Royal United Services Institute
for Defence and Security Studies

Occasional Paper

Exploring National Cyber Security Strategies

Policy Approaches and Implications

Sneha Dawda

Exploring National Cyber Security Strategies

Policy Approaches and Implications

Sneha Dawda

RUSI Occasional Paper, February 2021

Royal United Services Institute
for Defence and Security Studies

190 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 190 years.

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

Published in 2021 by the Royal United Services Institute for Defence and Security Studies.

This work is licensed under a Creative Commons Attribution – Non-Commercial – No-Derivatives 4.0 International Licence. For more information, see <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

RUSI Occasional Paper, February 2021. ISSN 2397-0286 (Online).

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

Acknowledgements

We would like to gratefully acknowledge the advice and comments from all who provided their time to help with this research. Special thanks go to Tim Stevens, Anna Sarri and Eric Luiijf. Their advice helped to shape this paper and provided invaluable guidance. We would also like to thank Jamie MacColl for bringing a fresh perspective and sage advice. Finally, thanks to RUSI's publications team for helping to publish this research. Many thanks go to Conrad Prince and James Sullivan who provided critical advice and assistance in shaping the direction of this research.

Executive Summary

THE UK'S 2016 National Cyber Security Strategy (NCSS) is reaching its conclusion. In 2021, the UK government is due to release a new strategy. To complement the increasing popularity of NCSSs around the world, this paper explores 22 strategies. In doing so, it identifies six recurring policy challenges to be considered when building a national cyber strategy:

- An overarching challenge is to set and appropriately communicate actionable strategic objectives. Metrics to track progress and investment should be aligned with these objectives.
- States need to clearly articulate their perception of the threat landscape, their priorities and greatest challenges. This may be based on an overall national threat assessment, or if little has changed from a previous strategy, simply rearticulating the threat.
- Closely aligned to the threat landscape, a strategy should outline the approach to tackling cybercrime. Cybercrime can cost the economy a great deal and erode trust between citizens and technology, further damaging the digital economy.
- Raising cyber security standards in critical national infrastructure (CNI) is a major challenge for all states and should be a priority alongside investment in emerging technology to modernise CNI.
- Public–private partnerships should be aligned to the priority areas set by the strategy and the role of stakeholders beyond the walls of government should be clearly articulated.
- There should always be room for investment in soft power objectives, such as cyber capacity building. These interventions can contribute to increasing national and global cyber resilience.

This paper highlights the importance of learning from other national approaches when formulating a new NCSS. There are no simple solutions in such a complex and evolving policy area, but by highlighting how states conceptualise cyber policy issues it is possible to draw out some common approaches. Cyber security is a global policy challenge, and the UK government should continue to remain aware of other national approaches. It should not develop a new strategy in isolation from this global context.

While this paper does not examine the UK's NCSS specifically, it is part of a wider RUSI research project on future UK cyber security strategy. A subsequent paper will present direct policy recommendations on the priorities that the next UK NCSS (for 2021 and beyond) should consider.

Introduction

THE UK IS approaching a cyber security milestone. The 2016 National Cyber Security Strategy (NCSS), together with its £1.9 billion of investment, reaches its conclusion in 2021.[1] The government is now focusing on building its next NCSS, for 2021 and beyond. This paper examines a selection of NCSSs from Europe, Australia and North America. Its aim is to provide high-level thematic insights into different national approaches to cyber security policy and strategy. In doing so, it identifies common policy challenges faced by NCSSs.[2] This informs policymakers and practitioners of the range of factors to consider when deciding the scope and direction of a future NCSS.

These 22 strategies were selected for analysis because they are not only comprehensive strategies but also originated in countries that face cyber threats comparable to those faced by the UK. The review is not intended to be an appraisal of their effectiveness. International benchmarking indices of NCSSs already exist. For example, the ITU Cybersecurity Index and the Belfer Cyber Power Index present ranking systems on a country's broader cyber security resilience.[3] Meanwhile, several organisations offer advice to states on national cyber security strategies, including: the European Union Agency for Cybersecurity (ENISA); the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE); the Commonwealth; and the International Telecommunication Union (ITU).

Instead, this paper is a high-level summary of existing strategies' respective structures and common themes. It compares different approaches towards six policy challenges: setting clear strategic objectives; national threat assessments; cybercrime; standards in critical national infrastructure (CNI); public–private partnerships; and national cyber security capacity building. They have significant overlap with the seven policy challenges identified in a briefing paper on the 2021 UK NCSS.[4] This highlights that the context in which the UK will shape its next NCSS is not unique, and that Whitehall must learn from other national approaches. Lessons derived

[1] National Audit Office, 'Progress of the 2016–2021 National Cyber Security Programme', 15 March 2019.

[2] The findings from this paper will feed into a second paper on a future UK national cyber security strategy (NCSS), which will provide policy recommendations, a vision and a framework for the UK's next NCSS for 2021 and beyond.

[3] International Telecommunications Union (ITU), 'Global Cybersecurity Index', <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx>, accessed 17 December 2020; Belfer Center for Science and International Affairs, 'Reconceptualizing Cyber Power', April 2020, <https://www.belfercenter.org/publication/reconceptualizing-cyber-power>, accessed 17 December 2020.

[4] James Sullivan and Conrad Prince, 'The UK Cyber Strategy: Challenges for the Next Phase', RUSI Briefing Papers, June 2019. The overlap highlights common challenges experienced by all states, not just the UK.

from this research may also help other countries explore alternative models for their own strategies and assist their research efforts.

Many of the strategies analysed during this research will evolve and be improved to meet their respective strategic objectives. They may also change with the shifting threat landscape and other national priorities. NCSSs do not exist in isolation from government policies or challenges outside of cyber security. As the coronavirus pandemic has shown, states must navigate crises while bearing in mind the strategic importance that cyber security has for national and economic security.

Methodology

This paper is based on a literature review as part of a larger research project to analyse future approaches to the UK NCSS. The literature review analysed 21 NCSSs and 1 cyber strategy. It is designed to be of use to policymakers from the UK and beyond as a standalone examination of various cyber policy approaches that could be consider in the future, based on existing NCSSs.

For this review, the research team conducted a cross-country thematic analysis of strategies between June 2019 and January 2020.[5] The core literature for this research is the NCSS of each country that has been examined. Research findings also draw on academic and policy literature relating to cyber security policy and national cyber strategies, open source government documents and media reports.

There are already authoritative and helpful analyses of NCSSs.[6] In comparison to those pieces of research, this study does not seek to rank or make judgements on the strategies, but to provide a bird's-eye lens on multiple policy approaches. In this sense, it is more descriptive, providing the context of various national approaches. Therefore, this paper does not seek to make recommendations, but highlights key findings and questions for the development phase of future NCSSs.

As with any qualitative research study based on thematic analysis of literature, there are limitations. Research is restricted to information available in the public domain. The paper focuses heavily on policy documents. Language is also a barrier to analysis. Many of the original strategies are written in their native language and the policy documents used for this paper are all translations of the original documents, many of which are provided by the EU Agency for Cybersecurity (ENISA).[7] However, due to language barriers in some cases, wider policy documents without translations were inaccessible.

[5] Despite this timeline, the 2020 Australian NCSS was also included to take into account the policy developments between Australia's previous and current strategies.

[6] See, for example, Daniela Schnidrig and Lea Kaspar, 'Multistakeholder Approaches to National Cybersecurity Strategy Development', Global Partners Digital, 27 June 2018; Darius Štitilis, Paulius Pakutinskas and Inga Malinauskaitė, 'EU and NATO Cybersecurity Strategies and National Cyber Security Strategies: A Comparative Analysis', *Security Journal* (Vol. 30, No. 4, 2016), pp. 1151–68; H A M Luiijf et al., *Ten National Cyber Security Strategies: A Comparison* (Berlin: Springer, 2013), pp. 1–17.

[7] EU Agency for Cyber Security (ENISA), 'National Cyber Security Strategies – Interactive Map', <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map>, accessed 15 November 2020.

I. Defining a National Cyber Security Strategy

NATIONAL CYBER SECURITY Strategies come in many forms. A number of states are yet to produce an NCSS and others have an established history of producing them.[8] The first state to release a national strategy was the US. In 2003, the US Department of Homeland Security (DHS) released its 'National Strategy to Secure Cyberspace'.[9] The first public UK NCSS, on the other hand, was not published until 2011.[10] This emphasises that NCSSs are a fairly recent policy phenomenon. Despite this, NCSSs have been ambitious in their scope, attempting to consolidate a whole-of-government effort. This chapter outlines why NCSSs play an important role in cyber security policymaking.

First, cyber security is complex. On a technical level, the architecture of cyberspace is layered, with stakeholders at every level with varying governance functions.[11] On a user level, for those who interact with the internet for services or to use and adapt elements to provide services, the stakeholders are broad and encompass the whole of society. If a state's goal is to build cyber resilience across the country, a whole-of-society response is required with the broad range of stakeholders involved in achieving this aim. A strategy could not only help organise stakeholders, but also identify their appropriate roles, the actions they need to take and relevant oversight mechanisms.[12] For a whole-of-society approach to succeed, stakeholders must have clarity about their respective roles and responsibilities.

Cyber security is also defined differently by states. For instance, Spain's 2019 NCSS describes cyber security as 'cyberspace security', alluding to security in the domain itself rather than just networks and systems.[13] It outlines that cyber security 'spreads beyond the mere sphere of protecting technological patrimony and delves into political, economic and social fields'.[14] Or,

[8] At present, 104 countries have some form of NCSS. See CIPedia, 'National Cyber Security Strategy', <https://websites.fraunhofer.de/CIPedia/index.php/National_Cyber_Security_Strategy>, accessed 15 November 2020.

[9] Cyber Security and Infrastructure Security Agency, 'National Strategy to Secure Cyberspace', February 2003.

[10] HM Government, 'The UK Cyber Security Strategy', November 2011.

[11] C Inglis, 'Cyberspace – Making Some Sense of It All', *Journal of Information Warfare* (Vol. 15, No. 2, 2016), p. 26.

[12] ITU, World Bank, Commonwealth Secretariat, Commonwealth Telecommunications Organisation and NATO Cooperative Cyber Defence Centre of Excellence, 'Guide to Developing a National Cybersecurity Strategy – Strategic Engagement in Cybersecurity', 2018, p. 23.

[13] Government of Spain, 'National Cybersecurity Strategy', 2019, p. 9.

[14] *Ibid.,* p. 15.

on the other hand, cyber security can mean securing 'trust' in digital infrastructure, as Germany outlines.[15] Definitions of cyber security can vary across strategies. The World Economic Forum defines cyber resilience as 'the ability of systems and organizations to withstand cyber events, measured by the combination of mean time to failure and mean time to recovery'.[16] Essentially, any definition of cyber security is ultimately driven by a deeper desire to be resilient, which can result in different activity or priorities.

Cyberspace is inherently interconnected and global. Although national risk assessments may focus on national vulnerabilities, threats arise from across the globe. NCSSs provide an insight into the risk assessments of other countries and identify areas of international cooperation that states can take advantage of to cooperate.[17] National cyber strategies help to identify areas of cooperation and can be used as a tool of cyber diplomacy where mutual interests exist. Open, free and secure access to the internet is a widely shared vision among democracies. This provides opportunities to collaborate on developing this idea while ensuring a balance between openness and security.

Strategies give governments an opportunity to set out an ambitious vision for their future security.[18] For instance, Australia's 2020 Cyber Security Strategy explicitly outlines a vision 'to create a more secure online world for Australians, their businesses and the essential services upon which we all depend'.[19] Many countries use the opportunity to voice their commitment to securing and growing the digital economy, trust in infrastructure and innovative technology. This sets an overall direction for the strategy and provides continuity with cyber resilience. Essentially, ensuring cyber resilience has a tangible end goal, be that strengthening the economy, technology or trust.

Many states have implemented a NCSS for some of these reasons. NCSSs provide a glimpse into the potential benefits of having a coherent national cyber strategy. This paper builds on this by articulating some of the policy challenges faced by states and the existing interventions presented in various national cyber strategies. This is relevant not only for UK policymakers in the build up to the next NCSS, but for other states seeking to increase national cyber resilience as well.

[15] Federal Ministry of the Interior of Germany, 'Cyber Security Strategy for Germany', 2016, p. 3.

[16] World Economic Forum, 'Partnering for Cyber Resilience', 2012, p. 14.

[17] ITU, 'Guide to Developing a National Cybersecurity Strategy', p. 23.

[18] *Ibid.*, p. 13.

[19] Government of Australia, 'Australia's Cyber Security Strategy 2020', 6 August 2020, pp. 4, 7.

II. Strategic Objectives in National Cyber Security Strategies

ALL COUNTRIES FACE challenges in prioritising the objectives and desired outcomes of their respective NCSSs. These are not only short-term objectives, but also long-term aims that prompt action from government and wider society to increase overall cyber resilience. Any NCSS is reliant on a set of objectives and desired outcomes because they provide a method of communicating goals in order to move government machinery and the private sector in a unified way.[20] It is a subtle mechanism that allows government to introduce societal goals in the form of guidance, rather than regulation.[21]

The US has one core NCSS, written by the White House, that sets outs the national vision. However, different US Departments also have their own strategies that are far reaching in scope and therefore worthy of inclusion in this analysis.[22] Each strategy takes a different approach to the government's strategic aims. First, the White House uses a 'Pillars' approach to communicate its aspirations to 'Protect the American People, the Homeland, and the American Way of Life', 'Promote American Prosperity', 'Preserve Peace through Strength' and 'Advance American influence'.[23] It views cyber security through the lens of US values and goals, thus representing the White House's priorities. However, the DHS's strategy (five pillars with seven goals) outlines specific goals for national cyber security.[24] These objectives are purposely driven by the DHS, and it requires specific ownership and influence to achieve them. This contrasts with the overarching White House strategy, which has a strategic values-driven direction. One risk with this approach is that there is scope for overlap. For instance, both the White House and the DHS prioritise securing federal networks, CNI and tackling cybercrime.[25] While this does indicate that these issues are important enough to appear in both strategies, there remains a risk of diminished central coordination if not carefully managed.

[20] ITU, 'Guide to Developing a National Cybersecurity Strategy', p. 30.

[21] *Ibid*.

[22] However, the White House strategy is a whole-of-government NCSS, whereas the DHS strategy is only specific to that Department. See White House, 'National Cyber Strategy of the United States of America', 2018; Department of Homeland Security (DHS), 'US Department of Homeland Security Cybersecurity Strategy', 2018.

[23] White House, 'National Cyber Strategy of the United States of America', 2018, pp. V–VI.

[24] DHS, 'US Department of Homeland Security Cybersecurity Strategy', p. i.

[25] *Ibid.*; White House, 'National Cyber Strategy of the United States of America', p. V–VI.

Australia’s 2020 NCSS is wholly different. Instead of being driven by objectives, it assigns responsibilities and then objectives under each stakeholder group.[26] It clearly outlines the role of government, the private sector and the community. See Figure 1 for the breakdown of objectives. An analysis of the responsibilities will take place in Chapter VI on public–private partnerships.

Figure 1: The 2020 Australian NCSS

<table>
<tr><th colspan="3">Vision
A more secure online world for Australians, their businesses and the essential services upon which we all depend.</th></tr>
<tr><th>Actions by governments</th><th>Actions by businesses</th><th>Actions by the community</th></tr>
<tr><td><b>Key themes</b>:
• Protect critical infrastructure, essential services and households.
• Combat cyber crime, including on the dark web.
• Protect Australian government data and networks.
• Share threat information.
• Strengthen cyber security partnerships.
• Support business to meet cyber security standards.
• Enhance cyber security capabilities.</td><td><b>Key themes</b>:
• Improve baseline security for critical infrastructure.
• Uplift cyber security for small and medium enterprises.
• Provide secure products and services.
• Grow a skilled workforce.
• Take steps to block malicious activity at scale.</td><td><b>Key themes</b>:
• Access and apply guidance and information on cyber security.
• Make informed purchasing decisions.
• Report cyber crime.
• Access help and support when needed.</td></tr>
</table>

Source: Government of Australia, ‘Australia’s Cyber Security Strategy 2020’, 6 August 2020, p. 18.

Austria’s NCSS emphasises a multi-stakeholder approach through its strategic objectives. Objectives 2, 3, 5, 6, 8 and 9 include partnership or cooperation with stakeholders, including international organisations, local and regional governance, the private sector and individuals.[27]

In contrast, France’s NCSS does not frame the government’s relationship with the private sector as a partnership – suggesting a more limited role for the private sector.[28] Instead, its strategy is focused on the state’s capabilities and responsibilities, stressing ways in which the French government will deliver improved national cyber security, rather than alluding to an agenda

[26] Government of Australia, ‘Australia’s Cyber Security Strategy 2020’, p. 18.

[27] Government of Austria, ‘Austrian Cyber Security Strategy’, p. 9.

[28] While France does not mention partnerships in the strategy, it does have experience doing so through mechanisms such as Critical Information Infrastructures Protection Law. See French National Cybersecurity Agency, ‘The French CIIP Framework’, <https://www.ssi.gouv.fr/en/cybersecurity-in-france/ciip-in-france/>, accessed 17 December 2020.

built on public–private partnerships.[29] The five strategic aims that outline the priorities of the French government do not focus on partnerships or multi-stakeholder engagement. Of note, the fourth aim, regarding the 'environment of digital technology businesses, industrial policy, export and internationalisation', outlines the actions for the French government to follow but does not refer to any other stakeholders.[30]

Iceland's NCSS has four main aims and is distinguishable for its unique timeline. As opposed to more short-term objectives found in other NCSSs analysed, its will be delivered over a period of 11 years, making it a unique model of cyber governance. One caveat is that Iceland's plan of action to achieve these aims will be updated every three years.[31] Unlike other strategies, there is recognition of the tension between short- and long-term objectives. The Icelandic strategy recognises that to achieve improved cyber security, continuous iterations of implementation plans are required over an extended period.

There are several ways to present objectives in a strategy, as outlined above. The recurring theme throughout is that they all infer roles and responsibilities of different stakeholders because of set objectives. The role of government is defined through establishing objectives for the strategy to achieve. This has several implications. First, to set objectives, a clear idea of the role of government is required. Second, the private sector must help build cyber resilience, but this should not burden them so significantly that it undermines their role in the economy. Third, it must be assessed whether the timelines for objectives are ambitious or unrealistic.

[29] French National Cybersecurity Agency, 'French National Digital Security Strategy', 2015, pp. 13, 19, 25, 29, 37.

[30] *Ibid*., p. 29.

[31] Ministry of the Interior of Iceland, 'Icelandic National Cyber Security Strategy 2015–2026', 2015, p. 8.

III. National Threat Perception

THE CHARACTER OF cyber threats to governments, businesses and individuals is constantly evolving. State and non-state actors can compromise the confidentiality, integrity and availability of critical infrastructure and technology, sometimes simultaneously.[32] Governments have limited resources and so typically attempt to identify and prioritise the cyber threats most likely to affect them.

NCSSs are used as a tool for articulating this kind of national threat assessment. They consistently seek to identify and prioritise threats to their country's cyber security and resilience of digital services. In the NCSSs analysed as part of this paper, there are several threats outlined as per the assessment these states took. Some countries explicitly focus on geopolitical rivals taking deliberate action to threaten their economic wellbeing and national security. Others explicitly address concerns relating to the disruption in the availability of critical civilian and government resources. This chapter examines what types of threat actors NCSSs have focused on and what threats they perceive.

Threat Actors

Countries face a series of decisions when it comes to which threat actors should be prioritised when developing an NCSS. They can range from state actors, state-sponsored actors, cybercriminals and individual hacktivists. Prioritising different threat actors remains an important exercise in determining which has the potential to cause the most harm and how that harm can be mitigated.

Some states are most concerned about hostile state activity. Australia, Germany, Ireland, the Netherlands, Norway and both US NCSSs name state actors as one of the main threats they face in cyberspace.[33] Only the US and Ukraine specifically name states they believe represent a threat, echoing the wider geopolitical context.[34]

[32] The 'CIA Triad' – confidentiality, integrity, availability – is a well-established model for understanding how data or systems can be affected by a cyber incident.

[33] Government of Australia, 'Australia's Cyber Security Strategy 2020', p. 12; Federal Ministry of the Interior of Germany, 'Cyber Security Strategy for Germany', 2016, pp. 2–3; Government of Ireland, 'National Cyber Security Strategy 2019–2024', 2019, p. 5; Ministry of Foreign Affairs of the Netherlands, 'National Cyber Security Agenda', 2018, p. 7; Government of Norway, 'National Cyber Security Strategy for Norway', 2019, p. 6; White House, 'National Cyber Strategy of the United States of America', pp. 1–2; DHS, 'US Department of Homeland Security Cybersecurity Strategy', p. 2.

[34] White House, 'National Cyber Strategy of the United States of America', pp. 1–2; Government of Ukraine, 'The National Cyber Security Strategy of Ukraine', 2016, p. 1.

In their respective NCSSs, many of these states also refer to the threats posed by non-state groups. Australia, France, Germany, Ireland, the Netherlands, Norway, Turkey and the US all explicitly cite concerns about non-state actors.[35] These actors vary in motivation and sophistication: from organised criminal groups engaging in financially motivated operations to hacktivists pursuing ideological goals. However, there are still differences in the ways NCSSs perceive the threats posed by non-state actors. The US White House NCSS clarifies that the two categories are not always mutually exclusive, and emphasises that non-state actors are 'often shielded by hostile states'.[36] Canada's NCSS adds to this and emphasises the threat from non-state actors perpetrating cyber-enabled and dependent crime.[37] Mapping and understanding respective threat groups and determining the scope of harm they can cause communicates why a strategy is vital to wider stakeholders.

Perceived Threats

Several countries partly look at the vulnerability of their militaries. Austria, the Czech Republic, Finland, Germany, Latvia, the Netherland and Switzerland's NCSSs all explicitly mention the potential military implications of cyber security breaches.[38] This is compounded by the complexity of attribution. Germany's strategy acknowledges that issues around malicious and potentially destructive cyber activity are complicated by the difficulty states face in attributing attacks.[39]

Other states focus more on the threat of espionage from countries. The Czech Republic, France, the Netherlands, Norway, Switzerland, Ukraine and the US DHS broadly name espionage as one

[35] Government of Australia, 'Australia's Cyber Security Strategy 2020', p. 13; French National Cybersecurity Agency, 'French National Digital Security Strategy', 2015, p. 7; Federal Ministry of the Interior of Germany, 'Cyber Security Strategy for Germany', 2016, pp. 2–3; Government of Ireland, 'National Cyber Security Strategy 2019–2024', p. 5; Ministry of Foreign Affairs of the Netherlands, 'National Cyber Security Agenda', p. 7; Government of Norway, 'National Cyber Security Strategy for Norway', 2019, p. 19; Ministry of Transport and Infrastructure of Turkey, '2016–2019 National Cyber Security Strategy', 2016, pp. 17–19; DHS, 'US Department of Homeland Security Cybersecurity Strategy', p. 2.

[36] White House, 'National Cyber Strategy of the United States of America', pp. 1–2.

[37] Public Safety Canada, 'National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age', 2018, p. 2.

[38] Government of Austria, 'Austrian Cyber Security Strategy', p. 6; National Security Authority of the Czech Republic, 'National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020', 2015, p. 5; Secretariat of the Security and Defence Committee of Finland, 'Finland´s Cyber Security Strategy', 2013, p. 1; Federal Ministry of the Interior of Germany, 'Cyber Security Strategy for Germany', 2016, pp. 2–3; Government of Latvia, 'Cyber Security Strategy of Latvia 2014–2018', 2014, p. 2; Ministry of Foreign Affairs of the Netherlands, 'National Cyber Security Agenda', p. 11; Government of Switzerland, 'National Strategy for the Protection of Switzerland (NCS) Against Cyber Risks', 2012, pp. 2–4.

[39] Federal Ministry of the Interior of Germany, 'Cyber Security Strategy for Germany', p. 3.

of their key cyber security concerns.[40] While there are many sectors threatened by espionage, a number of states, including the Czech Republic, Iceland and the Netherlands, specifically call out the threat of industrial espionage.[41] Linked to this, for states concerned about broader geopolitical ramifications, economic implications are explicitly voiced. Such concerns are based on the comprehensive economic damage that can be done on a much larger scale. Canada's strategy mentions theft of intellectual property and trade secrets.[42] Finland's strategy, on the other hand, expresses concerns about state actors' ability to exert economic pressure through cyber attacks.[43] Iceland's strategy explicitly recognises that 'such espionage constitutes a large part of … economic damage', alluding to the vulnerabilities of economies in light of cyber attacks.[44] The White House's strategy accuses China of large-scale industrial espionage.[45]

Given the increasingly important role of digital services in CNI and national resilience, a number of countries, including Turkey, Germany, Latvia and Canada, raise concerns about their disruption.[46] Germany's NCSS cites the 'breakdown of information infrastructures' as a key cyber security concern,[47] while Latvia's strategy discusses the need to address anything that might 'disturb or suspend the operation of the network'.[48] Other states focus on the implications of such a disruption. Austria's NCSS raises the point that breaches of cyber security could 'interfere with … proper functioning' of CNI.[49] Canada's strategy goes one step further and explicitly describes the potential impact on 'the infrastructure that we rely on for essential services and

[40] National Security Authority of the Czech Republic, 'National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020', p. 5; French National Cybersecurity Agency, 'French National Digital Security Strategy', p. 8; Ministry of Foreign Affairs of the Netherlands, 'National Cyber Security Agenda', p. 11; Government of Norway, 'National Cyber Security Strategy for Norway', p. 19; Government of Switzerland, 'National Strategy for the Protection of Switzerland Against Cyber Risks', 2012, pp. 2–4; Government of Ukraine, 'The National Cyber Security Strategy of Ukraine', 2016, p. 1; White House, 'National Cyber Strategy of the United States of America', pp. 1–2; DHS, 'US Department of Homeland Security Cybersecurity Strategy', p. 2.

[41] National Security Authority of the Czech Republic, 'National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020', p. 5; Ministry of the Interior of Iceland, 'Icelandic National Cyber Security Strategy 2015–2026', p. 5; Ministry of Foreign Affairs of the Netherlands, 'National Cyber Security Agenda', p. 11.

[42] Public Safety Canada, 'National Cyber Security Strategy', p. 2.

[43] Secretariat of the Security and Defence Committee of Finland, 'Finland´s Cyber Security Strategy', p. 1.

[44] Ministry of the Interior of Iceland, 'Icelandic National Cyber Security Strategy 2015–2026', p. 5.

[45] White House, 'National Cyber Strategy of the United States of America', pp. 1–2.

[46] Ministry of Transport and Infrastructure of Turkey, '2016–2019 National Cyber Security Strategy', pp. 17–19; Federal Ministry of the Interior of Germany, 'Cyber Security Strategy for Germany', p. 2; Government of Latvia, 'Cyber Security Strategy of Latvia 2014–2018', p. 2; Public Safety Canada, 'National Cyber Security Strategy', p. 2.

[47] Federal Ministry of the Interior of Germany, 'Cyber Security Strategy for Germany', 2016, p. 2.

[48] *Ibid*., pp. 2–3; Government of Latvia, 'Cyber Security Strategy of Latvia 2014–2018', p. 2.

[49] Government of Austria, 'Austrian Cyber Security Strategy', p. 4.

our way of life'.[50] This illustrates that some governments now unambiguously view the cyber security of CNI as crucial to the functioning of the state and essential services.

In addition to concerns on a national scale, many national cyber strategies also acknowledge the impact cybercrime can have on citizens. Users of technology are often vulnerable to threats from criminals. Austria, the Czech Republic, France, Greece, Ireland, the Netherlands, Switzerland and Turkey cite examples of cyber-dependent and cyber-enabled crimes that may affect individuals within their countries.[51] Ireland further acknowledges the difficulties raised by the challenges of attributing these smaller-scale security threats.[52] This threat can create demand on law enforcement and investigative capabilities within a country and heighten the need to have good cyber literacy across society.

Some states express unique concerns. France's NCSS, for example, highlights the threat posed by growing digital oligopoly.[53] Its NCSS alleges that this oligopoly is 'using their dominant position' to block new businesses from entering the digital marketplace.[54] The concerns may have been prompted by ongoing disputes between the EU and internet giants such as Facebook or Google.[55] This suggests that there is potential for an NCSS to take a broader view of what constitutes a cyber threat.

Overall, the national threat perception of individual countries within the NCSS is a common method of communicating to wider stakeholders the main cyber threats facing their country. By doing so, appropriate defences, processes and mechanisms can be identified. States have emphasised different cyber threats without necessarily communicating the impact they may have. This leaves further questions, including: how do states weigh up the potential threat and which ones they should prioritise over others? How much does national threat perception influence the strategic objectives outlined in a country's NCSS?

[50] Public Safety Canada, 'National Cyber Security Strategy', p. 2.

[51] Government of Austria, 'Austrian Cyber Security Strategy', p. 4; National Security Authority of the Czech Republic, 'National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020', p. 5; French National Cybersecurity Agency, 'French National Digital Security Strategy', p. 8; Government of Ireland, 'National Cyber Security Strategy 2019–2024', p. 5; Ministry of Transport and Infrastructure of Turkey, '2016–2019 National Cyber Security Strategy'; Ministry of Foreign Affairs of the Netherlands, 'National Cyber Security Agenda'; Government of Switzerland, 'National Strategy for the Protection of Switzerland (NCS) Against Cyber Risks'.

[52] Federal Ministry of the Interior of Germany, 'Cyber Security Strategy for Germany', pp. 2–3; Government of Ireland, 'National Cyber Security Strategy 2019–2024', p. 5.

[53] French National Cybersecurity Agency, 'French National Digital Security Strategy', p. 8.

[54] *Ibid*., p. 8.

[55] Liz Alderman, 'France Moves to Tax Tech Giants, Stoking Fight with White House', *New York Times*, 11 July 2019.

IV. Tackling Cybercrime

HOW TO DEAL with cybercrime is a consistent policy challenge in NCSSs due to its complexity. At the eighth Interpol-Europol Cybercrime Conference, Interpol Secretary General Jurgen Stock claimed that ‘in a world where more than 4.5 billion people are online, more than half of humanity is at risk of falling victim to cybercrime at any time’.[56] Cybercrime includes both cyber-enabled and cyber-dependent crimes, and can be treated separately by law enforcement in the UK and globally.[57] The sheer volume of cybercrime that affects citizens has strained law enforcement agencies globally. With this seemingly insurmountable issue for government and law enforcement agencies, NCSSs could acknowledge that tackling cybercrime requires an organised response.

Strategies highlight different ways of tackling cybercrime and many states use a combination of responses as opposed to a single policy or initiative. While a comprehensive list of these approaches is beyond the scope of this paper, analysis of NCSSs reveals four responses to cybercrime. These responses were selected because this paper seeks to highlight a wide range of policy options for policymakers.

The first response is to work with the existing structure of police forces and law enforcement to counter the threat, while acknowledging the need to re-skill, upskill or request additional specialists to work on cybercrime. The Czech Republic’s strategy seeks to reinforce existing structures and cooperation procedures to manage cybercrime by strengthening the agencies responsible. The Czech government hope to achieve this by hiring more personnel for cybercrime police departments, modernising existing equipment, bolstering cooperation between law enforcement agencies and security agencies, information sharing with international partners and creating a ‘multidisciplinary academic environment to enhance police capabilities for prosecution’.[58]

In another example, Iceland’s NCSS approaches cybercrime as closely coupled with their aspirations for a prosperous society in that adequate management of cybercrime will lead to

[56] Interpol, ‘INTERPOL-Europol 8th Cybercrime Conference: “Half of Humanity at Risk”’, 6 October 2020.

[57] Cyber-enabled crime is defined as traditional crimes that use technology to engage in offences on a large scale. Cyber-enabled crimes include fraud, cyber bullying or child sexual offences. Cyber-dependent crimes can only be committed using technology, where the devices are both the tool for committing the crime and the target of the crime. They include malware propagation or distribution and purposeful hacking to destroy or damage a network. See Crown Prosecution Service, ‘Cybercrime – Prosecution Guidance’, <https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance>, accessed 6 March 2020.

[58] National Security Authority of the Czech Republic, ‘National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020’, p. 20.

prosperity.[59] To achieve this, the strategy emphasises the need to upskill existing police officers and ensure they have access to specialists in Europol.[60] Similarly, in Finland's NCSS, there is an expectation that the Finnish government will assist in securing sufficient powers, people and resources for existing law enforcement agencies to tackle and prevent cybercrime.[61]

The second type of cybercrime policy response is to create a strong statistical and reporting basis on cybercrime. This type of data-driven approach is used to help authorities decide what actions to take. Finland's NCSS outlines their policy approach by aligning metrics for reducing cybercrime as targets for their law enforcement agencies to reach.[62] These agencies will be expected to produce a comprehensive analysis of the cybercrime landscape and share it with other government entities.[63] Finland has a Cyber Security Centre that also acts as a National Communications Security Authority with which law enforcement agencies are expected to cooperate and share information.[64] France's NCSS emphasises there are 'currently no reliable statistics specifically related to digital delinquency or cybercriminality'.[65] Before making decisions on areas in which cybercrime prevention is lacking, the French Ministry of Interior will seek to implement tools to measure cybercrime and guide future decision-making.[66] Before its 2015 NCSS, France had the most cybercrime victims in Europe, according to Symantec.[67]

A third policy response is to draw on the international frameworks and organisations that deal with cybercrime. This includes information sharing with international institutions, enshrining their approaches within domestic legislation and complementing their approach to cybercrime. Germany's NCSS, for example, acknowledges that the cybercrime issue is not solely domestic and seeks to strengthen partnerships, including the Council of Europe Convention on Cybercrime (Budapest Convention).[68] Since the Irish strategy was implemented, the government has passed the Criminal Justice Act of 2017 which incorporated many aspects of the Budapest Convention.[69] Ireland's government has since explored multiple areas of legislation, including drafting an additional Cybercrime Bill to ensure all areas of the Budapest Convention have been covered.[70]

[59] Ministry of the Interior of Iceland, 'Icelandic National Cyber Security Strategy 2015–2026', p. 12.

[60] *Ibid*.

[61] Secretariat of the Security and Defence Committee of Finland, 'Finland's Cyber Security Strategy', p. 8.

[62] *Ibid*.

[63] *Ibid*.

[64] French National Cybersecurity Agency, 'French National Digital Security Strategy', 2015, p. 22.

[65] *Ibid*.

[66] *Ibid*.

[67] *RFI*, 'France Has Most Cybercrime Victims in Europe', 3 October 2013, <http://www.rfi.fr/en/economy/20131003-france-has-highest-cybercrime-rate-europe>, accessed 6 March 2020.

[68] Federal Ministry of the Interior of Germany, 'Cyber Security Strategy for Germany', p. 4.

[69] The Budapest Convention is a binding international instrument to unify signatories' efforts against cybercrime; Government of Ireland, 'National Cyber Security Strategy 2019–2024', p. 44.

[70] Department of Justice of Ireland, 'Minister Flanagan Makes a Statement on the Budapest Convention on Cyber Crime and the Lanzarote Convention on the Protection of Children Against

A fourth policy response to cybercrime emphasises prevention. This approach views cybercrime as an endemic issue due to insecure technology and poor cyber hygiene. Subsequent responses are then aimed at securing technology and raising a base level of cyber awareness in society to mitigate the threat. The Netherlands' NCSS views its ambition to reduce cybercrime in conjunction with its capability to strengthen technology through secure development practices.[71] Their aim is to reduce the vulnerability of people in society when they use technology in order to reduce the risk of a cybercrime through secure technology. They highlight the National High-Tech Crime Unit in the Dutch National Police and the Public Prosecution Service's National Unit as pivotal experienced institutions to tackling advanced threats to national security.[72] However, low-level cybercrime is not mentioned.

There will undoubtedly be other strategic policy responses to cybercrime that are not highlighted in this chapter. The four policy responses here are drawn from 22 strategies, but countries outside North America, Europe and Australia may adopt different approaches. Deeper questions emerge from these approaches. Notably, what data is most important to collect regarding the French approach and what does a data-driven law enforcement response consist of? Furthermore, regarding international approaches, is there current sufficient cooperation between countries in tackling cybercrime? Due to its international nature, should NCSSs outline how they will work bilaterally and multilaterally with other states?

Sexual Exploitation and Sexual Abuse', <http://www.justice.ie/en/JELR/Pages/SP19000010>, accessed 18 December 2020.

[71] Ministry of Foreign Affairs of the Netherlands, 'National Cyber Security Agenda', p. 35.

[72] *Ibid*.

V. Raising Cyber Standards in Critical National Infrastructure

IN 2017, UKRAINE'S government, National Bank, transportation services and largest power companies ground to a halt due to an attack by Russia called NotPetya.[73] The attack had severe global consequences, amounting to more than $1 billion in recovery costs.[74] The vulnerability of CNI is a major global concern, especially after high-profile attacks such as this.

NCSSs, however, vary in their approaches to bolster defences in CNI. This chapter identifies two broad categories of policy response relating to CNI. The first is to raise standards in both public- and privately-owned CNI. The second is to build a response framework for CNI in the event of a major cyber incident. Both approaches work towards increasing cyber resilience and protecting CNI adequately.

Resilience and Reinforcing Existing Public and Private Infrastructure

Protecting and raising the resilience of existing infrastructure is a common theme throughout the strategic approaches to CNI. Many states classify CNI sectors differently, but in this research, the focus is on what policy measures they use to raise resilience overall, regardless of what they classify as critical.

Austria's strategy already has an established Austrian Programme for Critical Infrastructure Protection, which its NCSS outlines is a forum for building on existing guidance.[75] The Austrian government has also organised a Cyber Security Steering Group to engage with wider sectors. It prioritises developing skills for IT and cyber security staff involved in critical infrastructure, and proposes reforms to CNI providers' reporting of anomalies detected on their networks.[76] Likewise, France's NCSS hopes to raise the resilience of 'critical networks' through coordination and cooperation with private sector stakeholders.[77] France particularly outlines the risk of relying on fewer operators in infrastructure, as that magnifies risk by increasing the attack surface of a given system or network. The concept of vendor diversity is a common theme

[73] Thomas Brewster, 'Another Massive Ransomware Outbreak Is Going Global Fast', *Forbes*, 27 June 2017.

[74] Andy Greenberg, 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History', *Wired*, 22 August 2018.

[75] Government of Austria, 'Austrian Cyber Security Strategy', p. 13.

[76] *Ibid*.

[77] French National Cybersecurity Agency, 'French National Digital Security Strategy', p. 3.

around innovation and security in the telecommunications sector, including 5G.[78] France also announced further proposals for the infrastructure operators that require more cyber security measures in line with European initiatives.[79]

Greece's NCSS takes a step back and suggests the need to define what constitutes 'critical infrastructure'. Furthermore, the strategy suggests a need to conduct a risk assessment to map out the variety of vulnerabilities and threats. The Greek government will then seek to enhance the resilience of the IT systems used in critical infrastructure.[80] In 2018, Greece implemented a national strategy on the security of network and information systems, but due to language constraints, further details cannot be provided. Conducting a risk assessment of existing critical infrastructure is an important step to take when formulating a strategy because it provides context to the measures.

In Iceland's NCSS, a slightly different view is taken on building resilience. Instead of simply hardening *existing* digital elements of infrastructure and issuing standards and guidance after digital infrastructure has deployed, the government suggests the need to embed cyber security considerations into procurement and supply chains. They specifically call out 'reliable design' in the procurement of software, emphasising the crucial elements of cyber security in deciding what software to purchase.[81] They also put a level of expectation on the telecommunications infrastructure providers to ensure reliability and support to other areas of Iceland's internet and IT infrastructure.[82]

Some European NCSSs draw reference to the EU's European Network Information Security Directive (NIS Directive) as a starting point for their approach to cyber risk management of CNI. The directive sets standards for states to oversee the cyber security of their critical infrastructure sectors. Ireland's NCSS commits to building on top of existing NIS Directive requirements through a joint analysis from the Irish Defence Forces, the Irish National Cyber Security Centre and An Garda Síochána (national police service) by mapping the 'interdependencies' of services between CNI elements.[83] They also plan to broaden the scope of critical infrastructure to include aspects of the electoral system and higher education. The current Threat Sharing Group and All

[78] James Sullivan and Rebecca Lucas, '5G Cyber Security: A Risk-Management Approach', *RUSI Occasional Papers* (February 2020), pp. 16–17.

[79] French National Cybersecurity Agency, 'French National Digital Security Strategy', p. 17; Melissa Hathaway et al., 'France: Cyber Readiness at a Glance', Potomac Institute, 2016, p. 9. In 2016, in line with the implementation of the Network Information Security Directive, France implemented further measures to protect its CNI and in 2018 transposed the directive into French law. See French National Cybersecurity Agency, 'The French Critical Infrastructures Information Protection Framework'.

[80] Government of Greece, 'National Cyber Security Strategy: Version 3.0', 2017, p. 7. The Greek National Cyber Security Strategy included in this research is taken from ENISA.

[81] Ministry of the Interior of Iceland, 'Icelandic National Cyber Security Strategy 2015–2026', p. 10.

[82] *Ibid*.

[83] Government of Ireland, 'National Cyber Security Strategy 2019–2024', p. 27.

Island Information Exchange will be broadened to wider critical infrastructure. Finally, they will introduce further compliance standards for telecommunications infrastructure.[84]

The US's DHS is concerned with the 10 critical infrastructure sectors it oversees. It sees a number of stakeholders as appropriate to engage with on securing national infrastructure: 'sector-specific agencies, non-federal cybersecurity firms, individual critical infrastructure entities, and other stakeholders'.[85] The engagement will attempt to give a bird's-eye view of CNI in order to analyse any vulnerabilities or 'systemic risk' across all stakeholders.[86] They further seek to prioritise their efforts on the operators or providers that would have the greatest impact on national security and public safety. The US National Institute for Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity is the key body in managing US CNI.[87]

Incident Response Management

The second most common policy approach is to manage the process of stakeholder engagement and management in an incident response scenario. Finland's NCSS outlines the need for resiliency during a cyber attack, and that planning should prioritise the availability of services. They will do so through 'contingency planning and exercises', providing training and guidance where needed.[88] The overall goal is to minimise the effects of a cyber attack when it happens.

Iceland's strategy takes an information-driven approach to ensuring critical infrastructure is available during a crisis.[89] Once information sharing during the event has occurred, the next steps will provide a post-mortem on the attack and issue recovery measures. Iceland puts emphasis on pursuing the criminals and ensuring their arrest. The US's DHS combines information- and stakeholder-driven approaches by taking responsibility for leading the response during a cyber attack on infrastructure as part of wider government groups called the Cyber Unified Coordination Group and the White House-led Cyber Response Group.[90]

Throughout the national strategies analysed, CNI is a prominent area of weakness identified by many states. There is an awareness that many components of CNI have been digitalised without considering the cyber security implications. Therefore, many countries' policy approaches are centred around retroactively securing existing digital infrastructure. While these approaches are not exhaustive, they provide a snapshot of concerns that surround raising standards in critical national infrastructure. However, what is the potential for further policy development outside

[84] *Ibid*., pp. 27–28.

[85] DHS, 'US Department of Homeland Security Cybersecurity Strategy', p. 12.

[86] *Ibid*.

[87] NIST, 'Cybersecurity Framework', <https://www.nist.gov/industry-impacts/cybersecurity-framework>, accessed 8 June 2020.

[88] Secretariat of the Security and Defence Committee of Finland, 'Finland´s Cyber Security Strategy', p. 8.

[89] Ministry of the Interior of Iceland, 'Icelandic National Cyber Security Strategy 2015–2026', p. 10.

[90] DHS, 'US Department of Homeland Security Cybersecurity Strategy', p. 20.

incident response and securing the current technology in CNI? Are there methods of embedding cyber security as infrastructure digitalises, balanced with the need to innovate at pace?

VI. Public–Private Partnerships and Responsibility

EFFECTIVELY CAPITALISING ON public–private partnerships to meet the objectives or vision of the overall strategy is challenging. The relationship between the private sector and government is pivotal in delivering an impactful strategy.[91] Responsibility and public–private partnerships are approached differently across NCSSs. Each country has its own view of how to assign responsibility, and the kind of engagement via which this should be done. Public–private partnerships can also be called different names and vary widely dependent on the country.[92] This chapter is a snapshot of the potential policy areas and formats for these partnerships.

There are often assertions that national cyber security cannot be achieved without galvanising different parts of society to act.[93] However, to date, 'the reluctance of politicians to claim authority for the state to introduce tougher cyber-security measures by law, coupled with the private sector's aversion to accepting responsibility or liability for national security, leaves the "partnership" without clear lines of responsibility or accountability'.[94] The notion of 'responsibility' may also be problematic for the private sector if the development stages of the NCSS failed to consult and understand the parameters of current private sector accountability. This can then impact the behavioural levers that encourage action.[95] This accountability can involve a broad range of stakeholders for the private sector, including investors or shareholders, auditors, insurers and board members. According to ENISA, the main driving forces behind the creation of public–private partnerships are economic interests, regulatory requirements, public relations and social interests.[96] Using these levers can help build effective partnerships with engaged stakeholders.

Clear strategies can be a conduit for communicating to the private sector what is expected of them and how to work towards that collectively. It can also explain what the role of government is in supporting private sector involvement.

Often, responsibilities are tied closely to a government's view of what the strategy is trying to achieve. Norway's NCSS, for example, identified one potential area of public–private partnership:

[91] ITU, 'Guide to Developing a National Cybersecurity Strategy', p. 23.

[92] *Ibid*., p. 5.

[93] *Ibid*., p. 24.

[94] Madeline Carr, 'Public–Private Partnerships in National Cyber-Security Strategies', *International Affairs* (Vol. 92, No. 1, 2016), p. 43.

[95] *Ibid*.

[96] ENISA, 'Public Private Partnerships (PPP) Cooperative Models', November 2017, p. 11.

digital innovation. The government sees the development of technology as a part of improving cyber resilience, while the private sector can recognise a mutual aim to strive for innovation. To this end, Norway's strategy also outlines what responsibility Norwegian companies have and that they 'take responsibility for handling cyber-attacks targeted at their own business and for sharing information about these with the authorities and other relevant actors'.[97] This framework both engages with the private sector and provides structure around clear indications of what is expected of it.

The Latvian NCSS, however, outlines a much more hands-off approach from government towards the private sector. The strategy includes no mention of private sector responsibility for its own systems or otherwise. This may be interpreted to mean that the Latvian government envisions providing limited support for the private sector. The strategy only discusses involving government experts in the event of a crisis.[98] This implies limited engagement with the private sector and communicates little to organisations seeking advice, support or guidance.

France's NCSS, on the other hand, takes a more complex view of what the 'private sector' means and what responsibilities they assign corresponding with the expectations they have. They split responsibilities across three communities made of different stakeholders.[99] The first community comprises researchers, product and services inventors and integrators, cyber security businesses, network operators, internet service providers and remote data-processing services. This first community is expected to build technology with secure practices. The second community – made up of elected officials, the national government, local and regional governments and trade unions – has the highest level of responsibility. They are supposed to protect France from 'digital pirates' and drive the cyber security of digital transformation by developing technical parameters and implementing cyber security policies. They must also promote national industry and, in particular, exports.[100] The final community is made up of users, 'companies' managers', citizens and participants in civil society. Their sole responsibility is to embed secure practices within their technology use and avoid 'high-risk behaviours'.[101] The strategy draws together these three communities via the concept that their responsibilities are mutually beneficial.[102]

The German NCSS views public–private partnerships differently, emphasising the value of information sharing between the public and private sectors internationally and domestically, especially in the context of cybercrime. It plans to set up institutions with industry as well as government that act in an advisory capacity.[103] The strategy considers assigning responsibilities for providers of security technology, ensuring that basic products are available to users and small and medium-sized enterprises (SMEs) at the least. In addition, the German strategy

[97] Government of Norway, 'National Cyber Security Strategy for Norway', p. 19.

[98] Government of Latvia, 'Cyber Security Strategy of Latvia 2014–2018', p. 11.

[99] French National Cybersecurity Agency, 'French National Digital Security Strategy', p. 8.

[100] *Ibid*., p. 9. The strategy does not define what 'digital pirates' are.

[101] *Ibid*. The strategy does not define what 'high-risk behaviours' entail.

[102] *Ibid*.

[103] Federal Ministry of the Interior of Germany, 'Cyber Security Strategy for Germany', p. 10.

emphasises an organisational approach by ensuring that ‘every stakeholder takes the necessary measures in its remit on the basis of the jointly developed national cyber security assessment and coordinates them with the competent authorities as well as partners from industry and academia’.[104] Germany effectively communicates how a partnership with the private sector would entail joint commitment through an assessment and information sharing.

The US has a unique approach to public–private partnerships. The White House NCSS, among other activity with stakeholders, ‘will work with the private sector to manage risks to critical infrastructure at the greatest risk’ and trusts the ‘technology market to support and reward the continuous development, adoption, and evolution of innovative security technologies’.[105] On the other hand, the DHS is the sector-specific agency for 10 of the 16 critical infrastructure sectors and the regulator for both chemical and transport sectors.[106] Specifically, its NCSS seeks to ‘partner’ with information technology, communications and cyber security providers to ‘incentivise security’, address supply chain vulnerabilities and reduce the overall level of risk.[107] These slightly different approaches to public–private partnerships, in the context of critical infrastructure, could conflict. To ensure synchronisation, information-sharing mechanisms would have to be robust internally and the agenda set for critical infrastructure risk communicated by the White House to the DHS.

Public–private partnerships and assigning responsibilities across the private sector are approached differently and can often be indicative of different domestic priorities, contrasting conceptions of the role of the state, existing engagements and resources. There is a common desire across NCSSs to draw on and enable government to work more effectively with the private sector, leveraging their expertise. Further questions arise from this examination. First, what are the most effective mechanisms of incentivising the private sector to take on responsibility? Second, which industries and stakeholders in the private sector are more vital to engage with, depending on the aims of the strategy?

Partnerships, however, cannot exist without exceptional talent in the private sector and across many public sector roles. Many states are aware of the need to have a good level of cyber awareness across society in general and a strong pipeline of talent to fulfil critical cyber roles. In the next chapter, capacity building – in the form of general cyber literacy and awareness, cyber skills, and research and innovation – is examined.

[104] *Ibid.*, p. 8.

[105] White House, ‘National Cyber Strategy of the United States of America’, pp. 8, 14.

[106] *Ibid.*, p. 14. The 16 sectors are: chemical; commercial facilities; communications; critical manufacturing; dams; defence industrial bases; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors; material; and waste, transportation, water and wastewater systems.

[107] *Ibid*., p. 23.

VII. National Cyber Security Capacity Building

AN NCSS REQUIRES a significant amount of awareness, skills and innovation to be fed into the national effort in order to build resilience. Throughout the 22 strategies analysed for this research, capacity building remained a central goal. Cyber literacy concerns the overall awareness of cyber security across a group of people, or the whole of society across every age or demographic group. The cyber careers section refers to the initiatives countries pursue to increase the number of talented professionals entering the industry. Finally, innovation in cyber security refers to the national cyber security industry and the number of new entrants in the market providing innovative solutions to cyber security issues. This has a dual benefit in that the growth of cyber security start-ups is good for the national economy.

National Cyber Literacy

Raising the level of personal cyber hygiene is a common goal in NCSSs. Governments cannot realistically be responsible for the security of every user in the country. However, they can seek to educate their citizens in best practices and behaviours. Generally raising the cyber literacy of the population raises the overall resilience of the country. There are significant cognitive and practical barriers to encouraging citizens to adopt secure behaviours. Much behavioural analysis has been done on how to encourage secure user behaviours, but it remains a policy challenge.[108] Within the 22 strategies examined for this research, there were some varied approaches to behavioural campaigns.

A novel approach in Austria's NCSS was to focus on the cyber literacy of SMEs. Specific, but undefined, sectors will benefit from 'governmental cross-sectoral cyber exercises upon request'.[109] Furthermore, an ICT Security Internet Portal, coordinated by the Ministry of Finance, the Federal Chancellery and Secure Information Technology Centre Austria, will serve as an information and communication hub for awareness-raising measures.[110]

[108] Rachid Ait Maalem Lahcen et al., 'Review and Insight on the Behavioral Aspects of Cybersecurity', *Cybersecurity* (Vol. 3, No. 10, 2020); Benedikt Lebek et al., 'Information Security Awareness and Behavior: A Theory-Based Literature Review', *Management Research Review* (Vol. 37, No. 12, 2014), pp. 1049–92.

[109] Government of Austria, 'Austrian Cyber Security Strategy', p. 14.

[110] *Ibid.*; Lee Hadlington, 'Employees Attitude Towards Cyber Security and Risky Online Behaviours: An Empirical Assessment in the United Kingdom', *International Journal of Cyber Criminology* (Vol. 12, No. 1, 2018), p. 278.

Embedding secure behaviours within a workforce may lead to secure behaviours in the broader life of employees. However, there are variables that affect the likelihood of impact on awareness campaigns. In one study, results found that older people typically demonstrated a more receptive and positive attitude to cyber security.[111] This leads to uncertainty when running awareness campaigns as to whether they are impactful, targeted at the intended recipient and provide well-communicated benefits. The following NCSSs endorse running national awareness campaigns for the whole of society in an attempt to overcome these challenges.

As part of France's NCSS, the Ministry of National Education, Higher Education and Research, the State Secretariat for Digital Technology, with assistance from the government's Information Department and the National Agency for Information Systems Security, are committed to running a campaign on an awareness programme for professionals alongside a host of activity on national cyber awareness.[112]

Greece's strategy, on the other hand, stipulates that the National Cyber Security Authority will design and implement their national campaign and use other ministries to target different age groups. For instance, the Ministry of Education will be used for campaigns in primary and secondary schools. The country's National Cyber Security Authority will also organise, in partnership with universities, 'educational activities' for people, promoted through websites.[113] Like Greece, Croatia's NCSS targets school curriculums with cyber awareness campaigns as well.[114] Embedding secure behaviours at a younger age is deemed to be an efficient way to ensure future levels of cyber literacy.

Finally, Iceland's NCSS seeks to enhance the general cyber literacy of the Icelandic population to tackle cybercrime and embrace existing international sources of cyber security education.[115] Instead of creating their own novel approach to awareness raising, Iceland implicitly recognises that by using existing approaches, they reduce the amount of work needed and importantly, take best practice guidance and materials from other states.

Cyber Security Careers

With some estimating the global cyber workforce gap at approximately 4 million professionals,[116] cyber security careers are a key focus of capacity building within NCSSs. They appear in almost every one of the 22 strategies analysed for this research. The large number of stakeholders involved in delivering cyber careers information and skilling to different age groups, and the formats used to deliver the information, result in a complex mix of resources, actions and commitments.

[111] Hadlington, 'Employees Attitude Towards Cyber Security and Risky Online Behaviours'.

[112] French National Cybersecurity Agency, 'French National Digital Security Strategy', p. 26.

[113] Government of Greece, 'National Cyber Security Strategy: Version 3.0', p. 12.

[114] Government of Croatia, 'The National Cyber Security Strategy of the Republic of Croatia', 2015, p. 7.

[115] Ministry of the Interior of Iceland, 'Icelandic National Cyber Security Strategy 2015–2026', p. 12.

[116] ISC2, '(ISC)2 Finds the Cybersecurity Workforce Needs to Grow 145% to Close Skills Gap and Better Defend Organizations Worldwide', 6 November 2019.

For some, the pathway to moulding and shaping talent is unclear. The Czech Republic's NCSS provides a general acknowledgement that the problem exists. It admits that the existing higher, secondary and primary education system is not able to meet the standard to provide cyber security education. However, it also acknowledges that the demand for cyber professionals remains high and therefore action should be taken.[117]

Australia's 2020 strategy will create a Cyber Security National Workforce Growth Program to 'encourage businesses and academia to partner together to find innovative new ways to improve cyber security skills'.[118] The programme includes a wealth of activity including: scholarships; apprenticeships; specialist cyber security courses for professionals; retraining initiatives; training or professional development for teachers and board executives; internships; cadetships; staff exchanges; digital training platforms; and student-delivered cyber security services.[119] They will also look to embed cyber security in other professions, such as engineering or data science.

There are several strategies that target schools in particular. Ireland's NCSS combines approaches from three separate government documents: the NCSS; Future Jobs Ireland; and Technology Skills 2022. In doing so, Ireland hopes to build on current programmes and work with bodies such as Skillnet Ireland (aimed at private industries) and the Science Foundation Ireland (careers advice to schools) to implement apprenticeships, skills opportunities and further computer science training in schools.[120]

The Netherlands's NCSS views cyber security education within a wider framework of digital skills, which are the main focus of a review of the primary and secondary education curricula.[121] Kennisnet ('Knowledge Net'), funded by the Ministry of Education, Culture and Science, will support the review into the curriculum. Similarly, Austria views cyber security as part of the ICT curriculum in schools. It will focus on 'new media literacy', but it is unclear what this means.[122]

With a particular focus on university-level education, Iceland's NCSS stipulates that students achieving firsts in their undergraduate degrees will have access to postgraduate courses in cyber security, therefore meeting the pre-requisites required to take courses in other Nordic states. They further suggest that cyber security will be embedded in all 'computer-related studies' at schools.[123]

[117] National Security Authority of the Czech Republic, 'National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020', p. 15.

[118] Government of Australia, 'Australia's Cyber Security Strategy 2020', p. 33.

[119] *Ibid*.

[120] Government of Ireland, 'National Cyber Security Strategy 2019–2024', p. 38.

[121] Ministry of Foreign Affairs of the Netherlands, 'National Cyber Security Agenda', p. 40.

[122] Government of Austria, 'Austrian Cyber Security Strategy', p. 15.

[123] Ministry of the Interior of Iceland, 'Icelandic National Cyber Security Strategy 2015–2026', p. 9.

The US White House NCSS aims to work with Congress to provide opportunities in re-skilling people from different backgrounds and work on the National Initiative for Cyber Security (NICE). However, there appears to be little emphasis on working with private sector stakeholders.[124]

Skills building is approached from many angles. National strategies must be cognisant of the commitment to skills building as a long-term investment and not a short-term gain.

Innovation, R&D and Sector Growth

Cyber security innovation is a priority for industry and national security. In order to remain ahead of the next vulnerability and economically benefit from the growth of the cyber security sector, promoting it can be a challenging option. Recent reporting suggests that key drivers in sector growth – venture capitalists – are reducing the amount of investment in cyber security companies in the US.[125] This suggests that market drivers may not be reliable in growing the industry alone. Government intervention in research and development and promoting growth in the sector is an option if market forces struggle but can be a challenging path to take because of the high failure rate of start-ups.[126] The following states all intervene to varying extents.

To speed up ‘go to market’ times, the Austrian NCSS places emphasis on rapidly turning research and development projects into marketable services or products. They already have an established programme with some research projects and have committed to developing them further.[127] Similarly, the Czech Republic’s NCSS seeks an overall increase of investment in research and development, although it remains unclear how this will be achieved.[128]

Setting up centres of excellence through a hybrid university and industry collaboration is a common approach. Finland’s NCSS is to set up an innovation centre of excellence under the already established hub, ‘ICT SHOK’.[129] Greece’s strategy is to focus on academic centres of excellence, highlighting the value they bring in tackling an ever-evolving environment.[130] A similar research-based approach is supported by Ireland’s NCSS. The Science Foundation Ireland leads the SFI Research Programme and the Research Centre Spoke programme, which they will explore in setting up an initiative in cyber security research.[131]

[124] White House, ‘National Cyber Strategy of the United States of America’, p. 17.

[125] Jeff Stone, ‘Venture Funding in Security Startups Is Falling. Don’t Blame the Coronavirus’, *Cyber Scoop*, 19 March 2020.

[126] Neil Patel, ‘90% Of Startups Fail: Here’s What You Need to Know About the 10%’, *Forbes*, 16 January 2015.

[127] Government of Austria, ‘Austrian Cyber Security Strategy’, p. 15.

[128] National Security Authority of the Czech Republic, ‘National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020’, p. 19.

[129] Future Internet, ‘Finnish ICT SHOK Programme’, <http://www.futureinternet.fi/>, accessed 8 June 2020.

[130] Government of Greece, ‘National Cyber Security Strategy: Version 3.0’, p. 13.

[131] Government of Ireland, ‘National Cyber Security Strategy 2019-2024’, p. 38.

The US largely relies on market forces to drive innovation. The White House's NCSS seeks to 'prioritise innovation' by updating guidance and standards continuously to ensure the implementation of the latest information. They state they will work with the private sector to innovate beyond current technology but expect the marketplace to evolve and innovate.[132]

National cyber capacity building in the NCSSs explored in this paper is approached through three dimensions: cyber literacy or awareness; cyber security skills building; and cyber innovation and development. Countries are aware of their need to ensure capacity building remains a priority within national cyber strategies as future industry relies on it. However, further questions arise. Notably, in enhancing the cyber literacy of societies, is there sufficient emphasis on a behavioural approach to embedding good security practices? In cyber skills, which pathway through education is most effective at producing cyber talent? Is it through universities or through apprenticeships? Finally, in cyber innovation, is the private sector aligned with governments in their innovation goals?

[132] White House, 'National Cyber Strategy of the United States of America', p. 14.

Conclusion and Implications

THIS PAPER EXAMINES 22 strategies to provide some context for policymakers and display some of the trends and approaches that have emerged. In doing so, the research team has identified six recurring policy challenges that should be considered when developing a new UK NCSS. Several questions naturally arose from each policy area examined throughout the paper. These relate to context around the approaches and the practicality of implementing them, and may help with thinking about next steps when devising a future strategy.

Strategic Objectives

- What is the role of government in raising cyber resilience? Does it align with the national values of the country (for example, empowering stakeholders to improve their own cyber security)?
- Can a strategy's aims be realised within the timeframe it has been given and, if not, should the timeframe be reconsidered?
- Do the objectives encompass a whole-of-society approach to cyber security?

National Threat Perception

- How do countries prioritise threats?
- How much does national threat perception influence the strategic objectives of a country's NCSS?

Tackling Cybercrime

- What data is the most important to collect, and what does a data-driven law enforcement response consist of?
- Is there currently sufficient cooperation between countries in tackling cybercrime?
- Should national strategies outline how they will work bilaterally and multilaterally with other states when talking about cybercrime?

Critical National Infrastructure

- What is the potential for further policy development outside incident response and securing the current technology in CNI?
- Are there methods which balance the need to embed cyber security as infrastructure digitalises with the need to innovate at pace?

Public–Private Partnerships and Responsibility

- What are the most effective mechanisms of incentivising the private sector to take on responsibility?
- Which industries and stakeholders in the private sector are vital to engage with, in line with the aims of the strategy?

Capacity Building

- Is there sufficient emphasis on behavioural approaches to embedding good security practices across society?
- Which education pathway is most effective at producing cyber talent?
- Is the private sector aligned with government in their innovation goals?

These questions are merely a snapshot of the complexity involved when formulating an NCSS. They will inform the analysis of a forthcoming paper on a future UK NCSS, and provide an international context to the issues the UK faces. The questions also highlight areas of research to explore and considerations that the UK could learn from as it formulates its new cyber strategy for 2021 and beyond.

About the Author

Sneha Dawda is a Research Analyst in RUSI's Cyber Security research programme. She specialises in national cyber security strategies, internet governance, critical national infrastructure vulnerabilities and cybercrime.