leading	Meeting the bar	Meeting the bar	Meeting the bar	Meeting the bar
		State/regional government	Lagging	Meeting the bar	Leading	Meeting the bar	Lagging	Leading	Meeting the bar
		National interagency	Leading	Meeting the bar	Meeting the bar	Leading	Meeting the bar	Leading	Leading
	International cooperation	Regional allies and partners	Leading	Leading	Meeting the bar	Leading	Leading	Meeting the bar	Meeting the bar
		Global allies and partners	Meeting the bar	Meeting the bar	Meeting the bar	Leading	Leading	Leading	Leading
		Behavioral norms	Leading	Leading	Meeting the bar	Leading	Leading	Meeting the bar	Leading
		Technical standards	Meeting the bar	Meeting the bar	Lagging	Leading	Lagging	Meeting the bar	Leading

Category	Sub Category	Element	Australia (2023)	Germany (2021)	Japan (2021)	Singapore (2021)	South Korea (2024)	UK (2022)	US (2023)
Codifying Roles and Responsibilities	Government roles	National cyber coordinator	Leading	Meeting the bar	Meeting the bar	Leading	Leading	Leading	Meeting the bar
		Cybersecurity agencies	Leading	Leading	Leading	Leading	Meeting the bar	Meeting the bar	Leading
		Intelligence agencies	Leading	Leading	Meeting the bar	Meeting the bar	Leading	Meeting the bar	Leading
		Law enforcement	Leading	Meeting the bar	Leading	Meeting the bar	Meeting the bar	Meeting the bar	Leading
		Foreign ministry	Leading	Meeting the bar	Meeting the bar	Meeting the bar	Leading	Leading	Leading
		Regulatory agencies	Meeting the bar	Meeting the bar	Meeting the bar	Leading	Meeting the bar	Meeting the bar	Leading
		Internal cybersecurity responsibilities of governmer	Leading	Leading	Meeting the bar	Leading	Meeting the bar	Leading	Leading
	Private sector roles	Role of private sector partners in cybersecurity	Meeting the bar	Meeting the bar	Leading	Leading	Leading	Leading	Leading
		Obligations of private companies (to shareholders,	Leading	Leading	Meeting the bar	Meeting the bar	Meeting the bar	Meeting the bar	Leading
		Private sector cybersecurity incentive alignment	Meeting the bar	Meeting the bar	Meeting the bar	Meeting the bar	Meeting the bar	Meeting the bar	Leading
	Procedural responsibilities	Cyber advice and services	Leading	Leading	Leading	Leading	Meeting the bar	Leading	Meeting the bar
		Reporting obligations	Leading	Meeting the bar	Lagging	Meeting the bar	Lagging	Leading	Leading
		Incident response	Leading	Meeting the bar	Leading	Leading	Leading	Leading	Leading
		Regulatory harmonization	Meeting the bar	Leading	Meeting the bar	Leading	Lagging	Meeting the bar	Leading
		Counter-ransomware	Leading	Lagging	Lagging	Meeting the bar	Meeting the bar	Meeting the bar	Leading
	Technical standards and responsibilities	System and network hardening	Lagging	Meeting the bar	Meeting the bar	Leading	Meeting the bar	Meeting the bar	Leading
		Supply chain security	Meeting the bar	Meeting the bar	Leading	Meeting the bar	Meeting the bar	Meeting the bar	Leading
		Resilience and redundancy	Meeting the bar	Meeting the bar	Meeting the bar	Leading	Leading	Leading	Leading
		Emerging technology threats	Leading	Leading	Leading	Lagging	Meeting the bar	Leading	Leading
Communicating Clear Policy	Context	Assessment of threats and resources	Meeting the bar	Leading	Leading	Leading	Leading	Leading	Leading
		Policy precedents	Meeting the bar	Leading	Meeting the bar	Meeting the bar	Leading	Leading	Leading
	Presentation	Digestible language	Leading	Leading	Lagging	Leading	Leading	Meeting the bar	Leading
		Logical categories	Leading	Meeting the bar	Meeting the bar	Leading	Leading	Meeting the bar	Meeting the bar
		Comprehensiveness	Leading	Leading	Leading	Meeting the bar	Meeting the bar	Leading	Leading
		Specific action items	Meeting the bar	Meeting the bar	Meeting the bar	Meeting the bar	Lagging	Leading	Leading
	Accountability	Accountable parties	Leading	Meeting the bar	Meeting the bar	Meeting the bar	Meeting the bar	Meeting the bar	Leading
		Detailed timelines	Leading	Lagging	Lagging	Lagging	Lagging	Meeting the bar	Leading
		Outcome-oriented	Meeting the bar	Meeting the bar	Meeting the bar	Meeting the bar	Meeting the bar	Meeting the bar	Meeting the bar
		Progress and efficacy assessments	Meeting the bar	Meeting the bar	Leading	Lagging	Leading	Leading	Leading