Royal United Services Institute
for Defence and Security Studies

Global Approaches to Cyber Policy, Legislation and Regulation

A Comparative Overview

Pia Hüsch and James Sullivan

Global Approaches to Cyber Policy, Legislation and Regulation

A Comparative Overview

Pia Hüsch and James Sullivan

RUSI Special Resources, April 2023

Royal United Services Institute
for Defence and Security Studies

192 years of independent thinking on defence and security

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 192 years.

(ISC)² is an international nonprofit membership association focused on inspiring a safe and secure cyber world. Best known for the acclaimed Certified Information Systems Security Professional (CISSP®) certification, (ISC)² offers a portfolio of credentials that are part of a holistic, pragmatic approach to security. Our association of candidates, associates and members, more than 365,000 strong, is made up of certified cyber, information, software and infrastructure security professionals who are making a difference and helping to advance the industry. Our vision is supported by our commitment to educate and reach the general public through our charitable foundation – The Center for Cyber Safety and Education™. For more information on (ISC)², visit https://www.isc2.org/.

The views expressed in this publication are those of the authors, and do not reflect the views of RUSI or any other institution.

Published in 2023 by the Royal United Services Institute for Defence and Security Studies.

Royal United Services Institute
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org
RUSI is a registered charity (No. 210639)

Contents

Foreword

THE STAKES HAVE never been higher for the global cyber-security community. Geopolitical tensions and macroeconomic instability are exacerbating a complex, unrelenting threat landscape. High-profile data breaches, heightened physical security concerns, insatiable business and consumer demand for connectivity everywhere, smart devices, biometrics, remote workforces and more underscore how intertwined our national, economic and personal security has become.

(ISC)² is the world's largest association of certified cyber-security professionals, with more than 365,000 members, candidates and associates. Our members uphold the highest professional standards and are dedicated to securing governments, economies, infrastructure and personal data. Our adversaries are the threat actors breaching businesses, disrupting services and eroding the confidence of our citizens.

Cyber-security professionals need help. The global workforce is understaffed and underfunded. (ISC)² research estimates that while the global cyber-security workforce now surpasses 4.7 million, we are still facing a workforce gap of at least 3.4 million people.

In recent years, we have witnessed lawmakers, standard-setters, government entities and regulators explore cyber-security policies and frameworks aimed at driving secure, resilient digital economies and safer environments for citizens. Most encouraging is that these efforts include strong calls for cyber-security expertise through varying levels of commitment to invest in supporting and growing the global cyber-security workforce.

(ISC)² sponsored this policy guide to raise awareness of the world's leading cyber-security policies that will impact the future of the global cyber workforce. The paper provides an overview of the cyber regulatory environments across the UK, the EU, the US, Canada, Japan and Singapore – offering insights on how the regulatory landscape in these jurisdictions is evolving, and what that means for governments, businesses, individuals and cyber-security professionals.

(ISC)² is deeply committed to our vision of a safe and secure cyber world. We hope this paper will not only highlight the tremendous efforts and thoughtful policy being enacted around the world, but also serve as a launch pad for more action and even greater commitment to growing a strong and diverse cyber workforce. Only a well-equipped, skilled and fully staffed workforce can implement these policies and satisfy new regulatory requirements. Our aim is to use this and future research to build awareness and drive the global harmonisation of policy and professional standards in cyber security.

By Clar Rosso, CC, (ISC)² CEO

Executive Summary

THIS PAPER AIMS to serve as a guide to policymakers by examining different approaches to cyber-security policy, regulation and legislation. It provides an overview of the priorities of five countries (the UK, the US, Canada, Japan and Singapore) and the EU. The focus rests on cyber policy advanced in the period between January 2019 and March 2023.

The research underlying this paper focuses on four key research areas:

- The general context in which cyber policy is made.
- Priorities with regard to the protection of critical national infrastructure (CNI).
- Approaches to the development of cyber skills and the cyber workforce.
- International cooperation on norm development for cyberspace.

The Context

All jurisdictions follow a unique cyber strategy, but common approaches exist:

- Strategies are updated in line with domestic timelines but also adjust to changes in the cyber threat landscape (such as the rise of cybercrime) and respond to geopolitical events and the increased need to secure CNI and supply chains.
- Strategies increasingly focus on harmonising and streamlining each jurisdiction's cyber policies to avoid fragmentation and duplication of efforts.
- There is an increasing reliance on interventionist policies and regulations to enhance resilience and cyber-security standards.

On Critical National Infrastructure

Ensuring greater protection of critical national infrastructure (CNI) is a priority for all jurisdictions examined. This is often done by updating or increasing existing cyber-security obligations, or expanding them beyond CNI sectors to further support the resilience of supply chains. International businesses and cyber-security professionals must simultaneously comply with changing (and at times varying) obligations among different jurisdictions. Further research comparing the differing scopes of CNI designations and their respective cyber-security obligations is needed.

On the Cyber Workforce

The global cyber-security workforce shortage and the need for further skills development is seen in all jurisdictions examined. A wide range of initiatives, many of which resemble each other, are advanced by the respective jurisdictions to attract talent, diversify the workforce and increasingly harmonise existing efforts. For example, several jurisdictions have adopted skills frameworks, such as the US's National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework or the European Cybersecurity Skills Framework (ECSF), to harmonise language used to describe cyber-security roles. Little is known about the effectiveness of these initiatives in markedly reducing the cyber-security workforce gap in a quantifiable way. More research is needed to understand which initiatives help reduce the gap in the cyber-security workforce.

On International Cooperation on Cyber-Norm Development

All jurisdictions examined actively cooperate on cyber-norm development and seek to advance a free and secure cyberspace. They do so by supporting UN processes for norm development, by engaging in a range of multilateral, bilateral and multi-stakeholder arrangements, and by seeking greater cooperation on cyber (including on the development of cyber-security skills and closing the gap in the cyber workforce). More cooperation on skills development could further boost understanding of how to develop global solutions to a global problem.

Introduction

TECHNOLOGICAL INNOVATION AND advancement continue to disrupt society at pace. While the economic benefits of breakthrough technologies are fairly clear, there are new cyber risks to infrastructure and data to consider. In light of these dynamics, countries are constantly designing, monitoring and refreshing their cyber-security policies, legislation and regulation to protect national security and the economic security and safety of organisations and their citizens. While some of the trends in cyber security are global, each jurisdiction's approach to cyber policy and associated legislation and regulation follows its own themes and priorities.

While the content of cyber policies naturally varies, so do the mechanisms to implement them. Jurisdictions may prefer different types of levers to implement their cyber policies. Whereas one country may prefer to legislate heavily, others may advance cyber policies through standard-setting or non-binding policies. The approach a country chooses is shaped by a multitude of complex factors, including its political standpoint, constitutional structures, the cyber-threat landscape, the role of the private sector, and other socio-legal and historical factors.

Understanding national and regional approaches to cyber policy is crucial, as these directly impact individuals and organisations operating within the respective jurisdictions. This paper allows policymakers and businesses to understand regulatory trends in several jurisdictions, providing them with up-to-date insights on how the regulatory landscape in these jurisdictions is evolving – and what that means for businesses and individuals.

This guide sets out to compare the approaches of six different jurisdictions – the UK, the EU, the US, Canada, Japan and Singapore – with regard to their respective cyber-policy agendas. The aim here is to improve understanding of the impact these policy agendas have on businesses and individuals working in these jurisdictions. This paper provides a valuable overview of different approaches to cyber policy by identifying trends in key legislative and regulatory initiatives over the past four years. A comparative section at the end of the paper puts these initial findings into perspective and identifies areas for future research.

Research Questions

This paper aims to provide an overview of different approaches to cyber-security policy. To narrow down the wide research area of cyber-security policy, the research underlying the paper focuses on four key research questions:

1. What is the general background that shapes each jurisdiction's approach to cyber policy?
2. What are the national priorities for developing cyber-resilience measures for critical national infrastructure (CNI)?

3. How do the jurisdictions advance skills development and/or workforce regulation in the cyber context?
4. How do these jurisdictions approach international cooperation on cyber regulation and how do they engage with other countries and entities, for example, in the context of norm-developing frameworks?

Methodology and Scope

The research underlying this publication was primarily based on a review of existing literature. This involved the creation of search strings that were inputted into online repositories to identify sources. Google Scholar was the primary search engine used to find academic articles. Grey literature, including policy papers, was sourced through Bing and Google Search. From these initial sources, the research team identified further literature by examining article bibliographies and other references. Alongside these secondary sources, primary sources such as legislation, regulations and other official documents and government papers were also considered.

The research was conducted from December 2022 to March 2023. Analysis of the gathered sourced material was based on a thematic approach, assessing sources' provenance, arguments and conclusions in order to identify different approaches to cyber regulation in the EU and the five countries examined. The six jurisdictions studied – the UK, the EU, the US, Canada, Japan and Singapore – were chosen because they drive policymaking in cyber security and are leaders in the field, either as norm developers or because of their technology sectors. The research focused primarily on policies enacted or proposed between 2019 and 2023.

Throughout this paper, the term 'policy' is used in a broad sense and encompasses binding ('hard law') as well as non-binding ('soft law') instruments or other policies.

Limitations

This paper aims to provide policymakers with a guide on trends in recent cyber-security policy in various jurisdictions. It is therefore limited in scope and depth and serves as a starting point for future research. This means that reference can only be made to a selection of policies, regulations, or legislative activities, rather than listing them all. Nevertheless, the paper informs the reader about key issues and trends in the field, while keeping the level of detail appropriate for an initial overview.

Structure

The paper comprises six chapters, each dedicated to the approach to cyber-security regulation taken by one of the jurisdictions. Each chapter begins by setting out the jurisdiction's approach to cyber policy, regulation and legislation, structured around the four research questions listed above. After setting out the general context in which the approach to cyber-security policy must be seen, each chapter goes on to identify how the jurisdiction

advances cyber-resilience measures for CNI. Then, each chapter examines how the jurisdiction approaches skills development and workforce regulation, before analysing the approach to international cooperation on cyber-norm development. After the individual chapters, the paper offers some general concluding remarks that make initial comparative observations based on the jurisdiction-level analysis, and points out further areas of research.

The UK

Context

THE UK IS 'a highly capable cyber state'[1] that follows an ambitious approach to cyber policy. This is reflected in its 2022 National Cyber Strategy,[2] which advances a 'whole of society approach'. Although largely in line with its 2016 Strategy, which shifted UK cyber policy toward binding regulation, the UK's new strategy stresses a greater need for a holistic approach to cyber policy, as cyber issues relate to all areas of modern life. The 'whole of society' approach, as advanced in the UK cyber strategy, includes public–private partnerships and civil society, but also aspects such as 'education strategy, industrial policy, work on regulations and incentives, and foreign policy'.[3]

This new holistic approach also confirms the UK's commitment to being a 'cyber power', a term used throughout the strategy, solidifying the UK's strategic approach to cyberspace. It refers to the UK's position advanced in the 2021 Integrated Review, which stresses the importance of responsible and democratic cyber power to achieving the UK's national goals.[4] On the whole, the UK's strategy follows a 'strategic and wide-ranging approach to cyber'.[5] Next to the national cyber strategy, the UK also has a Government Cyber Security Strategy (2022–30)[6] and a cyber-resilience strategy for the UK National Health Service (NHS).[7]

The UK's strong position in the cyber field is supported by a wide range of public authorities working on cyber matters. The National Cyber Security Centre (NCSC) stands out for conducting

1. International Institute for Strategic Studies (IISS), 'Cyber Capabilities and National Power: A Net Assessment', June 2021, p. 29.
2. Cabinet Office, 'UK National Cyber Strategy 2022', December 2021, <https://www.gov.uk/government/publications/national-cyber-strategy-2022>, accessed 27 March 2023.
3. Conrad Prince, 'The UK Government's New Cyber Strategy: A Whole of Society Response', *RUSI Commentary*, 15 December 2021.
4. HM Government, *Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy* (London: The Stationery Office, 2021), p. 40ff. The Integrated Review was refreshed in March 2023: see HM Government, *Integrated Review Refresh 2023: Responding to a More Contested and Volatile World* (London: The Stationery Office, 2023).
5. Prince, 'The UK Government's New Cyber Strategy'.
6. HM Government, 'Government Cyber Security Strategy, 2022–2030: Building a Cyber Resilient Public Sector', <https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030>, accessed 27 March 2023.
7. Claudia Clover, 'UK Government Releases "Urgently Needed" Cyber Resilience Strategy for the NHS', *TechMonitor*, 22 March 2023, <https://techmonitor.ai/technology/cybersecurity/nhs-cybersecurity-strategy-uk-government>, accessed 27 March 2023.

central – primarily technical – work on UK cyber security since its establishment in 2016, analysing and researching key cyber threats and risks.[8] In 2020, the UK also confirmed the existence of its National Cyber Force, a unique body dedicated to offensive cyber operations. This agency sits between the intelligence agency GCHQ and the Ministry of Defence and 'covers the full range of the UK's national-security priorities', including serious crime, terrorism and state threats.[9] In 2023, the Department of Science, Innovation and Technology was formed, taking over tasks on cyber policy previously undertaken by the Department for Digital, Culture, Media and Sport (DCMS). Of primary relevance for the UK workforce is the UK Cyber Security Council, a self-regulatory body developing and promoting professional standards for the cyber workforce.

The wide range of threats facing the UK was underlined in the NCSC's 2022 Annual Review. These include ransomware attacks and other types of cybercrime, threats posed by state actors in cyberspace, and commercially available cyber tools.[10] The UK also faces a significant gap in the cyber-security workforce, which increased further in 2022.[11] The UK cyber strategy recognises this gap and signals an intention to expand the UK's cyber skills and train, attract and diversify a growing cyber-security workforce.[12]

Priorities for National Cyber-Resilience Measures for CNI

One of the priorities set out in the UK National Cyber Strategy is increasing the UK's resilience.[13] Confirming its whole-of-society approach, efforts to increase cyber resilience include (but are not limited to) improving the resilience of CNI. The UK government currently identifies 13 sectors as CNI, including civil nuclear, chemicals, food and health – education is not among the sectors listed. Given that a large percentage of UK CNI is owned by the private sector, close cooperation between the public and private sectors is required. The NCSC fosters such cooperation and provides a number of tools for guidance and advice for CNI businesses.[14] It has also set up the 'Industry 100' initiative for further cooperation with industry partners.[15] Furthermore, the 2023 Refresh of the UK's Integrated Review announced a National Protective Security Authority, which 'will engage with businesses and institutions to protect [the UK's] security and prosperity at home'.[16]

8. IISS, 'Cyber Capabilities and National Power', p. 34.
9. *Ibid*., pp. 30–31.
10. NCSC, 'Annual Review 2022', p. 8, <https://www.ncsc.gov.uk/collection/annual-review-2022>, accessed 27 March 2023.
11. (ISC)², 'Cybersecurity Workforce Study 2022: A Critical Need for Cybersecurity Professionals Persists Amidst a Year of Cultural and Workplace Evolution', p. 8.
12. Cabinet Office, 'UK National Cyber Strategy 2022', p. 54f.
13. *Ibid*., p. 65ff.
14. NCSC, 'Advice & Guidance' and 'Cyber Assessment Framework', <https://www.ncsc.gov.uk/section/advice-guidance/all-topics>, accessed 27 March 2023.
15. NCSC, 'Industry 100', <https://www.ncsc.gov.uk/section/industry-100/about%20>, accessed 27 March 2023.
16. HM Government, *Integrated Review Refresh 2023*, p. 4.

On the regulatory side, the UK has confirmed it will update its 2018 Security of Network & Information Systems Regulations (NIS Regulations).[17] Results of the consultation process on the proposal for the updated NIS Regulations were published in November 2022, stating that the government aims to update this legislation 'as soon as parliamentary time allows'.[18] Given the updated EU regulations on NIS, such an update comes as no surprise, but could potentially mark one of the first areas of divergence post-Brexit.[19] Businesses and their cyber-security staff operating in the EU and the UK which fall under the scope of both regulations will have to comply with two changing – but not necessarily identical – sets of requirements.[20]

One of the UK's priorities for the updated NIS Regulations is to broaden the scope of their application, to include more businesses that will have to comply with the respective binding obligations, technology providers in particular.[21] The regulations' two-tier system, which imposes stricter requirements on essential service providers than on digital service providers, will remain.[22] However, and arguably '[l]ong overlooked by the UK's NIS Regulations',[23] managed service providers will be added as a new category of digital service providers that must comply with the regulations' requirements. Although software companies are unlikely to be included, the illustrative list published by DCMS names IT outsourcing services, application management services, managed security operations centres and incident response services as managed IT services that will fall within the new scope of the NIS Regulations.[24] As a result, these entities' cyber workforces must comply with the new cyber-security obligations in the updated NIS Regulations. Furthermore, the updated regulations aim to improve the reporting of cyber

17. Herbert Smith Freehills, 'Building Cyber Security Resilience: NIS 2 Enters into Force', 30 January 2023, <https://hsfnotes.com/cybersecurity/2023/01/30/building-cyber-security-resilience-nis-2-enters-into-force/?utm_source=mondaq&utm_medium=syndication&utm_term=Technology&utm_content=articleoriginal&utm_campaign=article>, accessed 27 March 2023.
18. DCMS, 'Consultation Outcome: Government Response to the Call for Views on Proposals to Improve the UK's Cyber Resilience', 30 November 2022, <https://www.gov.uk/government/consultations/proposal-for-legislation-to-improve-the-uks-cyber-resilience/outcome/government-response-to-the-call-for-views-on-proposals-to-improve-the-uks-cyber-resilience>, accessed 27 March 2023.
19. Laura Gillespie, 'Regulatory Reform will Shape 2023 Cyber Risk Landscape', Pinsent Masons, 25 January 2023, <https://www.pinsentmasons.com/out-law/analysis/regulatory-reform-shape-2023-cyber-risk-landscape>, accessed 27 March 2023.
20. Tim Wright, 'Managed Service Providers are Falling Under New Regulatory Scrutiny', *TechMonitor*, 30 January 2023.
21. Stuart Davey, 'NIS: UK Cyber Reforms to Impact Tech Providers', Pinsent Masons, 8 December 2022, <https://www.pinsentmasons.com/out-law/news/nis-uk-cyber-reforms-impact-tech-providers>, accessed 27 March 2023.
22. Wright, 'Managed Service Providers are Falling Under New Regulatory Scrutiny'.
23. *Ibid*.
24. Davey, 'NIS: UK Cyber Reforms to Impact Tech Providers'.

incidents to regulators, likely expanding mandatory reporting to incidents 'even if they don't immediately cause disruption'.[25]

Beyond CNI – and mirroring the EU's proposal for a Cyber Resilience Act – the UK also passed the Product Security and Telecommunications Infrastructure Act in December 2022. This entails obligations for companies that manufacture, import or distribute smart consumer products, further enhancing cyber resilience in the UK; however, these obligations have not yet come into force, as they require additional regulation.[26] Such obligations may build upon the Code of Practice for Consumer IoT Security that the DCMS and NCSC developed in 2018.[27] In addition, the UK government is advancing a Data Protection and Digital Information Bill, seeking to update the data protection laws previously based on the EU's General Data Protection Regulation, and to reduce paperwork for businesses.[28]

Workforce and Skills Development and Regulation

In order to implement the regulatory updates outlined above and to enhance cyber resilience, the UK's National Cyber Strategy recognises a need for developing a more 'diverse and technically skilled workforce'.[29] Improving diversity, in this context, goes beyond targeting the gender imbalance in the field, but also includes the need for greater regional diversity.[30] London and the southeast of England employ nearly half of all UK cyber-security professionals.[31] In response to this imbalance, the UK government has funded 12 'cyber clusters'. Located throughout all four home nations, these organisations are tasked with enhancing cooperation with the (local) private sector and civil society, but also with various public stakeholders.[32]

25. DCMS, 'Cyber Laws Updated to Boost UK's Resilience Against Online Attacks', press release, 30 November 2022, <https://www.gov.uk/government/news/cyber-laws-updated-to-boost-uks-resilience-against-online-attacks>, accessed 27 March 2023.
26. Franz Konig and Stuart Hunt, 'Royal Assent for the PSTI Act: Security and Resilience of Connected Consumer Products in the UK and EU', DAC Beachcroft, 15 December 2022, <https://www.dacbeachcroft.com/en/gb/articles/2022/december/royal-assent-for-the-psti-act-security-and-resilience-of-connected-consumer-products-in-the-uk-and-eu/>, accessed 27 March 2023.
27. DCMS, 'Code of Practice for Consumer IoT Security', October 2018, <https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security>, accessed 27 March 2023.
28. Department for Science, Innovation and Technology, 'British Businesses to Save Billions Under New UK Version of GDPR', press release, 8 March 2023, <https://www.gov.uk/government/news/british-businesses-to-save-billions-under-new-uk-version-of-gdpr>, accessed 27 March 2023.
29. Cabinet Office, 'UK National Cyber Strategy 2022', Part 2, Pillar 1.
30. Sam Forsdick, 'Can the New National Cyber Strategy Make the UK a Security Leader?', *Raconteur*, 12 May 2022.
31. DCMS, 'Cyber Security Sectoral Analysis 2022', 18 February 2022, <https://www.gov.uk/government/publications/cyber-security-sectoral-analysis-2022/cyber-security-sectoral-analysis-2022>, accessed 27 March 2023.
32. UK Cyber Cluster Collaboration (UKC3), <https://ukc3.co.uk/>, accessed 27 March 2023.

Other government-backed initiatives for skills development include CyBOK (a programme setting up a body for collecting knowledge and making resources to develop cyber skills publicly available).[33] Further initiatives under the NCSC's CyberFirst programme for students include 'Cyber Explorers', a learning platform for young students,[34] and the CyberFirst bursary scheme, offering undergraduate students £4,000 per year in financial assistance and cyber-security training to support their careers in cyber security.[35] The UK Cyber Security Council has further established a cyber career framework, identifying 16 areas of specialism that provide practitioners with guidelines for career planning.[36] In addition, the UK Cyber Security Council has taken over the (formerly NCSC-run) Certified Cyber Professional Scheme. The Council has also launched a pilot professional registration scheme for some of the 16 specialisms in cyber security at three registration titles: Associate; Principal; and Chartered. This pilot scheme will be extended to more specialisms throughout 2023.[37] Such pilot projects can be seen as indicative of future developments in the professionalisation of the UK's cyber workforce. This is also in line with a DCMS consultation on the professionalisation of the cyber workforce, which envisages professional standard-setting by 2025.[38]

Nevertheless, the UK arguably still faces a significant shortage in the cyber-security workforce, and a cyber-security skills gap,[39] despite the fact that the government has launched a wide variety of initiatives.[40] A similar assessment is made in a DCMS study, 'Cybersecurity Skills in the UK Labour Market 2022', which found that many organisations lack skills in areas such as setting up configured firewalls or detecting and removing malware.[41] Other skills-development paths such as apprenticeships or skills transfers in later career stages could be better utilised to

33. CyBOK has so far identified 21 'knowledge areas' for cyber skills. See CyBOK, 'The Cyber Security Body of Knowledge', Version 1.1.0, 31 July 2021, <https://www.cybok.org/media/downloads/CyBOK_v1.1.0.pdf>, accessed 27 March 2023.
34. Cyber Explorers, <https://www.cyberexplorers.co.uk/>, accessed 27 March 2023.
35. NCSC, 'Bursary and Degree Apprenticeship', <https://www.ncsc.gov.uk/cyberfirst/bursary-and-degree-apprenticeship>, accessed 27 March 2023.
36. UK Cyber Security Council, 'Cyber Career Framework', <https://www.ukcybersecuritycouncil.org.uk/careers-and-learning/cyber-career-framework/>, accessed 27 March 2023.
37. UK Cyber Security Council, 'The Route to Chartership for the UK's Cyber Professionals', <https://www.ukcybersecuritycouncil.org.uk/professional-standards/the-council-s-route-to-chartership/>, accessed 27 March 2023.
38. DCMS, 'Consultation Outcome: Embedding Standards and Pathways Across the Cyber Profession by 2025', 20 June 2022, <https://www.gov.uk/government/consultations/embedding-standards-and-pathways-across-the-cyber-profession-by-2025/embedding-standards-and-pathways-across-the-cyber-profession-by-2025#executive-summary>, accessed 27 March 2023.
39. (ISC)², 'Cybersecurity Workforce Study 2022', p. 8.
40. Afiq Fitri, 'UK Cybersecurity Skills Gap Remains as Government Schemes Prove Ineffective', *TechMonitor*, 4 May 2022.
41. Gabriele Zatterin et al., 'Cyber Security Skills in the UK Labour Market 2022: Findings Report', DCMS and Ipsos, 3 May 2022, <https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2022>, accessed 27 March 2023.

try to close the gap even more.[42] Further research is thus necessary to better understand the effectiveness of existing initiatives for skills development.

International Interaction on Cyber-Norm Development

As well as advancing cyber policy on a domestic level, the UK also shapes international norm development in cyberspace. A 2022 ministerial document describes the UK as a 'leading responsible and democratic cyber power'.[43] The UK delivers on such ambitions by being actively involved in the UN norm-development processes, arguing in favour of norms of responsible cyber behaviour[44] and the applicability of international law in cyberspace.[45] The UK has also repeatedly argued in favour of a multi-stakeholder approach to cyberspace governance.[46] Furthermore, the UK government emphasises the need for a stable, peaceful and secure cyberspace that maintains human-rights standards.[47]

The UK's international cooperation on cyber-norm development is primarily advanced through the Foreign, Commonwealth and Development Office (FCDO), which funds a number of initiatives for greater norm cooperation in cyberspace; this includes, for example, funding projects identifying responsible cyber behaviour.[48] In addition, the UK actively supports and funds cyber capacity-building in cooperation with a range of jurisdictions, particularly Commonwealth countries. In 2021, an additional £22 million for cyber capacity-building in Africa and the Indo-Pacific was announced.[49]

---

42. Business, Energy and Industrial Strategy Committee, House of Commons Select Committee, 'UK Labour Market Inquiry, (ISC)2 Submission', <https://committees.parliament.uk/writtenevidence/109869/html/>, accessed 27 March 2023.
43. Sam Donaldson et al., 'UK Cyber Security Sectoral Analysis 2022: Research Report for the Department of Digital, Culture, Media and Sport', DCMS et al., February 2022, p. 1, <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1055565/Cyber_Sectoral_Analysis_2022_Report_V2.1.pdf>, accessed 31 March 2023.
44. Australian Strategic Policy Institute, 'The UN Norms of Responsible State Behaviour in Cyberspace', 22 March 2022, <https://www.aspi.org.au/report/un-norms-responsible-state-behaviour-cyberspace>, accessed 27 March 2023.
45. FCDO, 'Application of International Law to States' Conduct In Cyberspace: UK Statement', 3 June 2021, <https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement>, accessed 27 March 2023.
46. Cabinet Office, 'UK National Cyber Strategy 2022', Part 2, Pillar 4: Global Leadership.
47. *Ibid*.
48. FCDO, 'Responsible Cyber Behaviour Call for Bids: Further Guidance', 8 September 2022, <https://www.gov.uk/government/publications/national-cyber-programme-international-responsible-cyber-behaviour-call-for-bids/responsible-cyber-behaviour-call-for-bids-further-guidance>, accessed 27 March 2023.
49. FCDO, 'UK Pledges £22 Million to Support Cyber Capacity Building in Vulnerable Countries', press release, 12 May 2021, <https://www.gov.uk/government/news/uk-pledges-22m-to-support-cyber-capacity-building-in-vulnerable-countries>, accessed 27 March 2023.

More recently, the UK has cooperated with its allies with respect to sanctioning cyber-criminals,[50] as well as with attributing malicious cyber operations to state actors.[51] Finally, the UK has concluded a large number of bilateral agreements with other jurisdictions, setting out areas of cooperation in the cyber domain, including the US, the Netherlands,[52] Australia[53] and Italy.[54]

50. National Crime Agency, 'Ransomware Criminals Sanctioned in Joint UK/US Crackdown on International Cyber Crime', 9 February 2023, <https://www.nationalcrimeagency.gov.uk/news/ransomware-criminals-sanctioned-in-joint-uk-us-crackdown-on-international-cyber-crime>, accessed 27 March 2023.
51. Connor Jones, 'Five Eyes and US Governments Finally Confirm Russia was Behind Ukrainian Government, Viasat Cyber Attacks', *IT Pro*, 10 May 2022.
52. Government of the Netherlands, 'Joint Statement on the UK–NL Cyber Dialogue', 18 March 2022, <https://www.government.nl/documents/diplomatic-statements/2022/03/18/joint-statement-uk-nl-cyber-dialogue>, accessed 27 March 2023.
53. Australian Government, 'Australia–UK Cyber and Critical Technology Partnership Principals Meeting Joint Statement', 7 December 2022, <https://www.internationalcybertech.gov.au/Australia-UK-CCTP-Principals-Meeting>, accessed 27 March 2023.
54. UK Ministry of Defence, 'UK and Italy Agree to Deepen Cooperation in Space and Cyber Domains', press release, 9 February 2023, <https://www.gov.uk/government/news/uk-and-italy-agree-to-deepen-cooperation-in-space-and-cyber-domains>, accessed 27 March 2023.

The EU

Context

THE EU IS a well-established player in the field of cyber policy and actively shapes Europe's approach to the regulation of cyber security. Economically powerful, the EU has also proven to be highly influential on cyber-security matters, and not just when it comes to data protection. The EU implements its vision for a free and secure cyberspace through a combination of different instruments, binding regulations, standard-setting directives and influential policies (including cyber diplomacy). Whereas the EU cyber-security policy in the 2010s was still largely seen as fragmented or 'unsystematic',[55] many of the more recent efforts are working towards greater horizontal integration and harmonisation among EU member states.[56] Four key activities have stood out in the past few years.

Firstly, the EU updated its cyber-security strategy in 2020 to mark the new digital decade.[57] The updated strategy prioritises greater cyber resilience, especially for critical infrastructure, as well as increased cooperation and EU leadership on international norms and standards development. Activities in both areas are addressed in greater detail below.

Secondly, the role of the European Union Agency for Cybersecurity, ENISA, has been strengthened by the 2019 Cybersecurity Act,[58] giving the body a permanent mandate, as well as more tasks

55. Agnes Kasper, 'EU Cybersecurity Governance: Stakeholders and Normative Intentions towards Integration', in Mark Harwood, Stefano Moncada and Roderick Pace (eds), *The Future of the European Union: Demisting the Debate* (Institute for European Studies, University of Malta, 2020), pp. 166–85.
56. For example, by working towards establishing a common cyber-security framework. See 'EU Moves to Establish a Common Cybersecurity Framework', *European Security & Defence*, 28 November 2022, <https://euro-sd.com/2022/11/news/28451/eu-moves-to-establish-a-common-cybersecurity-framework/>, accessed 27 March 2023.
57. European Commission, 'EU Cyber Security Strategy for the Digital Decade', 16 December 2020, <https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0>, accessed 27 March 2023.
58. EUR-Lex, 'Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act)', <https://eur-lex.europa.eu/eli/reg/2019/881/oj>, accessed 27 March 2023.

and resources. The EU Cybersecurity Act introduces an EU-wide cyber-security certification framework for ICT products, services and processes.[59]

Thirdly, the European Commission and the European External Action Service set out the EU's new cyber defence policy in November 2022, which is 'intended to strengthen European Cybersecurity capacity, boost military and civilian cooperation, close potential loopholes, reduce strategic dependencies and develop cyber skills'.[60] This policy is primarily a response to deteriorating relations with Russia, and includes setting up an EU Cyber Defence Coordination Centre, as well as a network of military Computer Emergency Response Teams, an EU Cyber Commanders Conference and joint exercises.[61] Similarly, the newly proposed Cyber Solidarity Act envisages the creation of a cyber emergency fund for incident response in the event of a large-scale cyber attack.[62]

A final noteworthy development is the proposal of the EU Cyber Resilience Act.[63] The Commission's proposal from September 2022 'aims to impose cybersecurity obligations on all products with digital elements whose intended and foreseeable use includes direct or indirect data connection to a device or network'.[64] This includes cyber security by design as well as by default principles.[65] The proposal is not yet in its final form, but is said to require businesses such as hardware manufacturers or software developers (as well as distributors and importers) to comply with 'an "appropriate" level of cyber security, the prohibition [on selling] products with any known vulnerability, security by default configuration, protection from unauthorised access, limitation of attack surfaces, and minimisation of incident impact'.[66] The Cyber Resilience Act is widely seen as a shift away from the EU's sectoral approach to regulation, which imposes cyber-security regulations on specific products such as medical devices. Instead, the Cyber Resilience Act is intended to avoid both the fragmentation of market standards and duplication of obligations.[67]

59. European Commission, 'The EU Cybersecurity Act', <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act>, accessed 27 March 2023.
60. Luca Bertuzzi, 'EU Sets Out Plan for Cyber Defence Policy', *Euractiv*, 11 November 2022.
61. EU Cyber Direct, 'Countering Cyber Threats: A New EU Cyber Defence Policy', 11 November 2022, <https://eucyberdirect.eu/news/countering-cyber-threats-a-new-eu-cyber-defence-policy>, accessed 27 March 2023.
62. Luca Bertuzzi, 'What to Expect from the EU's Cyber Solidarity Act', *Euractiv*, 1 March 2023.
63. DR2 Consultants [now Publyon], 'European Cyber Resilience Act: Can New Requirements for Products Strengthen Your Organization's Cybersecurity Resilience?', 23 February 2023, <https://dr2consultants.eu/european-cyber-resilience-act/>, accessed 27 March 2023.
64. European Parliament, 'EU Cyber Resilience Act', p. 1, <https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/739259/EPRS_BRI(2022)739259_EN.pdf>, accessed 27 March 2023.
65. *Ibid*., p. 1.
66. DR2 Consultants [now Publyon], 'European Cyber Resilience Act'.
67. Pier Giorgio Chiara, 'The Cyber Resilience Act: The EU Commission's Proposal for a Horizontal Regulation on Cybersecurity for Products with Digital Elements: An Introduction', *International Cybersecurity Law Review* (3, 2022), pp. 255–72, see p. 255.

Priorities for National Cyber-Resilience Measures for CNI

The protection and resilience of CNI are also a growing priority for EU policymakers. In order to be prepared to respond to the landscape of heightened threats in the contemporary geopolitical context, the EU is currently seeking to update its directive on critical infrastructure (from 2008) and intends new legislation to be in force in 2024.[68]

This new legislation will be complemented by existing directives, primarily the Directive on Resilience of Critical Infrastructure and the Revised Directive on Security of Network and Information Systems (NIS 2 Directive). The former was proposed by the Commission in 2020 to strengthen the resilience of critical entities that provide essential services in case of disruption, e.g., terrorist or other attacks. Member states are required to have a strategy for such events and to 'carry out risk assessments'.[69]

Updated in 2022, the NIS 2 Directive complements the Directive on Resilience of Critical Infrastructure by obliging the same CNI entities to follow cyber-resilience obligations. It has further expanded in scope and 'now covers medium and large entities from more sectors that are critical for the economy and society'.[70] The updated NIS 2 Directive imposes strengthened cyber-security requirements on companies, covers the security of supply chains and further 'introduces accountability of top management for non-compliance with the cybersecurity obligations' alongside stricter enforcement requirements, alignment of reporting obligations and supervisory measures for national authorities.[71] The NIS 2 Directive came into force in January 2023, giving member states until October 2024 to incorporate the measures into national law.[72] However, there can still be national differences in implementation, and businesses and cyber-security professionals may have to comply with varying obligations, depending on the country in which they operate.

The obligations set out under the NIS 2 Directive, the Cyber Resilience Act and the Cyber Security Act increase cyber-security obligations and expand their application to a growing number of sectors and organisations. These obligations underline the need for cyber-security expertise and further require that businesses comply with new policies; this is likely to increase demand

68. Alexandra Brzozowski and Kira Taylor, 'EU Vows to Draw Up Plans to Protect Critical Infrastructure', *Euractiv*, 5 October 2022.
69. European Commission, 'The Commission Proposes a New Directive to Enhance the Resilience of Critical Entities Providing Essential Services in the EU', 16 December 2020, <https://home-affairs.ec.europa.eu/news/commission-proposes-new-directive-enhance-resilience-critical-entities-providing-essential-services-2020-12-16_en>, accessed 27 March 2023.
70. European Commission, 'Commission Welcomes Political Agreement on New Rules on Cybersecurity of Network and Information Systems', 13 May 2022, <https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2985>, accessed 27 March 2023.
71. *Ibid*.
72. European Commission, 'Cybersecurity Policies', <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies>, accessed 27 March 2023.

for more cyber professionals and more cyber expertise in related fields, e.g., in procurement or project management.

Workforce and Skills Development and Regulation

To implement the increased obligations for cyber resilience set out in new and updated regulations, cyber-skills development is necessary, and the cyber workforce needs to be able to comply with these new measures. The lack of cyber-security skills in the European workforce has frequently been addressed in the literature.[73] Not only is there a significant skills gap, which some studies find to be growing, but it is also increasingly difficult for companies to find and hire skilled cyber-security staff.[74] Studies imply that the cyber-security labour market has been unable to match the steep rise in cybercrime and the high demand for cyber-security professionals in light of increasing digitalisation.[75] Although skills and workforce development are dealt with by each individual member state, the EU is also responding to these issues, and has funded a wide range of initiatives in this sphere, particularly in terms of harmonising existing approaches.

In 2019, the European Commission launched four projects for cyber-security research, alongside training and education programmes, but their funding is now coming to an end.[76] They were launched in preparation for the European Cybersecurity Competence Centre (ECCC), which is currently being developed. The ECCC will be located in Bucharest and will, together with national competence centres, develop 'a common agenda for technology development', including in businesses, especially SMEs.[77] Furthermore, the European Commission has plans to set up a Cybersecurity Skills Academy[78] with a potential launch date in the third quarter of 2023.[79] This

73. See, for example, Borka Jerman Blažič, 'Changing the Landscape of Cybersecurity Education in the EU: Will the New Approach Produce the Required Cybersecurity Skills?', *Education and Information Technologies* (27, 2022), p. 3,011.
74. Joe Pettit, 'The Experts' Guide on Tackling the Cybersecurity Skills Gap', TripWire, 11 March 2020, <https://www.tripwire.com/state-of-security/expert-guide-tackling-cybersecurity-skills-gap>, accessed 27 March 2023.
75. Blažič, 'Changing the Landscape of Cybersecurity Education in the EU', p. 3,013.
76. See for example European Commission, 'European Network of Cybersecurity Centres and Competence Hub for Innovation and Operations', <https://cordis.europa.eu/project/id/830943>, accessed 11 April 2023. Ended February 2023.
77. European Cybersecurity Competence Centre, <https://cybersecurity-centre.europa.eu/about-us_en>, accessed 27 March 2023.
78. Anna Ribeiro, 'EU Cybersecurity Skills Framework Works Towards Commonalities of Roles, Competencies, Skills, Knowledge', *Industrial Cyber*, 22 September 2022, <https://industrialcyber.co/training-development/eu-cybersecurity-skills-framework-works-towards-commonalities-of-roles-competencies-skills-knowledge/>, accessed 27 March 2023.
79. Luca Bertuzzi, 'Leak: A Sneak Peek at the EU's Digital Agenda for 2023', *Euractiv*, 14 October 2022.

year, 2023, is also the European Year of Skills, prompting further initiatives to address the skills shortages among the EU workforce, including in cyber security.[80]

In line with the EU's other efforts to streamline its cyber-security policy, ENISA introduced the European Cybersecurity Skills Framework (ECSF) in September 2022. As a 'tool to build a common understanding of the cybersecurity professional role profiles', the ECSF sets out 12 roles and their respective skills and responsibilities, for example, those of 'cyber incident responder', or 'cybersecurity educator'.[81] However, previous studies have indicated the need for further research on what policies are most effective in supporting a robust talent pipeline for cyber-security professionals.[82] Alongside this Framework, ENISA has also created a Cybersecurity Higher Education Database, which lists cyber-security degrees from EEA countries and Switzerland. The database is intended as a point of reference for citizens wanting to upgrade their skills through further education and training.[83]

International Interaction on Cyber-Norm Development

In addition to its work on the close coordination of cyber policy within the EU, the EU is also active beyond the territory of its member states. The EU's 2020 Cyber Strategy sets out to ensure an open and safe internet and for the EU to 'step up its cooperation with partners around the world who share [its] values of democracy, rule of law and human rights'.[84] The EU has done much to act upon these aims, with some even referring to it as a 'norm superpower'.[85] Indeed, the EU's track record points towards the active role it has played in shaping the cyber-norm debate. On an international level, the EU has supported the UN processes on norm development, and also

80. European Commission, 'European Year of Skills 2023', <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-year-skills-2023_en#:~:text=The%20European%20Year%20of%20Skills%202023%20will%20help,new%20opportunities%20for%20people%20and%20the%20EU%20economy>, accessed 27 March 2023.
81. ENISA, 'European Cybersecurity Skills Framework (ECSF)', <https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework>; ENISA, 'European Cybersecurity Skills Framework Role Profiles', <https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles>, accessed 27 March 2023.
82. Tommaso De Zan and Fabio Di Franco, *Cybersecurity Skills Development in the EU: The Certification of Cybersecurity Degrees and ENISA's Higher Education Database* (Athens and Heraklion: ENISA, 2019), p. 4, <https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union>, accessed 27 March 2023.
83. *Ibid*., p. 3.
84. European Commission, 'The Cybersecurity Strategy', <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy>, accessed 27 March 2023.
85. Centre for European Policy Studies, 'Cybersecurity', <https://www.ceps.eu/cybersecurity-ceps/>; Nikola Schmidt et al., 'The EU as a Leader of Global Cyber Security Policy', Institute of International Relations, Prague, Policy Paper, 28 April 2022, p. 4, <https://www.iir.cz/the-eu-as-a-leader-of-global-cyber-security-policy>, accessed 27 March 2023.

supports the proposal for a Programme of Action to Advance Responsible State Behaviour in Cyberspace as a permanent mechanism within the UN.[86]

Furthermore, the EU actively cooperates with other countries to strengthen their cyber security. This includes funding cyber-security measures in Eastern European countries such as Ukraine (e.g., to secure data exchanges or to protect critical infrastructure),[87] as well as in Georgia.[88] Together with the US, the EU plans to provide further cyber-capacity-building in Africa and the Indo-Pacific region.[89] The EU has also funded EU CyberNet, a network of cyber-security experts and academics, to coordinate the EU's external cyber-capacity-building projects (although this is coming to an end in 2023),[90] as well as EU Cyber Direct, a think tank- and academia-led initiative in support of the EU's cyber diplomacy, focusing on norm development and capacity-building programmes.[91]

In May 2019, the European Council launched a sanctions regime which enables the EU to respond to (and deter) cyber attacks. This sanctions regime, which enables collective action by the EU and its member states, is part of the 'EU Cyber Diplomacy Toolbox', and it has since been extended until 2025.[92] Potential measures include asset freezing and travel restrictions. Since its first use in 2020,[93] the sanctions regime has been used on several subsequent occasions, for example, against the hackers who targeted the German Bundestag[94] and those behind (inter

86. European External Action Service, 'EU Statement – UN General Assembly 1st Committee: Cybersecurity', 25 October 2022, <https://www.eeas.europa.eu/delegations/un-new-york/eu-statement-%E2%80%93-un-general-assembly-1st-committee-cybersecurity_en?s=63>, accessed 27 March 2023.
87. EU4Digital, 'EU Supports Cybersecurity in Ukraine with Over €10 Million', 21 October 2022, <https://eufordigital.eu/eu-supports-cybersecurity-in-ukraine-with-over-e10-million/>, accessed 27 March 2023.
88. The European Union for Georgia, 'Strengthening Cybersecurity Capacities in Georgia', <https://eu4georgia.eu/projects/eu-project-page/?id=1458>, accessed 27 March 2023.
89. Matthew Gooding, 'US and EU Could Fund Cybersecurity Improvements in Developing Countries', *TechMonitor*, 15 June 2022.
90. EU CyberNet, <https://www.eucybernet.eu/vision/>, accessed 27 March 2023.
91. EU Cyber Direct, <https://eucyberdirect.eu/>, accessed 27 March 2023.
92. EU Cyber Direct, 'Sanctions Regime Against Cyber Attacks Extended until 2025', 16 May 2022, <https://eucyberdirect.eu/news/sanctions-regime-against-cyber-attacks-extended-until-2025>, accessed 27 March 2023.
93. European Union External Action Service, 'EU Imposes First Ever Cyber Sanctions to Protect Itself From Cyber-Attacks', 30 July 2020, <https://www.eeas.europa.eu/eeas/eu-imposes-first-ever-cyber-sanctions-protect-itself-cyber-attacks_en>, accessed 27 March 2023.
94. Simmons + Simmons, 'The European Fight Against Cybercriminals: "Cyber Sanctions"', 6 November 2020, <https://www.simmons-simmons.com/en/publications/ckh6ccivq1229095252uglboa/the-european-fight-against-cybercriminals-cyber-sanctions->, accessed 27 March 2023.

alia) WannaCry and NotPetya.[95] However, the attribution of cyber operations remains 'a major challenge for EU cyber sanctions'.[96]

95. Sasha Erskine, 'The EU Tiptoes into Cyber Sanctions Regimes', *RUSI Commentary*, 12 October 2020.
96. Annegret Bendiek and Matthias Schulze, 'Attribution: A Major Challenge for EU Cyber Sanctions', SWP Research Paper, December 2021, <https://www.swp-berlin.org/publications/products/research_papers/2021RP11_EU_CyberSanctions.pdf>, accessed 27 March 2023.

The US

Context

THE US HAS a strong record of advancing cyber-security policies that support an open, stable and secure cyberspace, and the country's large private sector makes it a particularly powerful actor in the field. In March 2023, the Biden administration published a new National Cybersecurity Strategy,[97] which is based on five key pillars:

- The defence of critical infrastructure.
- Disruption and dismantling of threat actors.
- Shaping market forces to drive security and resilience.
- Investing in a resilient future (including through workforce development).
- Forging international partnerships to pursue shared goals.

These key pillars will be referenced throughout this section.

The new cyber-security strategy marks a change in the US approach to cyber policy, in so far as it aims to increase regulatory oversight and paves the way for further federal cyber-security regulation. By advancing an increasingly coordinated approach to cyber-security regulation, the strategy seeks to impose further binding obligations on the private sector, meaning that hardware and software vendors will be increasingly responsible for implementing cyber-security standards.[98] If implemented into law, the new strategy proposes that technology companies may be liable for failing to implement these standards.[99] This new cyber-security strategy is, however, in line with a number of recent US cyber policies, for example, the regulations on cyber security for oil and gas pipelines that were introduced after the 2021 Colonial Pipeline hack.[100] Similarly, President Biden has increased binding obligations on businesses when introducing mandatory reporting for CNI operators experiencing a significant cyber attack (such as a

97. The White House, 'National Cybersecurity Strategy', March 2023, <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>, accessed 27 March 2023.
98. Glenn Gerstell, 'Biden's New Cyber Strategy Will Acknowledge an Essential Truth: Market Forces Aren't Enough', *Barron's*, 6 February 2023, <https://www.barrons.com/articles/biden-new-cyber-strategy-market-forces-cybersecurity-51675459082>, accessed 27 March 2023.
99. The White House, 'National Cybersecurity Strategy', p. 4ff; David E. Sanger, 'New Biden Cybersecurity Strategy Assigns Responsibility to Tech Firms', *New York Times*, 2 March 2023. For commentary see also Trey Herr et al., 'Building from the 2023 National Cybersecurity Strategy: Reshaping the Terrain of Cyberspace', *Lawfare*, 13 March 2023.
100. Ellen Nakashima and Tim Starks, 'U.S. National Cyber Strategy to Stress Biden Push on Regulation', *Washington Post*, 5 January 2023.

ransomware attack).[101] The new cyber-security strategy is the result of increased cooperation with the private sector, and this cooperation will remain a key component going forward.[102]

The new cyber-security strategy also intends to streamline US policy and to coordinate regulatory efforts. Previously, the Biden administration has often relied upon presidential interventions (for example, Executive Order 14028[103]), but Congress has also advanced additional legislation on cyber-security issues.[104] However, Congress can challenge or subsequently legislate contrary to an Executive Order. Similarly, in terms of the new cyber strategy, one risk is that party division in Congress could limit progress on implementing the strategy's objectives.[105] As a result, some think that the 'strategy won't have any regulatory teeth itself'.[106] The following sections take a closer look at specific aspects of US cyber-security strategy.

Priorities for National Cyber-Resilience Measures for CNI

One of the main pillars of the new US cyber-security strategy relates to defending CNI.[107] In line with the broader shift towards top-down regulatory measures set out in the cyber-security strategy, a similar shift is proposed for measures protecting CNI. In light of significant threats facing the US, Anne Neuberger, deputy national security adviser for cyber and emerging technology, considers that previous '[v]oluntary efforts have been insufficient'.[108] The new strategy thus intends to enhance regulation by establishing new cyber-security requirements in 'certain critical sectors' and by requiring new authorities to set regulations in other sectors.[109] Currently, only some of the 16 critical infrastructure sectors are subject to regulation. While five sectors (nuclear power, large energy generation, chemicals, financial services and major defence contractors) were subject to regulation prior to the Biden administration taking office, the Colonial Pipeline attack led to the regulation of further sectors, i.e., oil and gas pipelines, and aviation and

101. Alex Scroxton, 'Biden Signs Ransomware Reporting Mandate into Law', *Computer Weekly*, 16 March 2022.
102. Gerstell, 'Biden's New Cyber Strategy Will Acknowledge an Essential Truth'.
103. The White House, 'Executive Order on Improving the Nation's Cybersecurity', 12 May 2021, <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>, accessed 31 March 2023.
104. Shannon Flynn, 'What is the Biden Administration 2023 National Cybersecurity Strategy?', *MakeUseOf*, 15 February 2023, <https://www.makeuseof.com/biden-2023-national-cybersecurity-strategy/>, accessed 27 March 2023.
105. Derek B. Johnson, 'Biden Admin's Push for Cyber Regulations Could Clash with Skeptical Republicans', *SC Media*, 24 February 2023, <https://www.scmagazine.com/news/critical-infrastructure/biden-cyber-regulations-clash-republicans>, accessed 27 March 2023.
106. Josh Axelrod, 'As Cyberattacks Become "So Cheap", US Vendors Prep for New Rules', *Bloomberg*, 6 February 2023.
107. The White House, 'National Cybersecurity Strategy', p. 7ff.
108. Tim Starks, 'Anne Neuberger Discusses Work to Protect Critical Infrastructure', *Washington Post*, 30 January 2023.
109. The White House, 'National Cybersecurity Strategy', p. 7ff.

railways.[110] It is expected that the Environmental Protection Agency will also issue similar regulations for the water sector, leaving five sectors which are not subject to the oversight of an authority that has the competence to launch federal cyber regulation.[111] Here, Congress could legislate to enhance further binding cyber-security standards for these sectors.

The protection of CNI is further advanced by the Cybersecurity & Infrastructure Security Agency (CISA), founded in 2018, which has recently published its first Strategic Plan (for 2023–25). It identifies four key priorities:

- Leading 'the national effort to ensure the defense and resilience of cyberspace'.
- Reducing risk to CNI, but also increasing its resilience.
- Fostering whole-of-nation operational collaboration and information-sharing.
- Taking a unified approach as '[one] CISA through integrated functions, capabilities, and workforce'.[112]

As much of the US's CNI is owned by the private sector, government cooperation with industry is particularly important. Relevant initiatives include CISA's Automated Indicator Sharing Program, an early warning system enabling information-sharing between companies and public agencies.[113]

Further cyber-security standards and best practices are also developed and shared by the National Institute for Standards and Technology (NIST), which works closely with industry stakeholders and public agencies: for example, all federal agencies must implement its cyber-security standards.[114] Although guidelines such as those developed under Executive Order 14028 on Improving the Nation's Cybersecurity (May 2021) are primarily aimed at federal agencies, they can also be implemented by the private sector.[115] One priority featured in the recent

110. Nakashima and Starks, 'U.S. National Cyber Strategy to Stress Biden Push on Regulation'.
111. *Ibid*.
112. Cybersecurity & Infrastructure Security Agency (CISA), '2023–2025 Strategic Plan', <https://www.cisa.gov/strategic-plan>, accessed 27 March 2023.
113. Cynthia Brumfield, 'What is the CISA? How the New Federal Agency Protects Critical Infrastructure from Cyber Threats', *CSO*, 1 July 2019, <https://www.csoonline.com/article/3405580/what-is-the-cisa-how-the-new-federal-agency-protects-critical-infrastructure-from-cyber-threats.html>, accessed 27 March 2023.
114. NIST, 'Cybersecurity', <https://www.nist.gov/cybersecurity>, accessed 27 March 2023.
115. NIST, 'Improving the Nation's Cybersecurity: NIST's Responsibilities Under the May 2021 Executive Order', <https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity>, accessed 27 March 2023.

work of NIST is the protection of supply chains.[116] NIST is currently working on updating its Cybersecurity Framework (CSF 2.0). Initially aimed at CNI only, this framework is now used more widely, and has been updated using private and civil sector input. A draft of the new framework is expected by summer 2023.[117]

Updated regulations and an increase in binding cyber-security obligations across an expanding number of sectors also means that companies are reliant on cyber-security professionals to implement such obligations. The cyber workforce in these areas must have the relevant skills to fulfil such tasks, both to comply with regulations and to uphold cyber security more generally.

Workforce and Skills Development and Regulation

The obligation to comply with new cyber-security standards is linked to another key pillar of the new US cyber-security strategy – the investment in greater resilience. This pillar includes the aim of strengthening the cyber workforce and envisages the development of a National Cyber Workforce and Education Strategy.[118] Currently, the gap in the US cyber-security workforce is more than 410,000.[119] A number of initiatives support efforts to fill this gap and improve skills development throughout the US; one noteworthy example of such efforts is the National Cyber Workforce and Education Summit that took place in July 2022, bringing together relevant stakeholders from the public and private sectors and from civil society. In this context, several further efforts were announced by multiple stakeholders, including a Cybersecurity Apprenticeship Sprint, which concluded in November 2022.[120] The 'sprint' underlined a commitment to grow the adoption of apprenticeships as a pathway to employment in the US cyber-security workforce.[121] The new cyber-security strategy also stresses the need for greater diversity, equity and inclusion in the cyber workforce.[122] It thereby echoes previous efforts, such as a June 2021 Executive Order on Diversity, Equity, Inclusion, and Accessibility in the

116. NIST, 'Improving Cybersecurity in Supply Chains: NIST's Public–Private Partnership', <https://www.nist.gov/cybersecurity/improving-cybersecurity-supply-chains-nists-public-private-partnership>, accessed 27 March 2023.
117. In preparation for the draft, NIST published in January 2023 a concept paper on potential changes to the framework. See NIST, 'NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework', 19 January 2023, <https://www.nist.gov/system/files/documents/2023/01/19/CSF_2.0_Concept_Paper_01-18-23.pdf>, accessed 27 March 2023.
118. The White House, 'National Cybersecurity Strategy', p. 23ff. The Department of Defense published its cyber workforce strategy in March 2023: 'DoD Cyber Workforce Strategy: 2023–2027', 1 March 2023, <https://dodcio.defense.gov/Portals/0/Documents/Library/CWF-Strategy.pdf>, accessed 27 March 2023.
119. (ISC)², 'Cybersecurity Workforce Study 2022', p. 8.
120. Stakeholders included (ISC)². See the White House, 'Fact Sheet: National Cyber Workforce and Education Summit, 21 July 2021', <https://www.whitehouse.gov/briefing-room/statements-releases/2022/07/21/fact-sheet-national-cyber-workforce-and-education-summit/>, accessed 27 March 2023.
121. The White House, 'Fact Sheet'.
122. The White House, 'National Cybersecurity Strategy', p. 27.

Federal Workforce.[123] Several initiatives aim to increase such diversity, for example an internship programme seeking increased diversity in the New York City cyber workforce.[124]

Further examples of initiatives supporting cyber-security awareness and skills development in the US are manifold. For example, the US Security and Exchange Commission has proposed new rules that require board members of publicly traded companies to disclose their cyber expertise.[125] CISA has also set up awareness campaigns to increase national public awareness and enhance levels of cyber-security understanding.[126] CISA also supports a range of online training courses[127] and has a dedicated National Initiative for Cybersecurity Careers and Studies (NICCS).[128] The CyberSkills2Work initiative (2020) enables military veterans to transition into a career in cyber security.[129] Other initiatives – primarily aimed at the younger generations – involve a range of cyber-security games and competitions.[130] Meanwhile, individuals keen on advancing their cyber-security skills can consult the Cybersecurity Workforce Training Guide,[131] which, together with the Cyber Career Pathways Tool, allows individuals to set out a training plan in line with their skill level.[132] Businesses that want to identify the extent of the cyber-security workforce within a specific area, or the costs associated with hiring additional cyber-security

123. The White House, 'Executive Order on Diversity, Equity, Inclusion, and Accessibility in the Federal Workforce', 25 June 2021, <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/25/executive-order-on-diversity-equity-inclusion-and-accessibility-in-the-federal-workforce/>, accessed 27 March 2023.
124. Jonathan Greig, 'NYC Aims to Diversify Cybersecurity Field with New Internship Program', *The Record*, 9 March 2023, <https://therecord.media/nyc-cyber-internship-program>, accessed 27 March 2023.
125. See US Securities and Exchange Commission, 'Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure', <https://www.sec.gov/rules/proposed/2022/33-11038.pdf>, accessed 27 March 2023. For a commentary see Keri Pearlson and Chris Hetner, 'Is Your Board Prepared for New Cybersecurity Regulation?', *Harvard Business Review*, 11 November 2022.
126. CISA, 'Cybersecurity Awareness Program', <https://www.cisa.gov/cisa-cybersecurity-awareness-program>, accessed 27 March 2023.
127. CISA, 'Cybersecurity Training & Exercises', <https://www.cisa.gov/cybersecurity-training-exercises>, accessed 27 March 2023.
128. NICCS, 'About NICCS', <https://niccs.cisa.gov/about-niccs>, accessed 27 March 2023.
129. CyberSkills2Work, 'The National Cybersecurity Workforce Development Program', <https://cyberskills2work.org/i/>, accessed 27 March 2023.
130. National Initiative for Cybersecurity Careers and Studies, 'Additional Resources', <https://niccs.cisa.gov/cybersecurity-career-resources/additional-resources>, accessed 27 March 2023.
131. CISA, 'Cybersecurity Workforce Training Guide', <https://www.cisa.gov/sites/default/files/publications/Cybersecurity%20Workforce%20Training%20Guide_508c.pdf?trackDocs=Cybersecurity%20Workforce%20Training%20Guide_508c.pdf>, accessed 27 March 2023.
132. NICCS, 'Cyber Career Pathways Tool', <https://niccs.cisa.gov/workforce-development/cyber-career-pathways-tool>, accessed 27 March 2023.

staff, can also consult the CyberSeek initiative, which provides information and an interactive map on job postings.[133]

But the gap in the cyber-security workforce persists, despite this wide range of initiatives on skills development, meaning that further research is required to better understand the effectiveness of these initiatives. Here, the newly proposed National Cyber Workforce and Education Strategy is intended to coordinate the US approach to developing a stronger and more diverse cyber workforce.[134]

To harmonise the terminology used to describe the tasks and skills of cyber-security professionals, the US has adopted the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. This sets out categories of common cyber-security functions, specialist areas of cyber-security work, and work roles, providing detailed descriptions of the required knowledge, skills and abilities for each role.[135] Although initially launched in 2012, the current (fourth) version includes several updates made in 2020. The NICE Framework was initially advanced as a national initiative but has since been influential in many other jurisdictions, including Canada and Japan, underlining that workforce development is a global issue. Despite the widespread influence of the Framework, recent research indicates that US employers still find that graduates of US higher education institutions lack the NICE foundation.[136] The NICE Framework continues to be updated, including through public consultation on updated Framework data such as knowledge and skills statements.[137]

International Interaction on Cyber-Norm Development

Beyond its national policies, the US is a leader in international norm development on cyber security and the regulation of cyberspace. It strongly lobbies for a free, secure and open internet, and envisages a multi-stakeholder approach to the governance of cyberspace. This is reflected in a wide range of activities and initiatives, including the US-led (but now finished) UN Governmental Group of Experts, for which it sponsored a resolution for renewal for 2019–21,[138] as well as multiple initiatives and exercises conducted with NATO Allies.[139] Together with a range of like-minded countries, in 2019, the US advanced a statement on responsible state behaviour

133. CyberSeek, 'Interactive Map', <https://www.cyberseek.org/>, accessed 27 March 2023.
134. The White House, 'National Cybersecurity Strategy', p. 27.
135. NICCS, 'Workforce Framework for Cybersecurity (NICE Framework)', <https://niccs.cisa.gov/workforce-development/nice-framework>, accessed 27 March 2023.
136. Blažič, 'Changing the Landscape of Cybersecurity Education in the EU', p. 3,015.
137. NIST, 'Updated NICE Framework Knowledge and Skills Statements for Public Comment', 19 April 2022, <https://www.nist.gov/news-events/news/2022/04/updated-nice-framework-knowledge-and-skill-statements-public-comment>, accessed 27 March 2023.
138. Christian Ruhl et al., 'Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads', Carnegie Endowment, February 2020, p. 6.
139. NATO, 'Exercise Locked Shields 2022 Concludes', 23 April 2023, <https://shape.nato.int/news-archive/2022/exercise-locked-shields-2022-concludes>, accessed 27 March 2023.

in cyberspace, supporting the efforts of UN working groups.[140] The US also became part of the Paris Call, a multi-stakeholder initiative led by France and Microsoft, in 2021,[141] after initially being absent from the initiative.[142]

Additional partnerships also allow the US to engage in 'strategically-minded capacity building', for example in cooperation with the African Union.[143] Further partnerships such as the trilateral agreement AUKUS (with the UK and Australia) aim to strengthen cyber defence and resilience in the Indo-Pacific.[144] Cyber security in the Indo-Pacific is further supported through the Quad, particularly in light of increased threats in this area stemming from China and North Korea.[145]

The US also indirectly advances norms through cooperation with other countries, for example when attributing cyber operations to states together with Five Eyes partners and others, or when imposing sanctions on cyber criminals (as was done more recently with the UK).[146] In addition, a wide range of bilateral agreements further ensure US cooperation on cyber-security issues with like-minded jurisdictions such as Canada (on the protection of the shared energy infrastructure)[147] and the UK (for a joint cyber academy).[148] US cooperation with the EU is particularly noteworthy: after years of negotiations, the EU and the US recently agreed on a draft update for the EU–US

140. US Department of State, 'Joint Statement on Advancing Responsible State Behavior in Cyberspace', 23 September 2019, <https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/>, accessed 27 March 2023.
141. Paris Call, <https://pariscall.international/en/>, accessed 27 March 2023.
142. Ruhl et al., 'Cyberspace and Geopolitics', p. 11.
143. EU Cyber Direct, Atlas, 'United States: Resilience', <https://eucyberdirect.eu/atlas/country/united-states>, accessed 27 March 2023.
144. Jocelinn Kang, 'Enhancing Cyber Capabilities Through AUKUS', ASPI, 16 September 2022, <https://www.aspistrategist.org.au/enhancing-cyber-capabilities-through-aukus/>, accessed 27 March 2023.
145. Dipanjan Roy Chaudhury, 'Quad Meet to Boost Cyber Security in Indo-Pacific', *Economic Times*, 4 February 2023, <https://economictimes.indiatimes.com/news/politics-and-nation/quad-meet-to-boost-cyber-security-in-indo-pacific/articleshow/97588173.cms?from=mdr>, accessed 27 March 2023.
146. Jones, 'Five Eyes and US Governments Finally Confirm Russia was Behind Ukrainian Government, Viasat Cyber Attacks'; Maggie Miller, 'U.S., U.K. Sanction Russian Hackers in Ransomware Attacks', *Politico*, 9 February 2023.
147. Public Safety Canada, 'National Cyber Security Strategy 2019–2024: Report on the Mid-Term Review', <https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019-md-trm/index-en.aspx>, accessed 27 March 2023.
148. UK Ministry of Defence, 'New £50 Million Cyber Academy to Benefit Influential UK–US Relationship', 28 September 2022, <https://www.gov.uk/government/news/new-50-million-cyber-academy-to-benefit-influential-uk-us-relationship>, accessed 27 March 2023.

data privacy framework,[149] and in 2021 they set up the EU–US Trade and Technology Council for closer cooperation on digital transformation and technologies, based on shared values.[150]

With respect to workforce development, the new US cyber-security strategy acknowledges that workforce development is a global issue. The strategy therefore seeks to enhance cooperation with other countries and to learn from their experience to further develop a skilled and diverse cyber workforce.[151]

149. Natasha Lomas, 'EU Confirms Draft Decision on Replacement US Data Transfer Pact', *TechCrunch*, 13 December 2022, <https://guce.techcrunch.com/copyConsent?sessionId=3_cc-session_9b45383f-5ada-430c-ab1e-b1a0b129635f&lang=en-US>, accessed 27 March 2023.
150. European Commission, 'EU–US Trade and Technology Council', <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/stronger-europe-world/eu-us-trade-and-technology-council_en>, accessed 27 March 2023.
151. The White House, 'National Cybersecurity Strategy', p. 27.

Canada

Context

CANADA CENTRES ITS cyber policy around its National Cyber Security Strategy, which was published in 2018.[152] The core goals of this strategy were secure and resilient Canadian systems; an innovative and adaptive cyber ecosystem; and effective leadership, governance and collaboration. These goals remain valid, and an action plan guides their implementation.[153] The 2021 mid-review of the strategy found that its targets were being met, including the establishment of the Canadian Centre for Cyber Security, but that challenges persist 'in meeting the growing demands for cyber talent'.[154]

The cyber-threat landscape has expanded since the publication of Canada's National Cyber Security Strategy. While Canada has highly developed cyber-security systems, it is also one of the most targeted countries, especially when it comes to cybercrime.[155] The head of the Canadian Centre for Cyber Security wrote in 2022 that 'Cybercrime is still the number one cyber threat activity affecting Canadians [and the] state-sponsored cyber programs of China, Russia, Iran and North Korea continue to pose the greatest strategic cyber threat to Canada'.[156] Canada's internet usage has increased since the Covid-19 pandemic in 2020, thereby also expanding the threat surface, both for individuals and for organisations.[157]

Although they were not caused by cyber attacks, Canada experienced internet outages in 2021 and 2022 that demonstrated the vitalness of stable connectivity and the highly connected nature of critical infrastructure sectors.[158] The increased risk to critical infrastructure was confirmed by the Canadian Centre for Cyber Security's cyber-threat assessment for 2023–24. Threats include that posed by state-sponsored cyber operations; influence-seeking by cyber-threat actors that are 'degrading trust in online spaces'; and ransomware attacks and other forms of cybercrime

152. Public Safety Canada, 'National Cyber Security Strategy', 2018, <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf>, accessed 27 March 2023.
153. Public Safety Canada, 'National Cyber Security Action Plan (2019–2024)', 2019, <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019/index-en.aspx>, accessed 27 March 2023.
154. Public Safety Canada, 'National Cyber Security Strategy 2019–2024: Report on the Mid-Term Review'.
155. Paul Bischoff, 'Which Countries Have the Worst (and Best) Cybersecurity?', *CompariTech*, 26 September 2022.
156. Canadian Centre for Cyber Security, *National Cyber Threat Assessment 2023–2024* (Ottawa: Communications Security Establishment, 2022), p. iii, <https://cyber.gc.ca/sites/default/files/ncta-2023-24-web.pdf>, accessed 27 March 2023.
157. *Ibid*., pp. 1–2.
158. *Ibid*., p. 9.

targeting Canadians and Canadian organisations.[159] Canadian cyber policy focuses on adapting to this changing threat landscape and on tackling continuing issues, such as shortages of the cyber-security professionals necessary for ensuring resilience in the context of the morphing threat landscape.

Priorities for National Cyber-Resilience Measures for CNI

Like other jurisdictions discussed in this paper, Canada stresses the importance of increasing the resilience of its critical infrastructure. Canada defines its critical infrastructure as comprising 10 sectors.[160] Canadian CNI has been subject to several significant cyber incidents, in particular the healthcare sector and local government.[161] The National Cyber Threat Assessment 2023–2024 points out that critical infrastructure depends on its supply chains, making CNI especially vulnerable as attackers might first target a supplier to infiltrate or disrupt CNI.[162] Despite deteriorating relations with Russia and China, however, Canada's 2023–24 Cyber Threat Assessment concludes that 'state-sponsored cyber threat actors will very likely refrain from intentionally disrupting or destroying Canadian critical infrastructure in the absence of direct hostilities'.[163]

To further secure its CNI, Canada has 'increased bilateral collaboration with the United States on critical energy infrastructure protection'.[164] In June 2022, Canada introduced Bill C-26, which requires designated operators (i.e., those providing vital services, including in the energy, finance, transport and telecommunications sectors) to increase their cyber-security measures and to report attacks. If the bill becomes law, such measures will be enforceable by the authorities with the help of audit powers, fines and even criminal penalties.[165] This legislation, if passed, would have a direct impact on private companies operating in Canada. If designated as operators under Bill C-26, companies will have to establish, maintain and review a cyber-security programme within 90 days, report incidents, comply with directions and maintain

159. *Ibid.*, p. iv.
160. Public Safety Canada, 'National Strategy for Critical Infrastructure', 2009, <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf>, accessed 27 March 2023.
161. See for example *CBC News*, 'N.L. Health-Care Cyberattack is Worst in Canadian History, Says Cybersecurity Expert', 4 November 2021; Corin Faife, 'A Small Canadian Town is Being Extorted by a Global Ransomware Gang', *The Verge*, 22 July 2022, <https://www.theverge.com/2022/7/22/23274372/st-marys-canada-lockbit-ransomware-cyber-incident>, accessed 27 March 2023.
162. Canadian Centre for Cyber Security, *National Cyber Threat Assessment 2023–2024*, p. 10.
163. *Ibid.*, p. 9.
164. Public Safety Canada, 'National Cyber Security Strategy 2019–2024: Report on the Mid-Term Review'.
165. Jim Bronskill, 'Ottawa's Cybersecurity Bill Flawed and Should Be Amended, New Report Warns', *Global News*, 18 October 2022.

records of incidents and compliance.[166] Implementing such suggested obligations will require a skilled cyber workforce.

The government's bill has been criticised as 'potentially impair[ing] the ability of private companies to dispute demands, orders, or regulations that are issued by the government' and for having 'overly broad secrecy clauses', raising concerns over transparency and accountability.[167] Others see the mandatory reporting and information sharing between agencies as necessary steps to combat cybercrime, which in turn benefits both organisations and individuals.[168] The bill recently finished its second reading in the Canadian House of Commons, and has yet to go to the Senate, and so it could still be amended over the course of the legislative procedure, but it could become law in 2023.[169]

Workforce and Skills Development and Regulation

As with the other jurisdictions examined in this paper, the implementation of cyber-security obligations in Canada and the achievement of good cyber-security standards more generally there – in order to increase the country's cyber resilience – requires a skilled cyber workforce. The shortage in Canada's cyber-security workforce remains stable but considerable.[170] Canada actively competes for the skilled workers it needs, particularly with the US. As US entities pay relatively higher salaries, the US is an attractive place of work for Canadians. While this leads to the risk of a 'brain drain' in the Canadian cyber-security sector, some commentators see lower Canadian wages as an opportunity for investors in the cyber-security sector.[171] Within

166. Fasken, 'Bill C-26: New Cybersecurity Requirements in Critical Infrastructure', 23 June 2022, <https://www.fasken.com/en/knowledge/2022/06/23-new-cybersecurity-requirements-in-critical-infrastructure>, accessed 27 March 2023.
167. Christopher Parsons, 'Cybersecurity Will Not Thrive in Darkness: A Critical Analysis of Proposal Amendments in Bill C-26 to the Telecommunications Act', *Citizen Lab*, Research Report 158, 18 October 2022, p. 41, <https://citizenlab.ca/wp-content/uploads/2022/10/Report158-critical-analysis-telecom-act.pdf>, accessed 27 March 2023.
168. Shane Morganstein et al, 'Bill C-26: New Canadian Critical Infrastructure Cyber Security Law', BLG, 20 June 2022, <https://www.blg.com/en/insights/2022/06/bill-c26-new-canadian-critical-infrastructure-cyber-security-law?utm_source=mondaq&utm_medium=syndication&utm_term=Technology&utm_content=articleoriginal&utm_campaign=article>, accessed 27 March 2023.
169. Parliament of Canada, Legisinfo, 'C-26 – An Act Respecting Cyber Security, Amending the Telecommunications Act and Making Consequential Amendments to Other Acts', <https://www.parl.ca/legisinfo/en/bill/44-1/c-26>, accessed 27 March 2023.
170. (ISC)², 'Cybersecurity Workforce Study 2022', p. 8.
171. Information and Communications Technology Council, 'Cybersecurity Talent Development: Protecting Canada's Digital Economy', May 2022, p. 10, <https://www.digitalthinktankictc.com/ictc-admin/resources/admin/cybersecurity-talent-development.pdf>, accessed 27 March 2023; Philippe Ferland, 'Why U.S. Cybersecurity Firms Choose Canada', Invest in Canada, <https://www.investcanada.ca/blog/why-us-cybersecurity-firms-choose-canada>, accessed 27 March 2023.

Canada itself the number of job postings among the different provinces varies considerably, with Ontario serving as the main hub of cyber-security-related jobs.[172]

With respect to cyber workforce qualifications, Canada provides both formal cyber-security education (through universities) and a range of complementary options via online courses, coding bootcamps and certification schemes.[173] Furthermore, the Future Skills Centre supports a number of initiatives aimed at diversifying Canada's cyber-security workforce, for example the Canadian Cybersecurity Skills and Talent Transformation scheme, a joint project with Rogers Cybersecure Catalyst.[174] Canada has also adopted a Cybersecurity Skills Framework, which largely overlaps with the established US Cyber Security Workforce Framework (NICE), but which focuses on the needs of the Canadian labour market and SMEs.[175]

Nevertheless, in 2022 the Canadian Chamber of Commerce – in cooperation with tech companies and civil society – demanded publicly that the government further prioritise the cyber-security sector, including bolstering the cyber-security workforce 'by investing in cybersecurity education, talent development, retention and programs that diversify and expand the cyber workforce'.[176] TECHNATION, a not-for-profit initiative representing Canadian technology companies, lists four main challenges for workforce development in Canada, including: the need to generate and retain cyber security talent; the need for technical and non-technical roles to gain sufficient knowledge, skills and abilities; and the need to normalise cyber security within the workplace. In addition, the Canadian workforce must be 'responsive to the changing technology landscape'.[177] In February 2023, the Canadian government announced additional support in the form of 250 million CAD for upskilling its workforce, including in the cyber-security profession, with the help of short-cycle upskilling programmes run in partnership with Palette Skills.[178]

172. Information and Communications Technology Council, 'Cybersecurity Talent Development', p. 16.
173. *Ibid*., p. 22.
174. Future Skills Centre, 'Canadian Cybersecurity Skills and Talent Transformation', <https://fsc-ccf.ca/projects/canadian-cybersecurity/>, accessed 27 March 2023.
175. TECHNATION Canada, 'TECHNATION Releases Canadian Cybersecurity Skills Framework', 30 June 2020, <https://itac.ca/wp-content/uploads/2020/06/June2020-Newsletter-Cybersecurity-Skills-Framework-Final.pdf>; TECHNATION Canada, 'Canadian Cybersecurity Skills Framework', <https://technationcanada.ca/en/future-workforce-development/cybersecurity/cybersecurity-skills-framework/>, accessed 27 March 2023.
176. Canadian Chamber of Commerce, 'Open Letter: Ottawa Needs to Get Serious About Cybersecurity. Right. Now.', 2022, <https://chamber.ca/wp-content/uploads/2022/03/CRN-OpenLetter20220120.pdf>, accessed 27 March 2023.
177. TECHNATION Canada, 'Canadian Cybersecurity Skills Framework'.
178. Government of Canada, 'Canada Steps Up to Meet the Skilled Labour Needs of High-Growth Sectors', 27 February 2023, <https://www.canada.ca/en/innovation-science-economic-development/news/2023/02/canada-steps-up-to-meet-the-skilled-labour-needs-of-high-growth-sectors.html>, accessed 27 March 2023.

International Interaction on Cyber-Norm Development

Canada has been an active partner for international cyber-norm development, for example when advocating for an open, secure and multi-stakeholder-led internet, and supporting the application of existing international law and norms of responsible behaviour in cyberspace. Canada is not in favour of the conclusion of a new international law treaty on the regulation of cyberspace. Instead, in 2022, Canada published its interpretation of existing international law applicable to cyberspace,[179] and has promoted the applicability of norms of responsible state behaviour in various forums, such as the G7, the G20 and NATO.[180]

In its international cooperation on cyber policy, Canada is focused in particular on 'help[ing] other countries expand their capacity building activities', which has been 'a key aspect of Canada's cyber engagement strategy'.[181] This commitment is demonstrated in a number of initiatives, focusing largely on Latin America, the Caribbean and Southeast Asia.[182] For example, Canada has contributed significantly to cyber capacity-building, especially in Latin America, by allocating funds to the Anti-Crime Capacity Building Program.[183] Similarly, Canada works with the Inter-American Committee against Terrorism to improve participation in UN processes on cybercrime and cyber-security negotiations.[184] Within the Organisation of American States, Canada also funded a project (as of 2022) to support other member states in targeting and understanding the implications of the gender gap in the cyber-security workforce.[185]

In cooperation with other allies, especially the Five Eyes community, Canada has repeatedly attributed malicious cyber activities to other states.[186] It has also funded projects related to how

179. Government of Canada, 'International Law Applicable in Cyberspace', <https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng>, accessed 27 March 2023.
180. EU Cyber Direct, 'Canada', <https://eucyberdirect.eu/atlas/country/canada>, accessed 27 March 2023.
181. *Ibid*.
182. European Commission, 'International Cyber Capacity Building: Global Trends and Scenarios: Annex 3: Notes on Cyber Capacity Building Funders', September 2021, p. 10ff, <https://www.iss.europa.eu/sites/default/files/EUISSFiles/CCB%20Annex%203%20Final_0.pdf>, accessed 27 March 2023.
183. *Ibid*., p. 10ff.
184. Cybil, 'Canada's Support to the OAS and its Member States to Prevent, Combat and Mitigate Cybersecurity Threats in the Americas', <https://cybilportal.org/projects/canadas-support-to-the-oas-and-its-member-states-to-prevent-combat-and-mitigate-cybersecurity-threats-in-the-americas-phase-2/>, accessed 27 March 2023.
185. Cybil, 'Canada's Support to the OAS and its Member States in Addressing the Gender Gap in the Cybersecurity Agenda', <https://cybilportal.org/projects/canadas-support-to-the-oas-and-its-member-states-in-addressing-the-gender-gap-in-the-cybersecurity-agenda/>, accessed 27 March 2023.
186. Howard Solomon, 'Canada, Allies Accuse China of Widespread Malicious Cyber Activity', *IT World Canada*, 19 July 2021, <https://www.itworldcanada.com/article/canada-allies-accuse-china-of-widespread-malicious-cyber-activity/455953>, accessed 27 March 2023.

attribution can be made.[187] Attribution is critical, as it helps to hold malicious actors accountable, and is in line with Canada's increasingly active role in this and other related areas.[188]

187. Government of Canada, 'Cyber Attribution for the Defence of Canada', <https://www.canada.ca/en/department-national-defence/programs/defence-ideas/element/competitive-projects/challenges/cyber-attribution-for-the-defence-of-canada.html>, accessed 27 March 2023.
188. See for example Mike Wendling, 'Canada Bans TikTok on All Government Devices', *BBC News*, 28 February 2023.

Japan

Context

IN JAPAN, THE award of the 2020 Olympic Games prompted a significant increase in cyber-security awareness.[189] Aiming to protect the 2020 Olympic Summer Games from cyber attacks, the Japanese government launched widespread campaigns to build up cyber resilience (including in the private sector) and to educate the workforce. The Olympics thus arguably served as a springboard for further raising cyber-security standards in the Japanese private sector.[190] This aim was also reflected in the country's 2018 Cyber Security Strategy (for 2018–21),[191] which focused primarily on the Olympic and Paralympic Games, recognising 'the potential cyber threat from hostile states', and referring on its first page to the growing danger of 'organised, sophisticated, and possibly state-sponsored' cyber attacks.[192] Japan's cyber-security strategy thus focuses on protecting critical infrastructure, on stakeholder cooperation, and on the improvement of cyber security in the private sector.[193]

While these approaches were widely considered to have been successful in protecting the (Covid-19-delayed) Olympic Games, the priorities outlined above remain highly relevant in 2023. However, Japan's approach to cyber security changed significantly in 2022, in light of an increasing number of cyber attacks against the country,[194] and in particular given the deteriorating relationships with China and Russia.[195] While still in the process of determining a cyber-security budget for 2024, Japan announced a significant change in its cyber strategy, including the adoption of an active cyber defence.[196] Japan had previously alluded to deterrence

189. Brian Gant, 'The Tokyo Olympics are a Cybersecurity Success Story', *Security Magazine*, 17 August 2021.
190. Gabriel Dominguez, 'As Japan's Neighbors Ramp Up Offensive Capabilities in Cyberspace, SDF Aims to Bolster Defense', *Japan Times*, 8 September 2022, referencing Mihoko Matsubara, chief cyber-security strategist at telecoms company NTT.
191. For a summary, see NISC, 'Summary of the [sic] Japan's Cybersecurity Strategy (July 27, 2018 Cabinet Decision)', <https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-shousaigaiyou-en.pdf>, accessed 27 March 2023.
192. IISS, 'Cyber Capabilities and National Power', p. 80.
193. *Ibid*.
194. For several prominent examples, see Cyberlands, 'Top 14 Cybersecurity Breaches in Japan', <https://www.cyberlands.io/topsecuritybreachesjapan>, accessed 27 March 2023.
195. See, for example, Jesse Johnson, 'Japan Eyes Eased Rules for Firing on Aircraft Violating Airspace', *Japan Times*, 15 February 2023. There is Russia–Ukraine, but also cyber attacks on Japanese government websites by the pro-Russian Killnet group: see Zach Marzouk, 'Japan Investigates Potential Russian Killnet Cyber Attacks', *IT Pro*, 7 September 2022.
196. Jun Osawa, 'How Japan is Modernizing its Cybersecurity', Stimson, 2 February 2023, <https://www.stimson.org/2023/japan-cybersecurity-policy/>, accessed 27 March 2023.

capabilities in its 2018 strategy,[197] but the recent shift is significant. Some even consider it to be a 'turning point' for Japan's defence policy,[198] which is traditionally limited by Japan's pacifist constitution (as well as by privacy considerations). This recent shift constitutes an atypical, proactive approach, which is considered necessary to 'actively pre-empt and stop attacks before they reach Japan's systems'.[199]

Overall, Japan primarily pursues a top-down approach when advancing cyber-security measures domestically, relying predominantly on 'government regulators to establish cyber-security requirements'.[200] Japanese cyber-security policy includes key areas such as the protection of national infrastructure and the development of the cyber workforce, which will be addressed in more detail in the following sections.

Priorities for National Cyber-Resilience Measures for CNI

Among the key issues in Japanese cyber policy are the protection of critical infrastructure and improving the resilience of supply chains, as well as wider cyber-security awareness, particularly in the private sector. While 'Japan remains a world leader in cyberspace technologies',[201] its own cyber-security standards have raised concerns in the past, for example in the US, which has criticised Japan's weak cyber-security practices and has considered these to be a barrier to deeper cooperation and intelligence sharing.[202] Yet the US and Japan have been working to overcome these differences through bilateral talks, including signing a Memorandum of Cooperation on Cybersecurity in January 2023 to strengthen the collaboration between the two countries in the area of cyber security.[203]

Japan's CNI is primarily owned by the private sector. The Basic Cyber Security Act entails duties for operators of critical infrastructure businesses,[204] a group that has expanded in recent years, and which now includes 14 sectors.[205] However, these obligations are often vague, for

197. IISS, 'Cyber Capabilities and National Power', p. 80.
198. Takahashi Kosuke, 'Japan's Major Turning Point on Defense Policy', *The Diplomat,* 17 December 2022; Osawa, 'How Japan is Modernizing its Cybersecurity Policy'.
199. Zach Marzouk, 'Japan Considers Creating New Cyber Defence Agency as Attacks Ramp Up in Region', *IT Pro*, 24 November 2022.
200. IISS, 'Cyber Capabilities and National Power', p. 84.
201. *Ibid*., p. 82.
202. Christopher Johnstone, 'Japan's Transformational National Security Strategy', CSIS, 8 December 2022.
203. *Reuters*, 'U.S. and Japan Agree to Step Up Cybersecurity Cooperation', 7 January 2023.
204. Kazuyasu Shiraishi and Masaya Hirano, 'Cybersecurity in Japan', TMI Associates, <https://www.lexology.com/library/detail.aspx?g=5a1b0e44-9f84-432e-9bed-88523b2ebb6a>, accessed 27 March 2023.
205. Kenji Watanabe, 'PPP (Public-Private Partnership)-Based Cyber Resilience Enhancement Efforts for National Critical Infrastructures Protection in Japan', in E. Luiijf, I. Žutautaitė, B. Hämmerli (eds), *Critical Information Infrastructures Security* (Cham: Springer, 2019), pp. 170–71, <https://link.springer.com/chapter/10.1007/978-3-030-05849-4_13>, accessed 27 March 2023.

example when requiring that CNI providers 'deepen [their] interest in and understanding of the importance of cybersecurity',[206] and information-sharing on cyber incidents remains limited, for cultural and structural reasons.[207]

In an updated action plan from June 2022, the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) offers guidance for safety standards and information-sharing systems to further improve cyber-security standards in Japan. The plan, which is only available in Japanese, further recommends that businesses develop risk-management procedures, and sets out specific requirements to be met by CNI businesses and staff, including Chief Information Security Officers.[208]

Moreover, Japan passed an economic security bill in May 2022 that provides greater protection for supply chains and infrastructure with regard to cyber attacks.[209] More specifically, it imposes obligations on companies in critical infrastructure sectors to inform the government of software updates and to 'vet some equipment procurement'.[210] The private sector requires a skilled workforce to implement these obligations and to raise cyber-security awareness and resilience.

Beyond these measures, Japan continues to strengthen its strategic partnership with the US on cyber cooperation to ensure greater resilience, particularly if confronted with hostile actions by China.

206. Art. 6, The Basic Act on Cyber Security, Act No. 104, 12 November 2014, subsequently amended, as translated via Japanese Law in Translation, <https://www.japaneselawtranslation.go.jp/en/laws/view/3677/en#:~:text=Article%201The%20purpose%20of,the%20foundation%20of%20cybersecurity%20initiatives%2C>, accessed 27 March 2023.
207. IISS, 'Cyber Capabilities and National Power', p. 84.
208. One Trust Data Guidance, 'Japan: NISC Releases Cybersecurity CI Action Plan', 20 June 2022, <https://www.dataguidance.com/news/japan-nisc-releases-cybersecurity-ci-action-plan>, accessed 27 March 2023.
209. *Japan Times*, 'Japan Passes Economic Security Bill to Guard Sensitive Technology', 11 May 2022.
210. *Ibid*.

Workforce and Skills Development and Regulation

Like other jurisdictions dealt with in this paper, Japan is experiencing shortages in the cyber-security workforce,[211] and overall cyber-security awareness is arguably relatively low in Japan.[212] This situation is augmented as many Japanese companies outsource their IT and cyber-security work, resulting in smaller in-house teams compared with other countries.[213] Furthermore, Japanese work culture traditionally foresees a high rate of job rotation, which comes at the cost of acquiring specialised cyber-security skills.[214]

To respond to these skill shortages, the Japanese government has supported cyber-security skills development, for example by inaugurating the National Cyber Training Center (NICT),[215] which offers training courses, especially for under-25s, and the Industrial Cyber Security Center of Excellence for training for mid-career and senior professionals.[216] The NICT established a training programme, Cyber Colosseo, in advance of the Olympic Games,[217] and also holds CYDER defence exercises, particularly for government officials and CNI businesses.[218] However, information in English remains limited.[219] To establish a common language for cyber-security skills, Japan has previously adopted the US NICE workforce framework, a choice made attractive by the fact that many Japanese companies outsource their IT outside Japan, and require an international understanding of what cyber-security talents are needed.[220]

Individuals qualified in this area are thus in high demand in Japan and have good job opportunities. One IT recruitment agency reports that qualifications such as (ISC)²'s Certified Information Systems Security Professional (CISSP) are considered useful; that there is an increased demand for cloud engineers, such as Amazon Web Services engineers; and that demand is particularly

211. (ISC)², 'Cybersecurity Workforce Study 2022', p. 8.
212. Dominguez, 'As Japan's Neighbors Ramp Up Offensive Capabilities in Cyberspace, SDF Aims to Bolster Defense'; see also Sophos study showing little cyber-security awareness on Japanese boards: Sophos, 'The Future of Cybersecurity in Asia Pacific and Japan', April 2022, p. 25, <https://assets.sophos.com/X24WTUEQ/at/f3vctf7kcmj7rp3xrb3k73/sophos-future-of-cybersecurity-apj-2022-wp.pdf>, accessed 27 March 2023.
213. Mihoko Matsubara and Dai Mochinaga, 'Japan's Cybersecurity Strategy: From the Olympics to the Indo-Pacific', IFRI, February 2021, <https://www.ifri.org/en/publications/notes-de-lifri/asie-visions/japans-cybersecurity-strategy-olympics-indo-pacific>, accessed 27 March 2023.
214. Ibid.
215. National Cyber Training Center, <https://nct.nict.go.jp/>, accessed 27 March 2023.
216. Mihoko Matsubara, 'How Can Japan–UK Cybersecurity Cooperation Help ASEAN Build Cybersecurity Capacity?', Council on Foreign Relations, 16 April 2018.
217. Mihoko Matsubara and Dai Mochinaga, 'Japan's Cybersecurity Strategy', pp. 9–10.
218. *Ibid*., p. 10.
219. Mihoko Matsubara, 'How can Japan–UK Cybersecurity Cooperation Help ASEAN Build Cybersecurity Capacity?'
220. Cynthia Brumfield, 'Why NIST is So Popular in Japan', *Cyberscoop*, 8 November 2018, <https://cyberscoop.com/nist-japan-workforce/>, accessed 27 March 2023.

high for personnel related to public cloud services such as SaaS and IaaS.[221] The Japanese Ministry of Defense is also increasing its role as an employer of cyber-security workers, and has plans to increase cyber-defence personnel, aiming to expand today's 800 staff members to 5,000 by 2027.[222]

An initiative involving academia, government and the private sector founded the Cross-Sector Forum (2015) 'to build an ecosystem to educate, recruit, retain, and train cybersecurity talent' in Japan.[223] The Forum has been active in advancing definitions of relevant talents and skills, and has created guidelines and provided funding for universities for cyber-security courses on which staff members of consortium partners can teach.[224]

International Interaction on Cyber-Norm Development

Alongside these domestic policy considerations focused on increasing resilience and workforce development, Japan undertakes cyber-security diplomacy based on three main principles: the promotion of the rule of law; cooperation on capacity building; and the development of confidence-building measures.[225] Japan has also contributed to discussions on norm development in cyberspace, for example by participating in several rounds of UN expert group discussions on cyber norms; and, in 2021, it made a public statement on its interpretation of international law in cyberspace in the UN forum.[226]

With respect to norm development, Japan has stressed a preference for voluntary and non-binding norms on responsible state behaviour in cyberspace (as identified by the UN Group of Governmental Experts (UN GGE) report in 2015), and has voiced caution, both about extending these norms and about what it sees as the risk of prematurely debating a binding new treaty.[227] Japan is a member of the Budapest Convention against Cybercrime and, as of 2022, had joined NATO's Cooperative Cyber Defence Centre of Excellence.[228] The country is also a regular

221. G Talent Blog, 'IT Skills in Demand in Japan', 11 April 2022, <https://www.gtalent.jp/blog/japanwork-en/job-hunting-en/it-skills-in-demand-in-japan>, accessed 27 March 2023.
222. *Japan Times*, 'Japan Plans to Boost Cyberdefense Personnel to 5,000 By Fiscal 2027', 30 October 2022.
223. Mihoko Matsubara and Dai Mochinaga, 'Japan's Cybersecurity Strategy', p. 8.
224. Mihoko Matsubara and Dai Mochinaga, 'Japan's Cybersecurity Strategy'.
225. Ministry of Foreign Affairs of Japan, 'Japan's Security/Peace & Stability of the International Community', 7 February 2023, <https://www.mofa.go.jp/policy/page18e_000015.html>, accessed 27 March 2023.
226. Ministry of Foreign Affairs of Japan, 'Basic Position of the Government of Japan on International Law Applicable to Cyber Operations', 28 May 2021, <https://www.mofa.go.jp/files/100200935.pdf>, accessed 27 March 2023.
227. EU Cyber Direct, 'Japan', <https://eucyberdirect.eu/atlas/country/japan>, accessed 27 March 2023.
228. Laura Dobberstein, 'Japan Officially Joins NATO's Cyber Defense Center', *The Register*, 7 November 2022, <https://www.theregister.com/2022/11/07/japan_joins_nato_cyber_defence/>, accessed 27 March 2023.

participant in the ASEAN Regional Forum's efforts on cyber issues and participates in the G7 Cyber Expert Group.[229]

Japan also supports a number of capacity-building initiatives. These are coordinated by the NISC and focus primarily on ASEAN states. They include the annual ASEAN–Japan Cybersecurity Policy meeting and related working groups and activities.[230] Since 2018, Japan has funded the ASEAN–Japan Cybersecurity Capacity Building Centre, which supports talent development for the region's cyber-security workforce.[231]

Japan has a range of bilateral agreements to strengthen technology and cyber cooperation with other countries, for example with the US and the UK. With respect to the latter, both nations are currently seeking to 'make it easier for businesses to operate in both countries by aligning approaches to digital regulation'; to improve cyber resilience; and to 'promote initiatives to standardise the security of internet-connected products and apps'.[232]

229. IISS, 'Cyber Capabilities and National Power', p. 85.
230. European Commission, 'International Cyber Capacity Building: Global Trends and Scenarios: Annex 3', pp. 16–17.
231. ASEAN Japan Cybersecurity Capacity Building Centre, <https://www.ajccbc.org/about.html>, accessed 27 March 2023.
232. DCMS, 'New Plans to Strengthen Tech Ties Between UK and Japan', 7 December 2022, <https://www.gov.uk/government/news/new-plans-to-strengthen-tech-ties-between-uk-and-japan>, accessed 27 March 2023.

Singapore

Context

SINGAPORE IS A highly digitalised city state with advanced cyber-security regulation and policies. But as '[t]he cyber ecosystem in Singapore is expanding rapidly',[233] Singapore has also experienced a high number of cyber attacks in recent years, for example in the form of 'SMS-phishing scams targeting bank customers'.[234] One study finds that 65% of organisations in Singapore were hit by ransomware attacks in 2021.[235]

To respond to the changing threat landscape and boost cyber resilience, Singapore updated its cyber-security strategy in 2021. This now rests on three strategic pillars: building resilient infrastructure; enabling a safer cyberspace; and enhancing international cyber cooperation. In addition, the strategy identifies two foundational enablers: developing a vibrant cyber-security ecosystem; and growing a robust talent pipeline.[236]

With these priorities in mind, Singapore's strategy is that of a nation that 'has long set its sights on becoming a world-class, tech-driven city-state' and which, as a consequence, considers cyber security to be a matter of national security.[237] As regulation remains critical to supporting cyber resilience, Singapore's government 'explore[s] expanding the government's regulatory remit' under the updated cyber-security act, for example, to further expand regulation beyond CNI businesses.[238]

At the same time, Singapore has launched multiple initiatives and projects in coordination with other countries and the private sector that seek to enhance cyber resilience and to educate

233. Amirah Syahirah Bte Baharun, 'Securing the Digital Realm: Building Cyber Resilience in Singapore', *KrASIA*, 27 June 2022, <https://kr-asia.com/securing-the-digital-realm-building-cyber-resilience-in-singapore>, accessed 27 March 2023.
234. Genevieve Chow, 'Public Affairs Tracker: Singapore Refreshes Cybersecurity Strategy to Build a Cyber-Resilient Nation', *Sandpiper Singapore*, 10 March 2022, <https://sandpipercomms.com/corporate-communications/singapore-refreshes-cybersecurity-strategy-to-build-a-cyber-resilient-nation/>, accessed 27 March 2023.
235. Sophos, 'The State of Ransomware 2022', Sophos Whitepaper, April 2022, p. 12, <https://assets.sophos.com/X24WTUEQ/at/4zpw59pnkpxxnhfhgj9bxgj9/sophos-state-of-ransomware-2022-wp.pdf>, accessed 27 March 2023.
236. Cyber Security Agency of Singapore (CSA Singapore), *Singapore Cybersecurity Strategy* (Singapore: CSA, 2021) <https://ccdcoe.org/uploads/2018/10/Singapore_Cybersecurity_Strategy_2021.pdf>, accessed 27 March 2023.
237. Syahirah Bte Baharun, 'Securing the Digital Realm'.
238. Chow, 'Public Affairs Tracker'.

and cultivate a much-needed IT workforce.[239] One way the government seeks private sector engagement is through the Cybersecurity Industry Call for Innovation 2022,[240] in which the government invites cyber-security businesses to join the effort to identify and develop 'innovative solutions to address specific cybersecurity challenges'.[241]

Priorities for National Cyber-Resilience Measures for CNI

As outlined in its cyber-security strategy, building a resilient infrastructure is a key pillar of Singapore's cyber policy. To further enhance cyber-resilience measures for Critical Information Structure (CII), that is, any 'computer or computer system located wholly or partly in Singapore' that is 'necessary for the continuous delivery of an essential service',[242] Singapore's Cyber Security Agency (CSA) has launched a supply chain programme. This comes in the context of the increasingly complex threat landscape, but also in response to advanced digitalisation in the post-pandemic environment.[243] The programme sets out five initiatives, including a toolkit, a handbook, a certification scheme and a learning hub, designed to support businesses in the sector, as well as a platform for international cooperation.[244]

A complementary code of practice (CCoP 2.0) sets out measures and standards that businesses in the respective CII sectors must implement.[245] The second edition of these standards of performance came into force in July 2022 and 'specif[ies] the minimum requirements' that businesses in these sectors must adhere to.[246] Companies can, however, request waivers of

239. Syahirah Bte Baharun, 'Securing the Digital Realm'.
240. CSA Singapore, 'CSA Launches Cybersecurity Industry Call for Innovation 2022', press release, 31 August 2022, <https://www.csa.gov.sg/News-Events/Press-Releases/2022/csa-launches-cybersecurity-industry-call-for-innovation-2022>, accessed 27 March 2023.
241. Michael Hill, '22 Notable Government Cybersecurity Initiatives in 2022', CSO, 29 September 2022, <www.csoonline.com/article/3674954/23-notable-government-cybersecurity-initiatives-in-2022.html?page=2>, accessed 27 March 2023.
242. Cybersecurity Act 2018, Section 7(1), available at Singapore Statutes Online, <https://sso.agc.gov.sg/Acts-Supp/9-2018/>, accessed 31 March 2023.
243. CSA Singapore, 'Critical Information Infrastructure Supply Chain Programme: A National Effort in Managing Cyber Supply Chain Risks', 27 July 2022, <https://www.csa.gov.sg/Tips-Resource/publications/2022/cii-supply-chain-programme-paper>, accessed 27 March 2023.
244. *Ibid*.
245. CSA Singapore, 'Codes of Practice/Standards of Performance', <https://www.csa.gov.sg/Legislation/Codes-of-Practice>, accessed 27 March 2023.
246. Anna Ribeiro, 'Cyber Security Agency of Singapore Publishes CCoP 2.0 with Regulations for Owners of Critical Information Infrastructure', *Industrial Cyber*, 5 July 2022, <https://industrialcyber.co/critical-infrastructure/cyber-security-agency-of-singapore-publishes-ccop-2-0-with-regulations-for-owners-of-critical-information-infrastructure/>, accessed 27 March 2023.

requirements for valid reasons.[247] The CCoP further provides, among other things, incident response plans, and sets out design principles for cyber security.[248]

These increased cyber-security obligations have to be implemented by businesses and the cyber workforce. However, this can prove challenging, for example with respect to the CII supply chain guide, which some have perceived as offering limited concrete points for companies to implement, for instance in case of a supply chain attack or to prevent supply chain risks.[249]

Workforce and Skills Development and Regulation

In contrast to other jurisdictions examined in this paper, Singapore's shortage in the cyber-security workforce lessened significantly in 2022.[250] As it is Singapore's ambition to be a world leader in all things cyber, the government of Singapore has introduced a broad set of measures to attract highly skilled workers, including those in the IT sector. Alongside five-year visas and visa programmes such as the TechPass,[251] Singapore has an advanced digital infrastructure, ensuring that it is an attractive place to work.

But even where favourable conditions and the right regulations are in place, 'digital transformation will remain but a vision without the right talent to execute it', according to Senior Minister of State Tan Kiat How.[252] To secure such talent, further initiatives like the TechSkills Accelerator create links between students from education institutions such as the Singapore Institute of Technology and private sector companies, for example in the form of internship programmes.[253] At the same time, there have been calls for companies to engage in more skills-based assessments, rather than relying on formal academic qualifications during hiring processes.[254]

---

247. CSA Singapore, 'Cybersecurity Code of Practice for Critical Information Infrastructure: Second Edition, Revision 1, Cybersecurity Act 2018', para. 1.6, p. 13, <https://www.csa.gov.sg/docs/default-source/legislation/ccop---second-edition_revision-one.pdf?sfvrsn=421a71ab_1>, accessed 31 March 2023.
248. *Ibid*., para 3.5, p. 20.
249. Eileen Yu, 'Singapore Champions Asean CERT as Region's Cyber Armour', *ZDNet*, 20 October 2022, <https://www.zdnet.com/article/singapore-champions-asean-cert-as-regions-cyber-armour/>, accessed 27 March 2023.
250. (ISC)², 'Cybersecurity Workforce Study 2022', p. 8.
251. Singapore Economic Development Board, 'Tech.Pass', <https://www.edb.gov.sg/en/how-we-help/incentives-and-schemes/tech-pass.html>, accessed 27 March 2023.
252. Woo Hoi Yuet and Ranamita Chakraborty, 'What Comes Next in Digitalisation, and How Can Singapore Prepare for It?', *GovInsider*, 29 July 2022, <https://govinsider.asia/intl-en/article/what-comes-next-in-digitalisation-and-how-can-singapore-prepare-for-it-35th-cio-workshop-accenture>, accessed 27 March 2023.
253. *Ibid*.
254. *Ibid*.

In line with Singapore's preference for regulation of the cyber-security sector, businesses providing cyber-security services and operating in Singapore are also subject to several regulatory frameworks. For example, where businesses offer penetration testing or managed security operations centre monitoring services, as of 2022, they are required to obtain a licence. Such measures, which could still be extended to other cyber-security services, are intended to protect consumer interests as well as to 'improve service providers' standards and standing over time'.[255]

Singapore's CSA has also initiated a certification scheme that recognises businesses that have 'adopted and implemented good cybersecurity practices'.[256] More concretely, SMEs can achieve the CSA's 'Cyber Essentials' standard, which recognises good cyber-hygiene practices. For larger and international corporations, the CSA launched the 'Cyber Trust' mark, which recognises 'comprehensive measures and practices'.[257] The CSA's CEO, David Koh, sees the certification system as a means for companies to demonstrate their commitment 'to ensure that they remain cyber-secure, giving them an edge over their competitors' while simultaneously 'providing greater assurance to their customers'.[258]

International Interaction on Cyber-Norm Development

One of the strategic pillars of Singapore's 2021 cyber-security strategy aims to enhance international cyber cooperation to 'foster an open, secure, stable, accessible, peaceful, and interoperable cyberspace'.[259] Singapore is already proactively engaging in a wide range of initiatives fostering international cooperation on cyber matters. For example, Singapore has been an active participant in UN norm processes, including the UN's GGE and the Open-Ended Working Group, where Singapore has called for a 'UN cyber fellowship program for small states that would support the training in cyber issues for mid- to senior level officials from smaller developing countries'.[260] Furthermore, Singapore co-chairs, with Estonia, the UN Group on e-governance and cybersecurity, and chairs the UN Group of Friends on Digital Technologies, in cooperation with Finland and Mexico.[261]

255. Eileen Yu, 'Singapore Begins Licensing Cybersecurity Vendors', *ZDNet*, 10 April 2022, <https://www.zdnet.com/article/singapore-begins-licensing-cybersecurity-vendors/>, accessed 27 March 2023.
256. Michael Hill, '22 Notable Government Cybersecurity Initiatives in 2022'.
257. *Ibid*.
258. CSA Singapore, 'CSA Launches New Cybersecurity Certification Programme to Recognise Enterprises with Good Cybersecurity Practices', 29 March 2022, <https://www.csa.gov.sg/News-Events/Press-Releases/2022/csa-launches-new-cybersecurity-certification-programme-to-recognise-enterprises-with-good-cybersecurity-practices>, accessed 31 March 2023.
259. CSA Singapore, *Singapore Cybersecurity Strategy*, p. 2.
260. Geneva Internet Platform, 'Capacity-Building', <https://dig.watch/event/un-oewg-2021-2025-1st-substantive-session/capacity-building>, accessed 27 March 2023.
261. Ministry of Foreign Affairs of Singapore, 'Cybersecurity', <https://www.mfa.gov.sg/SINGAPORES-FOREIGN-POLICY/International-Issues/Cybersecurity>, accessed 27 March 2023.

Singapore hosts the annual Singapore International Cyber Week, a high-level event on cyber security fostering cooperation in the field, including on norm implementation.[262] Singapore has also been active in regional capacity building, for example when it announced in 2019 that it would provide around $22 million for the establishment of the ASEAN–Singapore Cybersecurity Centre of Excellence which, among other things, trains computer emergency response teams.

To further support these ambitions, Singapore has multiple bilateral agreements with countries such as Australia, Japan, France, Germany, the UK and the US, all working on improving cyber capabilities in Southeast Asia.[263] In late 2022, the Inaugural US–Singapore Cyber Dialogue was held, providing a platform of exchange for officials to discuss both further cooperation and topics such as supply-chain security, cyber capacity building, and cyber talent and workforce development.[264]

262. Geneva Internet Platform, 'Singapore International Cyber Week 2022', <https://dig.watch/event/singapore-international-cyber-week-2022#:~:text=18%20Oct%202022%20%2D%2020%20Oct%202022>, accessed 27 March 2023.
263. Keiko Kono, 'ASEAN Cyber Developments: Centre of Excellence for Singapore, Cybercrime Convention for the Philippines, and an Open-Ended Working Group for Everyone', NATO CCDCOE, <https://ccdcoe.org/incyder-articles/asean-cyber-developments-centre-of-excellence-for-singapore-cybercrime-convention-for-the-philippines-and-an-open-ended-working-group-for-everyone/>, accessed 27 March 2023.
264. US Department of State, 'Inaugural U.S.–Singapore Cyber Dialogue', 3 November 2022, <https://www.state.gov/the-inaugural-u-s-singapore-cyber-dialogue/>, accessed 27 March 2023.

Concluding Remarks

THE FOLLOWING CONCLUDING remarks set out initial comparative observations based on the research underlying this paper, and point to areas that require further research to better understand the various regulatory approaches to cyber-security issues.

- All the jurisdictions discussed in this paper have advanced a cyber strategy. While these strategies certainly take into account the cyber threat landscape and wider global contexts, aspects of the strategies remain specific to each jurisdiction (such as the Olympic Games in Japan). However, some common themes can be observed across the strategies:

    - Strategies are regularly updated in line with domestic timelines, but they also respond to international events. In the timeframe examined for this paper, recent trends include the rise of cybercrime, Russia's invasion of Ukraine, heightened tensions between China and Taiwan, and the increased need to secure CNI and supply chains.
    - These strategy updates increasingly focus on harmonising and streamlining each jurisdiction's existing and developing cyber policies. Such harmonisation is advanced to avoid both fragmentation and the duplication of effort. This is reflected in the UK's 2022 strategy and its 'whole of society' approach, and in the EU's efforts to move away from a sectoral approach towards a more cohesive cyber policy, including the development of a skilled cyber workforce.
    - There is a noticeable trend towards interventionist policies that emphasise regulatory approaches to cyber security, rather than voluntary standards. This trend was already apparent in the UK's 2016 cyber strategy, and is now also reflected in the US's 2023 National Cybersecurity Strategy. In line with this trend, businesses and cyber-security professionals must anticipate regulatory changes if they are to keep up with varying and increasingly binding obligations.

- Greater protection of CNI is a priority for all the jurisdictions discussed in this paper. Although the number and scope of sectors categorised as CNI varies from one jurisdiction to another, many of the designated sectors are common. Further efforts to advance mandatory cyber-security measures beyond CNI sectors is also a priority for many jurisdictions, which again has a direct impact on businesses and the cyber-security professionals who have to implement them. Thus businesses and cyber-security professionals have to simultaneously comply with changing and at times varying obligations among different jurisdictions – particularly if they operate internationally. Further research comparing and contrasting the varying scope of CNI designations and the respective cyber-security obligations for businesses and cyber-security professionals could help clarify ways for them to navigate the different requirements, and identify

the skills required from the workforce where businesses operate across a range of jurisdictions. Further research could also explore opportunities and approaches for harmonising the range of frameworks, policies, initiatives and changing regulations that currently exist.

- Although often a whole range of tools, frameworks and initiatives improving public–private partnerships are available to guide businesses in implementing these measures, it is not always clear what these obligations entail in detail. This is especially true for non-binding or vague standards. Although much information is available in English, where this is not the case it is especially challenging for external businesses and cyber-security professionals to understand how to comply with these obligations. Again, further comparative research would help businesses and cyber-security professionals understand the practical impact of changing regulations, new cyber-security measures and – especially – the varying obligations they must comply with, such as reporting requirements.
- A common theme seen across all the jurisdictions examined is the shortage of personnel in the cyber-security workforce, exacerbated by global events and trends, such as the Covid-19 pandemic and increased digitalisation. In fact, many of the jurisdictions outlined here compete directly with each other for skilled workers (for example, the US and Canada) or rely heavily on outside cyber expertise (as is the case for Japan). Governments have responded to such shortages by acknowledging the need to improve skills development through a range of initiatives. Many of the measures in place across the different jurisdictions resemble one another, especially where they focus on attracting young people to cyber-security professions, or involve adopting skills frameworks such as NICE or the ECSF to harmonise the language used to describe cyber-security roles. Some jurisdictions prioritise specific aspects in their efforts to support a robust talent pipeline, for example when aiming for greater diversity with respect to gender (Canada, the US) and region (the UK). However, despite the multitude of initiatives fostering skills development, little is known about their effectiveness. More research is needed to understand which initiatives help eliminate discrepancies between education and the demands of industry and, as a result, reduce the gaps in the cyber-security workforce. Singapore would make an interesting case study, providing further insights into the effectiveness of measures taken in 2022, when the city state was successful in reducing its gap in the cyber workforce.
- Overall, the jurisdictions studied in this paper share a cooperative, proactive attitude to the development of norms applicable to cyberspace, and seek to advance a free and secure internet. All entities covered are active supporters of the UN processes for norm development in cyberspace and engage in a range of multilateral, bilateral and multi-stakeholder arrangements, seeking greater cooperation on cyber issues with other states, regional organisations, and the private sector. Areas for cooperation include norm development and capacity building, but also the development of cyber-security skills and closing the gap in the cyber workforce.

About the Authors

Pia Hüsch is a Research Analyst in cyber, technology and national security at RUSI. Her research focuses on the impact, societal risks and lawfulness of cyber operations. Prior to joining RUSI, Pia conducted her doctoral research on the lawfulness of low-intensity offensive cyber operations in international law at the University of Glasgow. Her PhD focuses on the principles of sovereignty and non-intervention in cyberspace. Previously, Pia has been a visiting researcher at McGill University and has worked at the Glasgow Centre for International Law and Security, as well as in the Brussels office of the German Marshall Fund of the United States, where she conducted policy research and was part of the strategic convening team.

James Sullivan is the Director of Cyber Research at RUSI. He founded and has grown a research group at RUSI that considers a number of themes including: the role of national cyber strategies; the cyber threat landscape; cyber security and risk management; offensive cyber; cyber statecraft and diplomacy; and ransomware.

James joined RUSI from Deloitte's Cyber Risk team, where he provided analysis on the cyber-threat landscape and advised on defensive measures and risk-management strategies. Prior to this, James worked at the National Crime Agency as an Intelligence Analyst specialising in cybercrime threats.

James has contributed to a variety of publications and media outlets, such as the *Financial Times*, the BBC and CNN, and has provided briefings on aspects of the cyber threat to high-level forums such as the G7.