THE FUTURE NATIONAL CYBER SECURITY STRATEGY: DEFENDING VALUES IN CYBER

BY DR DANNY STEED

HJS
Henry
Jackson
Society

DEMOCRACY | FREEDOM | HUMAN RIGHTS

CENTRE ON CYBER SECURITY AND ONLINE THREATS

June 2021

Published in 2021 by The Henry Jackson Society

The Henry Jackson Society
Millbank Tower
21-24 Millbank
London SW1P 4QP

Registered charity no. 1140489
Tel: +44 (0)20 7340 4520

www.henryjacksonsociety.org

The views expressed in this publication are those of the author and are not necessarily indicative of those of The Henry Jackson Society or its Trustees.

Title: “THE FUTURE NATIONAL CYBER SECURITY STRATEGY: DEFENDING VALUES IN CYBER”
By Dr Danny Steed

ISBN: 978-1-909035-67-6

£9.95 where sold

Front Cover: Map of the United Kingdom indicating a connected web (https://www.shutterstock.com/image-illustration/map-united-kingdom-indicating-connected-web-1717777330).

THE FUTURE NATIONAL CYBER SECURITY STRATEGY: DEFENDING VALUES IN CYBER

BY DR DANNY STEED

HJS
Henry
Jackson
Society

DEMOCRACY | FREEDOM | HUMAN RIGHTS

CENTRE
ON CYBER
SECURITY
AND ONLINE
THREATS

June 2021

About the Author

Dr Danny Steed is a research fellow who is particularly engaged in the Henry Jackson Society's Centre on Cyber Security and Online Threats. Previously Danny was Lecturer in Strategy and Defence at the University of Exeter, where he created and delivered numerous courses specialising in national security strategy to student, professional, and military cadres.

Danny has also worked in UK government service in an operational cyber security capacity. Since then, Danny has been in private industry as a Head of Strategy. During that time, he avidly continued his own scholarship, as a visiting fellow to both the University of Cranfield and the Cyber Norms Program at the University of Leiden in 2019, and continuing to contribute to taught courses, publications and academic events.

Frequently requested as a public speaker, Danny's most notable keynote address was delivered at the Dutch government's *One Conference 2019* in The Hague, where he spoke on the future generations of cyber security strategies.

He is the author of two books, *British Strategy and Intelligence in the Suez Crisis*, and *The Politics and Technology of Cyberspace*, published by Palgrave in 2016 and Routledge in 2019 respectively.

Acknowledgments

The author wishes to give thanks on behalf of the Henry Jackson Society for the generosity and input of the following people: Dr Jade McGlynn, Dr Joe Devanny, Eilish O'Gara, Jack Capizzi, Mart Viires at the Estonian Embassy in London for facilitating the interview with representatives of the Estonian Ministry of Foreign Affairs, and Ozaki Koichi at the Japanese Embassy in London for facilitating exchanges with the Japanese Ministry of Foreign Affairs.

Contents

About Us

HJS
Henry
Jackson
Society

DEMOCRACY | FREEDOM | HUMAN RIGHTS

About The Henry Jackson Society

The Henry Jackson Society is a think-tank and policy-shaping force that fights for the principles and alliances which keep societies free, working across borders and party lines to combat extremism, advance democracy and real human rights, and make a stand in an increasingly uncertain world.

CENTRE
ON CYBER
SECURITY
AND ONLINE
THREATS

About the Centre on Cyber Security and Online Threats

The **Centre on Cyber Security and Online Threats** is a bold, policy-focused, international research centre, which seeks to provide contrarian policy options that safeguard a free and open cyberspace, and help challenge online threats to liberal Western democracies.

Cyberspace is one of the liberal world's greatest gifts to humanity, yet it also poses numerous security challenges from the international level down to each and every individual walking the planet. This Centre's purpose is to challenge the policy thinking of liberal democratic governments to engage cyberspace as one of the 21st century's central geopolitical challenges, and to robustly engage the vision and actions of authoritarian exploitation of technology.

Executive Summary

- Of all the UK's National Cyber Security Strategies to date, this year's comes at a time of heightened challenges, both from the world of cyber itself as well as from the UK's own political context.
- The *Integrated Review* is correct in its broad political direction for the UK but is ultimately lacking in the detail required to bridge policy desire with achievable actions.
- The vision of future UK national security from the *Integrated Review* is very technology-centric, with cyber interweaved throughout.
- The pursuit of national domestic resilience is a necessary, but not sufficient, condition to ensuring a free, open, peaceful, and secure cyberspace.
- The UK's true cyber security challenges lie in its international politics, where there are significant problems and opportunities. Addressing these is far less about technology than it is about imaginative policy actions.
- The next National Cyber Security Strategy must, above all, put internationalism at its heart. This is a moment when the UK can become a global leader by shaping the future of cyberspace into the free and open vision so cherished by democratic nations. But that moment must be seized, for external challenges to this vision are mounting.
- This report offers a series of tangible recommendations that should be considered within the remit of the next National Cyber Security Strategy.

Introduction

As the UK approaches the eve of its fourth generation National Cyber Security Strategy (NCSS), it does so at a time of arguably unprecedented challenge. Since the last strategy in 2016, the global financial losses to cybercrime have grown each year. [1] In 2017, the world witnessed the first global ransomware attacks with WannaCry and NotPetya. The attackers were armed with zero-day exploits stolen from a Western intelligence agency which they then unleashed back on the world, causing tens of billions of dollars damage to businesses. In the past six months alone, the world's fears about supply chain security were confirmed by the hacking of SolarWinds' Orion software – infecting tens of thousands of organisations worldwide – and the breach of the Microsoft Exchange servers.

Politically, things have changed for the UK as well. The last strategy was born into the immediate post-EU referendum context, but its focus on establishing national domestic resilience arguably incubated it from the Brexit saga. The new strategy must better address international issues on cyber security as well as fit into the evolving challenge of Britain's role outside the EU. The *Integrated Review (IR)* emerged in this same political context in March 2021, providing an outline of the UK's future vision for its national security, defence, and foreign policy.

Cyber is interwoven throughout all the main strands of the *IR*. The Government's desire to "cement the UK's position as a responsible, democratic cyber power" [2] is accompanied by descriptions of the UK's ambitions for what to do with that power. Chief among them is a wish to shape "the open international order of the future" [3] which, for cyberspace, means ensuring it continues to reflect "democratic values and interests". [4] This stems from a recognition that the rules-based international order is subject to increasing challenge, and that a "defence of the status quo is no longer sufficient for the decade ahead." [5]

While broadly correct in its overall vision of direction for the UK, the *IR* offers precious little detail of exactly how to achieve this in cyberspace, or indeed what key policy challenges to anticipate when trying to bridge policy vision into a viable strategy.[6] This report addresses these gaps in policy detail across five chapters, each of which deals with a significant cyberspace policy challenge that the UK will encounter in the coming years. Each chapter carries its own unique requirements and recommendations on how the UK can respond to challenges that no amount of national domestic resilience will solve in isolation.

Chapter one examines digital authoritarianism and its argument of Cyber Sovereignty, and outlines the growing adversarial challenge to the concept of a free and open internet. Chapter two considers the place of allies and alliances and attempts to map the key diplomatic 'battlegrounds' and possible policy actions. The third chapter focuses on challenging wrongdoing and the evolution of public attribution, taking into consideration the US-UK decision to attribute the SolarWinds hack to the Russian state. How attribution is developed in UK policy circles will greatly inform the fourth chapter, which explores how to set red

[1] Zhanna Malekos Smith and Eugenia Lostri, *The Hidden Costs of Cybercrime*, McAfee (7 December 2020), 3: Figure 1, https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf.

[2] HM Government, *Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy* (Cabinet Office, 16 March 2021), 35, https://www.gov.uk/government/collections/the-integrated-review-2021.

[3] Ibid, 18.

[4] Ibid, 55.

[5] Ibid, 11.

[6] This report subscribes to the concept of strategy as a bridging function between the worlds of policy and action. "Strategy is the only bridge built and held to connect policy purposefully with the military and other instruments of power and influence." (Colin S. Gray, *The Strategy Bridge: Theory for Practice* (Oxford: Oxford University Press, 2010), 262.).

lines in UK policy. Here, I examine the concept of deterrence with the aim of elucidating the best methods for setting political red lines in cyberspace – a task that has proven difficult to superimpose over traditional concepts of deterrence thinking.

The final chapter examines how achieving the vision of 'Global Britain' can be best served by the UK's nascent development as a leading cyber power. This is about how the UK crafts its operating concepts and its doctrine for cyber power itself, as well as whether elements of cyber security remain over-classified and outside public debate. Realising the UK's vision of becoming a responsible democratic cyber power depends first on the UK answering the question of its post-Brexit place in the world. Secondly, it depends on how the UK can develop its cyber power as a tool of statecraft to protect and promote a free, open cyberspace through influence, not force.

Chapter 1 – Digital Authoritarianism and Cyber Sovereignty

Establishing a robust defence of liberal values in cyberspace must begin by: a) recognising that there is an active geopolitical contest between different states; and b) identifying which countries play an adversarial role to the West in this contest. [7] This is a position that was an enduring and obvious reality by the time the 2020s had begun, as reflected by the Ministry of Defence's (MOD) *Cyber Primer*, which states that "Cyberspace is permanently contested by our adversaries". [8]

The recent *IR* reiterated this view, recognising that: "There will be a struggle to shape the global digital environment between 'digital freedom' and 'digital authoritarianism'." [9] Yet, while acknowledging the general challenges posed by Russia [10] and also by China, as a "systemic competitor", [11] the *IR* fails to openly name or challenge the Cyber Sovereignty movement. For almost a whole decade, the Russian and Chinese governments have been increasingly active in developing Cyber Sovereignty, the clearest political manifestation of digital authoritarianism. This report calls for a clear acknowledgement in the next NCSS that the Cyber Sovereignty movement is a direct adversarial position to the vision of a "free, open, peaceful and secure cyberspace" [12] as articulated in the *IR*.

What is Cyber Sovereignty?

In a speech to the Second World Internet Conference in 2015, President Xi Jinping of China provided a working definition of Cyber Sovereignty:

> We should respect the right of individual countries to independently choose their own path of cyber development, model of cyber regulation and internet public policies, and participate in international cyberspace governance on an equal footing. No country should pursue cyber hegemony, interfere in other countries' internal affairs, or engage in, connive at or support cyber activities that undermine other countries' national security. [13]

Cyber Sovereignty is the clearest outward expression of the "digital authoritarianism" referred to in the *IR*. It is opposed to the notion of a free and open cyberspace – "The Free Internet Coalition" [14] as Alexander Klimburg refers to such nations – through a series of clear beliefs that can be deduced from Xi Jinping's remarks:

- A rejection of the multi-stakeholder governance model in favour of state-centric approaches.
- An assertion of non-interference in internal affairs that extends to media coverage and external criticism.

[7] Defining the 'West' is of course a perilous exercise with a vast literature devoted to it that is beyond the scope of this report to engage. Suffice to say here that this report accepts McNeill's caution that what the West means "depends entirely on who is invoking the term and for what purpose." However, to offer a tangible subscription that this report adheres to is Emmott's concept that what is shared among the West is a unifying idea centred on "liberalism" or "liberal democracy" based on two crucial ideas: openness and equality. (William H. McNeill, "What We Mean by the West," *Orbis* (Fall 1997), 514, and Bill Emmott, *The Fate of the West: The Battle to Save the World's Most Successful Political Idea* (London: Profile Books, 2017), 10-14.).

[8] Ministry of Defence, *Cyber Primer: Second Edition* (Swindon: Development, Concepts and Doctrine Centre, 2016), 21.

[9] HM Government, *Integrated Review* (2021), 29.

[10] Ibid, 61.

[11] Ibid, 26.

[12] Ibid, 56.

[13] "Remarks by H.E. Xi Jinping, President of the People's Republic of China, at the Opening Ceremony of the Second World Internet Conference," 16 December 2015, https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml.

[14] Alexander Klimburg, *The Darkening Web: The War for Cyberspace* (London: Penguin Press, 2017), 16.

- An opaque interpretation of national security designed to reinforce non-interference in internal affairs.

As Gordon Corera has argued, the Chinese Government betrays the paranoid motivation that internet freedom "is simply the freedom to be spied on and exploited by the US and its companies."[15] Reference has been routinely made to Edward Snowden's leaks about US–UK intelligence surveillance operations in 2013 as justification for such a view, reminding the international community that it was Western intelligence agencies that were first caught carrying out bulk digital surveillance operations. The Snowden leaks were even cited in a May 2021 interview with Sergei Naryshkin, the Director of Russia's Foreign Intelligence Service (SVR), in response to the attribution of the SolarWinds hack to the SVR.[16]

How does Cyber Sovereignty work?

Cyber Sovereignty subverts the very discourse of cyber security by appropriating terms and extending their interpretation to suit national interests. There are two ways that this is demonstrated in practice. First, Jon Lindsay asserts that the Chinese Government's conception of information security emphasises internet *content* on an equal footing with technical network security.[17] This is a clear indicator of the authoritarian need to establish uncontested control over information among its populace; the recent ban of the BBC World Service for its coverage of coronavirus and Uighur persecution is the clearest example of such a belief put into action.[18]

Second, it is important to note that the Chinese Government harbours a more expansive view of the word "sovereignty" than Western nation-states, whose Westphalian concept[19] differs to that established by Gordon Barrass and Nigel Inkster. Barrass and Inkster's translation of the word sovereignty in Chinese – *zhu quan* – carries strong connotations to the much older Chinese concept of 'mandate of heaven'. Therefore, for the Chinese Government, sovereignty could not be more different to the Westphalian concept, as it is "not about sharing power, but about the Chinese government being the uncontested sovereign in its own 'world'."[20]

Cyber Sovereignty is presented as a seemingly innocuous request to respect a nation's integrity. In reality, it is an assertion of absolute sovereignty, reinforced by censorship, bans, and the need to do what all authoritarians must: ensure regime stability by preventing dissent from within and without. Cyber Sovereignty presents nothing less than a geopolitical challenge, an adversarial contest, to the multi-stakeholder model of internet governance and a free and open cyberspace. Lukas Kello is correct to argue that a "sovereignty gap"[21] exists in cyberspace, but there are radically different perspectives between democratic and authoritarian nations as to how to address the systemic challenges cyberspace has brought to society. To digital authoritarians, building closed systems protected by absolutist views of sovereignty is the answer. The risk is articulated in an interview this author carried out with representatives of the Estonian Ministry of Foreign Affairs (MFA) based in Tallinn, who described how: "So-called Cyber Sovereignty would allow authoritarian control over the internet, legitimise state

[15] Gordon Corera, *Intercept: The Secret History of Computers and Spies* (London: Weidenfeld & Nicolson, 2016), 267-268.

[16] "SolarWinds hack: Russian denial 'unconvincing'," *BBC News*, 18 May 2021, https://www.bbc.co.uk/news/technology-57156197.

[17] Jon R. Lindsay, "Introduction – China and Cybersecurity: Controversy and Context," in *China and Cybersecurity: Espionage, Strategy and Politics in the Digital Domain*, ed. Jon R. Lindsay, Tai Ming Cheung and Derek S. Reveron (Oxford: Oxford University Press, 2015), 13.

[18] "China bans BBC World News from broadcasting," *BBC News*, 12 February 2021, https://www.bbc.com/news/world-asia-china-56030340.

[19] The territorial, sovereign state is traditionally dated from 1648's Peace of Westphalia, "the collective term for the peace treaties that drew an end to the Thirty Years War in Europe and heralded the formal beginning of the modern European states system." (Peter Sutch and Juanita Elias, *International Relations: The Basics* (Abingdon: Routledge, 2007), 6.).

[20] Gordon Barrass and Nigel Inkster, "Xi Jinping: The Strategist Behind the Dream," *Survival* 60:1 (2018): 51.

[21] Lukas Kello, *The Virtual Weapon and International Order* (New Haven: Yale University Press, 2017), 254.

surveillance and censorship, and hinder democratic processes."[22] To democratic nations, multi-stakeholderism, greater cooperation and openness are key not only to securing cyberspace on a technological level, but also to developing acceptable behavioural norms. The differences could not be clearer.

The logical extension of Cyber Sovereignty is to undo decades of governance that enables the free movement of data based on universal, shared technical standards. This is a view that lends increased credence to Parag Khanna's "Connectography" argument, according to which information has not only migrated to the digital world, but so has geopolitics. In Khanna's view, geopolitics now plays out less in territorial conquest "and more in the matrix of physical and digital infrastructure."[23] UK policymakers need to acknowledge and confront the geopolitical challenge presented by digital authoritarianism.

Recommendation 1 – Explicitly declare UK opposition to Cyber Sovereignty

The next NCSS should expand upon the concept of digital authoritarianism outlined in the *IR* by targeting its clearest political manifestation, Cyber Sovereignty. By declaring Cyber Sovereignty to be a directly adversarial position to the notion of a free and open internet, the UK can then direct policy options and diplomatic efforts towards a coherent objective: countering the Cyber Sovereignty argument. The UK's arguments for a free and open internet have been lacking in detail and rigour, allowing space for Cyber Sovereignty to gain traction. It is time for the UK to explicitly acknowledge the adversary and aggressively challenge the narrative.

[22] Interview carried out by Dr Danny Steed with representatives of the Estonian Ministry of Foreign Affairs (MFA) in Tallinn (13 April 2021).

[23] Parag Khanna, *Connectography: Mapping the Future of Global Civilisation* (Manhattan: Random House, 2016), 29.

Chapter 2 – Allies and Alliances

The 2016-2021 NCSS contained a declared set of objectives in the international arena, including aims to "champion the multi-stakeholder model of internet governance; oppose data localisation; and work to build the capacity of our partners…" [24] Although there has been some progress, it must be recognised that British efforts internationally did not receive the attention they needed because Brexit dominated the political agenda.

During these five years, the international arena in cyberspace itself did not develop in ways that suit the interests of democratic nations. Numerous data localisation laws were passed worldwide, [25] and the main forum for government discussion on the use of Information and Communications Technologies (ICTs), the UN Open-Ended Working Group (OEWG) and Government Group of Experts (GGE), failed to reach a consensus in 2017. This failure effectively stalled progress in international cyber diplomacy; as Dennis Broeders has argued, "there has not been a consensus report in the UN on cyber since 2015, and cyber years are long." [26] Encouragingly, however, the Open-Ended Working Group has reconvened, covering subjects such as threats, international law, norms, confidence-building measures, capacity building and regular institutional dialogue within the 2021 proceedings. [27] Therefore, even if consensus has stalled, multilateral dialogue continues.

Since the last GGE consensus report, the world has seen an escalating list of cyber incidents by actors shaping norms of behaviour for the worse. These include interference in the 2016 US Presidential election, global ransomware campaigns in WannaCry and NotPetya in 2017, year-on-year increases in financial losses to cybercrime, and, in the recent SolarWinds and Microsoft Exchange Server hacks, confirmation of state actors compromising the global supply chain. Since the UK developed its last strategy, the number and scale of risks and incidents taking place has outmatched diplomatic efforts to contain them. To state the position bluntly, the stakes have grown precipitously since 2015. Britain needs a 'cyber diplomacy surge' on the international arena to operationalise its intent to shape the future international order.

The *IR* displays a desire to conduct this type of diplomatic surge but offers precious little detail beyond cross-government dialogues on how the UK will "grow the international coalition" [28] needed to maintain a free and open cyberspace. What is needed – perhaps not in the strategy itself but certainly in the policy detail – is more than a mere repetition of the UK's intention to support and lead diplomatic efforts; instead, policymakers and strategists must map the diplomatic battleground for important arenas. Within this, there are three key areas towards which Britain must direct its diplomatic efforts: norms, laws, and internet governance.

As far as norms are concerned, British efforts began in 2011 under the then-Foreign Secretary William Hague's "finding the rules of the road" [29] initiative, which the UK should reinvigorate. It is telling of Britain's much vaunted soft-power influence that it was able to convene and

[24] *National Cyber Security Strategy 2016-2021*, HM Government, (2016), 63, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

[25] See Annex 1 for an example list.

[26] Dennis Broeders quoted in Emily Taylor, "A Breakthrough for U.N. Governance of Cyberspace," *World Politics Review*, 16 March 2021, https://www.worldpoliticsreview.com/articles/29496/a-breakthrough-for-global-cyber-governance.

[27] *Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, Third substantive session, Chair's Summary*, UN General Assembly (10 March 2021), https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3-technical-reissue.pdf.

[28] HM Government, *Integrated Review* (2021), 45.

[29] As outlined in his 2011 speech. William Hague, "Security and freedom in the cyber age – seeking the rules of the road," 4 February 2011, https://www.gov.uk/government/speeches/security-and-freedom-in-the-cyber-age-seeking-the-rules-of-the-road.

begin international dialogue in this arena in 2011, hosting a well-publicised London conference. Unfortunately, it failed to capitalise on this potential or to make significant progress on these issues thereafter. Since this 2011 conference, the gravity of cyber security incidents - including Stuxnet's discovery, the Saudi Aramco breach, the WannaCry and Not-Petya ransomware attacks, and now the breaches of SolarWinds and Microsoft Exchange – demonstrates that norms of behaviour have not progressed in the direction sought by liberal democratic nations. Instead, the normative behaviour that has been shaped through the decade of the 2010s has been of ever-increasing insecurity, where attacks are more brazen, the losses ever more severe, and the long-term fallout and consequences harder to quantify.

Regarding laws, a key concern is the growing list of domestic data localisation laws that other nations are enacting. [30] Britain's own *Investigatory Powers Act* [31] contains elements of data localisation requirements, but more authoritarian nations have much more stringent requirements and impose entirely different criteria upon foreign businesses operating within their country. For example, Vietnam approved their *Cybersecurity Law* [32] in June 2018, which then took effect in 2019. This law requires foreign businesses to not only store data generated within Vietnam itself, but also to establish permanent offices there. This drew protests from tech giants Facebook and Google, who did not maintain any physical office presence within the country before this law was passed.

Russia has provided perhaps the most expansive example of such legislation in the form of Federal Law No. 242-FZ, [33] which came into effect in 2015. Russian practice differs significantly in that it declares sovereignty over the data of Russian citizens no matter where that citizen is or where their data was created. This view is reflected in the legal requirement on "all domestic and foreign companies to accumulate, store, and process personal information on Russian citizens on servers physically located within Russia's borders." [34] Clearly, data localisation is in the eye of the beholder, with radically differing interpretations being imposed depending on the nation one analyses.

Therefore, it is important that the UK Government monitors the differences in how other nations or regional blocks, like the EU, impose data localisation. These will affect British nationals and businesses to varying degrees, so government support and guidance is a necessity. British policy efforts in this vein must be two-fold. First, Foreign, Commonwealth and Development Office (FCDO) embassy missions should be tasked with representing British views and objections to certain legislative parameters that may be detrimental to the rights of British nationals, expatriates, and businesses, attempting to influence such measures as far as possible. Second, the UK Government should consider providing legal advice on digital rights and business requirements for Britons and businesses seeking to travel, work, live, or do business in nations with different laws affecting digital rights. Much the same as the FCDO offers travel advice to Britons and the Department for International Trade (DIT) offers business advice, the inclusion of briefing materials and support on digital rights and responsibilities within other legal jurisdictions would go far in protecting the interests of British nationals and businesses overseas.

[30] Numerous details of this aspect were covered more expansively by this author in Danny Steed, *The Politics and Technology of Cyberspace* (Abingdon: Routledge, 2019), 70-74.

[31] HM Government, *Investigatory Powers Act* 2016, https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted.

[32] Socialist Republic of Vietnam, *Law on Cybersecurity* 2018, https://www.economica.vn/Content/files/LAW%20%26%20REG/Law%20on%20Cyber%20Security%202018.pdf.

[33] The Federal Service for the Supervision of Communications, Information Technology, and Mass Media, Federal Law No. 242-FZ 2014, https://pd.rkn.gov.ru/authority/p146/p191/.

[34] Matthew Newton and Julia Summers, "Russian Data Localization Laws: Enriching 'Security' and the Economy," The Henry M. Jackson School of International Studies, 28 February 2018, https://jsis.washington.edu/news/russian-data-localization-enriching-security-economy/.

Finally, the UK must also examine internet governance itself. Internet governance takes place across a complex web of numerous multi-stakeholder bodies, such as the Internet Engineering Task Force (IETF), the Internet Corporation for Assigned Names and Numbers (ICANN), the Internet Governance Forum (IGF) – which Japan describes as “the mechanism that best personifies internet governance through a multi-stakeholder approach”[35] – and the International Telecommunication Union (ITU). Most of these bodies have always been centred on *technical*, not *political* governance, with decisions based on consensus, not political wish. Accordingly, volunteers from strong technical backgrounds have carried out the bulk of representation.

Strategically, this renders internet governance susceptible to demographic influence, as it is a relatively small cadre of professionals who safeguard the technical standards on which cyberspace operates. It is a historical coincidence that the first generations of people leading internet governance standards were overwhelmingly from or operating in democratic nations, but representation will diversify with the influx of new cadres of technical professionals emerging from non-democratic nations.[36]

This poses an obvious challenge to ambitions to cement Britain as a leading cyber power because it presents a grassroots-level challenge to the fundamental underpinnings of cyberspace’s technical standards. So far, those standards have been – almost by default – geared towards an open internet that aims to freely share information equally across the world. With authoritarian regimes deliberately deploying technical professionals in increasing numbers, the ensuing subversion of open standards, through the internet’s own governance structures, will reduce internet freedom.

To address this, Britain needs an ambitious programme to help nurture and deploy the next generation of volunteers to ensure a permanent presence of liberal values within the structures of technical standards according to which cyberspace operates. A public–private partnership initiative akin to the National Cyber Security Centre’s (NCSC) *Industry 100* programme should be established with the aim of identifying suitably qualified technical specialists across British industry who can volunteer to participate in these essential governance mechanisms. Government efforts like the *Industry 100* have so far been aimed at supplementing British technical capability for cyber intelligence analysis or incident response; in this case, there is clear cause to develop a similar secondment programme to augment British diplomatic capability. Participation from industry will help ensure that British engineering expertise contributes to the development of internet governance mechanisms and decision making. This is a necessary foundation on which to build Britain’s aspirations to ensure a free and open internet, to shape the future international order, and to cement Britain’s role as a leading cyber power. The UK Government must take efforts to safeguard and influence the technical standards according to which the internet operates if it wishes to achieve its cyberspace aspirations.

Recommendation 2 – The UK should lead international cyber diplomacy wherever possible

This is an admittedly broad mandate, but the UK should pursue the ambitions articulated in the *IR* through energetic diplomacy. Executing a ‘diplomatic surge’ is the most feasible way to help the UK assert disproportionate influence worldwide and further develop itself as one of the world’s foremost cyber powers. Making such diplomatic efforts should be classed as a top priority for the FCDO.

[35] Email communication by Dr Danny Steed with the Japanese Ministry of Foreign Affairs (M)FA) (10 May 2021).

[36] The best singular source to highlight the dominant role of Western-based engineers, scholars and innovators is Walter Isaacson, *The Innovators: How a group of Inventors, Hackers, Geniuses and Geeks Created the Digital Revolution* (London: Simon & Schuster, 2014), especially Ch. 7 & 11.

Given that the FCDO is operating at a time of constricted human resources, resource leveraging will be essential to ensure the department can progress within cyber diplomacy. Creating a diplomatic equivalent to the *Industry 100* would augment FCDO capacity, as would seconding technical expertise from other departments to assist the FCDO during especially busy periods of cyber diplomatic activity on the international scene. The FCDO will need to find ways to augment its capacity if it is to deliver on the UK's high ambitions in cyber diplomacy.

Recommendation 3 – UK embassy missions to challenge data localisation laws

With other nations taking ever more stringent stances on data localisation laws, there is scope for the embassy missions to represent formal challenges to statutes that seek to undermine internet freedom domestically and, by extension, the free and open internet internationally. Through active and regular opposition to stringent data localisation abroad, embassy missions can align their actions to a more aggressive leadership stance in foreign policy and diplomacy, showing clear consistency in British positions on punitive legislation.

Recommendation 4 – FCDO and DIT to monitor data localisation laws

Just as the FCDO and DIT already offer guidance and advice to UK businesses and individuals travelling or working abroad, this remit should be expanded to include the restrictions on digital rights that British nationals can expect overseas. Such an extension is a logical addition to existing services that aim to support UK business growth overseas, as well as fundamentally helping to protect the rights of individual Britons abroad.

Recommendation 5 – Establish an Industry 100 for internet governance

The NCSC's *Industry 100* programme should be replicated to bolster diplomatic efforts with industry support, including by deploying seconded industry personnel for grassroots participation in basic internet governance mechanisms. With the UK Government already struggling to plug the skills gap in society, it is a logical next step to augment British diplomatic capability with industry expertise to represent the needs and views of British industry within essential internet governance forums. Long-term representation of British views in internet governance can be enhanced by an effort organised and coordinated by central government that harnesses existing industry expertise.

Chapter 3 – Challenging Wrongdoing

Attribution – as Thomas Rid and Ben Buchanan have argued – *"is what states make of it"*. [37] While technically difficult to achieve, attribution is not impossible, and is now more challenging in political terms than it is technical. Many cyber incidents in recent years have evaded public attribution not because the UK did not know who was behind them, but instead because of political hesitancy to set a precedent of attributing, especially to nation states.

Thankfully, this situation is now changing, after the US and UK governments attributed the SolarWinds hack to Russia's Foreign Intelligence Service (SVR) in April 2021. The scale of the breach to SolarWind's Orion software finally led to a decision point that could easily have been made much earlier and certainly since 2017 – specifically, when public attribution for Operation Cloud Hopper (a cyber espionage campaign against UK IP providers) was held back by the NCSC, which opted instead to allow private corporations (PWC and BAE in this instance) to attribute the incident to Chinese actors. [38]

While the NCSC attributed the 2017 NotPetya ransomware attack to the Russian state, [39] it did not impose any real costs or take any clear actions. This failure prevented the establishment of feasible and preventative red lines. The NCSC also failed to impose consequences resulting from wrongful action or to facilitate progress towards building a cyber deterrence posture that could be used in similar incidents in the future.

The improvements in recent years show that technical attribution is possible, but public attribution is still difficult to achieve politically. However, the attribution of SolarWinds is a powerful step forward in solving this challenge.

An announcement in April 2021 from the White House stated that "the United States is formally naming the Russian Foreign Intelligence Service (SVR) … as the perpetrator of the broad-scope cyber espionage campaign that exploited the SolarWinds Orion platform…" [40] The UK Foreign Secretary Dominic Raab mirrored the attribution by saying that the "UK will continue to work with allies to call out Russia's malign behaviour where we see it." [41] In contrast to the NotPetya attribution, the UK and US imposed numerous economic sanctions and diplomatic expulsions after the SolarWinds attribution.

The UK and US decision to publicly criticise Russia validates the very timely public attribution model developed by Florian Egloff and Max Smeets, who argue that public attribution "remains an unsolved issue". [42] The statements from both the US and UK indicate the need for a more coherent approach to determining not only the decision to attribute, but also the logic according to which it is declared, as well as the actions that should accompany such criticism. Egloff and Smeets' framework has five categories that serve as a worthy basis on which to consider decision making: intelligence, incident severity, geopolitics, handling, and follow-on

[37] Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks", *Journal of Strategic Studies*, 38:1-2 (2015): 7 (italics original).

[38] "Uncovering a new sustained global cyber espionage campaign," *PWC UK*, April 2017,https://www.pwc.co.uk/issues/cyber-security-services/insights/operation-cloud-hopper.html.

[39] "Russian military 'almost certainly' responsible for destructive 2017 cyber attack," *NCSC*, 14 February 2018, https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack.

[40] "Fact Sheet: Imposing Costs for Harmful Foreign Activities by the Russian Government," *The White House Briefing Room*, 15 April 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/.

[41] "Russia: UK and US expose global campaign of malign activity by Russian intelligence services," *FCDO*, 15 April 2021, https://www.gov.uk/government/news/russia-uk-and-us-expose-global-campaigns-of-malign-activity-by-russian-intelligence-services.

[42] Florian Egloff and Max Smeets, "Publicly attributing cyber attacks: a framework," *Journal of Strategic Studies* (2021): 21.

actions. [43] Yet they also provide a warning that serves to highlight the careful consideration required of UK policymakers: "Public attribution requires *consistent* goals..." [44]

The SolarWinds attribution does lack clarity in one area, namely in defining the penalty: should it align with the penalty applied for an act of espionage or the penalty for undermining democracy? Or should it incorporate both? A statement from US President Biden conflates election interference and SolarWinds, before stating that: "If Russia continues to interfere with our democracy, I'm prepared to take further actions to respond." [45] President Biden's own line lends credence to the idea that this move is actually about election interference more broadly, rather than punishment for a specific act of espionage through the SolarWinds breach. There is a concern, therefore, that the US is unclear about which actions incur which costs. Any lack of clarity inherently undermines deterrence, and could cause difficulties and confusion in affected countries, such as Russia.

UK policy will need to construct more consistent attribution goals, as the SolarWinds attribution revealed a weakness in tightly aligning the threshold crossed with actions to impose costs. Robust frameworks to assist decision makers in this regard will be needed in future; otherwise, if state attribution is made more often, inconsistencies in the UK's approach will undermine the credibility of its overall policy. Indeed, attribution is what states make of it, and this is a timely opportunity, following the SolarWinds attribution, to tighten how the UK carries out public attribution henceforth.

Recommendation 6 – Establish political thresholds for attribution

The National Security Council (NSC) and the NCSC should be charged with developing a framework for establishing political thresholds against which attribution will be made. This is a process that can be pursued either by an existing Deputy National Security Adviser or indeed the FCDO could be tasked with convening an inter-departmental working group to inform and develop such a framework. While a political choice, decision makers will need a reference framework against which incident severity can be mapped to the political thresholds that matter most to the UK. Achieving this will aid the construction of any later credible concept of cyber deterrence by properly aligning policy desire to red lines.

This recommendation is closely aligned to those developed in the following chapter on setting red lines, as the establishment of political thresholds necessarily helps to frame which red lines to declare and it also helps to inform consideration of the spectrum of available responses. Advisers must take care to ensure that the attributions and actions to impose costs follow proportionate and gradual implementation, to leave decision makers with flexibility and scope for escalation where needed.

[43] Ibid, 4.

[44] Ibid, 22 (italics original).

[45] "Remarks by President Biden on Russia," *The White House Briefing Room*, 15 April 2021, https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/04/15/remarks-by-president-biden-on-russia/.

Chapter 4 – Setting Red Lines

The setting of red lines is a key component in establishing clarity among allies and adversaries alike and these lines are the foundation for any credible notion of deterrence. This chapter will examine the flawed application of traditional deterrence theory against the challenges of modern cyber security, before arguing for a more policy-driven – rather than capability-driven – vision for deterrence.

Deterrence as a flawed concept

There is no lack of literature devoted to applying the concept of deterrence to cyber security. Yet the argument in this report is that deterrence is flawed as a concept not because of the technological dimensions of cyber capabilities and how they undermine traditional models of nuclear deterrence, but instead because of the lack of psychological clarity in deterrence positions. Lucas Kello, referring to deterrence by punishment, states: "the deterring logic of penalties is a *psychological* mechanism. It works by creating a credible expectation of intolerable losses that induces the opponent to believe that it is in his interest not to initiate an attack." [46] Simply put, deterrence works not only by holding real capability and sincere intent, but by successfully invoking a psychological change in others that forces a change in behaviour.

Deterrence operates in two main forms: deterrence by denial and deterrence by punishment. Regarding its application to cyber, the former is very intimately tied to cyber defence. "Together, they technically, financially and psychologically impose costs on potential adversaries by increasing the level of difficulty associated with penetrating computers and networks." [47] Or, in the spirit of the UK's 2016 cyber strategy, such deterrence was to "make the UK a high-cost, high-risk environment in which to operate..." [48] While efforts in the UK since 2016 have been commendable, the number, scale, and severity of cyber-attacks have consistently risen, meaning that deterrence by denial has yet to bear real fruit.

This is borne out by findings in the Department for Digital, Culture, Media and Sport's (DCMS) annual *Cyber Breaches Survey*, which revealed in its 2018 edition that – regardless of industry type – 43 percent of all UK businesses surveyed had detected a cyber-attack within the previous 12 months. In addition, 75 percent of respondents had received that most pernicious of cyber-attacks – the phishing email – in the same period. [49] In another example, the American FBI's Internet Crime Complaint Centre (IC3) detailed that global losses to one particular vector of cybercrime – Business Email Compromise (BEC) – had increased 500 percent in the period 2016-2019 compared to 2013-2016, accounting for $26.2 billion in losses. [50] Statistics abound, but the picture remains constant: since 2016, losses to cyber incidents and cybercrime have been on the rise all round.

Meanwhile, deterrence "by punishment operates at the international, national, and sub-national levels." [51] Punishments rely not only on the capability but also the credibility of one's signalling towards those to be deterred. Regardless of the credibility of one's capability and intent,

[46] Kello, *The Virtual Weapon*, 199 (italics added).

[47] Damien Van Puyvelde and Aaron F. Brantly, *Cybersecurity: Politics, Governance and Conflict in Cyberspace* (Cambridge: Polity Press, 2019), 124.

[48] The Cabinet Office, *NCSS* (2016), 48.

[49] *Cyber Security Breaches Survey 2018*, DCMS (2018), 1-4, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf.

[50] "Business Email Compromise: The $26 Billion Scam," *Federal Bureau of Investigation* (IC3), 10 September 2019, https://www.ic3.gov/Media/Y2019/PSA190910.

[51] Van Puyvelde and Brantly, *Cybersecurity*, 131.

the fundamental problem of instilling clarity in signalling fail to deter those who should be deterred. This is because the psychological point of deterrence is to deliver mutually assured – and understood – lines against which behaviours and actions will be punished. Any lack of clarity in such signalling progressively undermines deterrence, and even renders the concept itself baseless.

In essence, what is absent from British policy in cyber is less a question of whether the UK's capabilities are credible, or even if the UK lacks the will to act. Instead, the targets of the deterrence simply do not know on what bases the UK would act, because clear red lines of unacceptable behaviour have never been firmly set, only implied. It is this lack of clearly articulated red lines that the UK Government must redress in the next national strategy.

Arguably the closest the UK has come to clearly signalling its cyber deterrence intentions was when then-Prime Minister Theresa May delivered the Lord Mayor's Banquet speech in November 2017. Commenting on Russian disinformation campaigns, she stated:

> We know what you are doing. And you will not succeed. Because you underestimate the resilience of our democracies, the enduring attraction of free and open societies, and the commitment of Western nations to the alliances that bind us." [52]

However, while a signal, if the intent were to establish a basis for deterrence, the speech did not contain what is necessary to achieve it. Prime Minister May's signal in the speech did not include any specific costs, indications of credible response via established capabilities, or any articulation of exactly what Russian behaviour would be deemed unacceptable to the UK's interests.

Recommendation 7 – Establish Tier 1 Red Lines in the NCSS

The UK should clearly articulate in policy the explicit red lines that will incur the greatest costs, with the following two proposed as a start point for consideration.

Tier 1:

- Actions that interfere with and/or undermine the practice of parliamentary democracy.
- Actions that compromise the integrity and/or operations of the UK's Critical National Infrastructure (CNI).

Recommendation 8 – Convene a working group on additional tiers

A cross-departmental working group should be convened to model a series of tiered red lines and likely UK response options to cyber transgressions.

The UK needs to build a tiered approach to setting red lines in cyberspace. While the full range of tiers is a matter for further policy discussion, this report recommends immediately establishing a Tier 1 of unacceptable red lines, the crossing of which is liable to severe reciprocation, including actions outside of cyber capabilities. This should be immediately followed by considered discussion through a working group in Whitehall as to further tiers that model a spectrum of possible responses to adversarial activity in cyberspace.

Such a working group – in addition to the outlining of Tier 1 unacceptable behaviour – will go far in signalling normative developments internationally, as well as begin to bridge the gap between the UK's policy wish list and its actions in pursuing cyber deterrence to date. There will be a delicate balance in terms of what is made public and signalled publicly about the

[52] "PM speech to the Lord Mayor's Banquet 2017," *Prime Minister's Office*, 10 Downing Street, 13 November 2017, https://www.gov.uk/government/speeches/pm-speech-to-the-lord-mayors-banquet-2017.

UK's red lines versus private signalling, to ensure maximum flexibility when engaging other actors. Whatever the public–private balance ultimately is, clarity is needed first and foremost in the minds of UK policymakers. There is little evidence that this clarity exists now. To date, UK cyber deterrence internationally has failed in large measure because the UK has neglected to clearly state what it will not tolerate, and match response options with capabilities that are unambiguously signalled to adversaries.

Chapter 5 – Global Britain and Cyber Power

The *IR* has put Britain on a bold direction of travel for national security and foreign policy, yet the true policy actions for numerous areas still need to be worked out in detail. Nowhere is this truer than in the nation's next cyber strategy. Essentially, the *IR* has set a very high bar for the next NCSS if it is to achieve the UK's ambitions in cyberspace. This begs the question, in a challenging, post-EU era for Britain on the world stage, what does the Global Britain concept mean in relation to the development of UK cyber power?

Global Britain has been a relatively amorphous term, deployed since 2016 as a mechanism for discussing the post-Brexit vision of Britain's role in the world. [53] The lack of articulation until the *IR* sparked criticism from the Foreign Affairs Committee, which argued that it was a phrase that carried little tangible meaning beyond a soundbite. [54] Yet the *IR*'s insistence that Global Britain "is best defined by actions rather than words" [55] does create an opportune moment for the next NCSS to craft a vision for Britain in cyberspace that positions it as a global leader in spearheading the defence and continued expansion of the free and open internet.

Achieving such a vision that marries the upcoming NCSS with the desired vision for Global Britain would go a long way towards bridging the gap between current cyber capabilities and cementing Britain's status not only as a leading cyber power, but also as a responsible and democratic power. The stakes could not be higher – with digital authoritarianism challenging the very notion of a free and open internet through Cyber Sovereignty, and cyber incidents taking on ever greater severity, the time is ripe for the UK to display international leadership. In short, Global Britain should include cyber as a centrepiece of its internationalist efforts.

Recommendation 9 – Codify the operating concept and doctrine of cyber power

In the *IR*, the UK adopted the 2020 *National Cyber Power Index* from Harvard Kennedy School's Belfer Center for its statement that the UK is currently the third ranked cyber power in the world. [56] Yet the *IR* offered no codification or definition of cyber power beyond its traditionalist view of cyber power as "the ability to protect and promote national interests in and through cyberspace." [57] This current definition offers little of real substance to understanding and evolving a mature concept of British cyber power moving forward.

The UK needs to explicitly codify its concept and doctrine for cyber power. The building blocks on which this will be based are already evident: national domestic resilience; cyber diplomacy; and offensive cyber operations. Yet despite cyber being intimately weaved throughout the *IR*, the document fails to indicate a clear concept of cyber power status except to state that the UK enjoys this status and wishes to retain and enhance this position. Moving this from policy ambition to realisation will require a conceptual exploration to be articulated in the NCSS as to how to combine national domestic resilience, cyber diplomacy, and offensive cyber operations to protect and promote British interests in and through cyberspace.

Anything less will render the notion of cyber power little more than a concept borrowed from the scholarly world, bereft of true strategic meaning in the UK's application. Without its

[53] "Research Briefing: Global Britain," *House of Commons Library*, 6 January 2021, https://commonslibrary.parliament.uk/research-briefings/cdp-2021-0002/.

[54] Ibid, 2, footnote 2.

[55] HM Government, *Integrated Review* (2021), 14.

[56] Julia Voo et al., *National Cyber Power Index 2020: Methodology and Analytical Considerations*, Harvard Kennedy School, Belfer Center (September 2020), https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf.

[57] Ibid, 42.

own original operating concept, the use of UK cyber power risks falling prey to expedience, unguided by strategic considerations that will leave it pursuing old ground, not those areas of vital interest to the UK. Namely, there is a risk of pursuing only domestic resilience to the detriment of reshaping the international order, an ambition that lies at the heart of the *IR* and a necessary precondition for safeguarding the future of the free and open internet.

Recommendation 10 – Increase cyber security capacity building efforts overseas

The broad recommendations for cyber diplomacy were outlined in chapter two above, yet another capability that the UK can mine for diplomatic influence is to increase its efforts to build cyber security capacity. This should be included within the revised development agenda now subsumed into the FCDO from the previous Department for International Development (DfID). National resilience is a central cyber security goal for all nations, and the UK has much to export to nations seeking to gain from greater internet freedom, especially when coordinated with allied nations in other regions who share the UK's objectives in cyberspace.

With increased cyber capacity, the UK will augment its cyber diplomacy by delivering tangible outputs to other nations that will then allow these countries to develop their indigenous capabilities and grow into robust cyber security allies. In the first instance, the UK should focus on those nations and regional areas into which digital authoritarianism is encroaching, so that the UK can help protect vulnerable partners from the malign influence of authoritarians. Allied partners are already open to such activities. In an interview with the author, the Estonian MFA said that Estonia is open to pursuing greater cooperation in capacity building efforts, "particularly in the European neighbourhood, but also globally." [58] Such cooperation was mirrored by the Japanese Ministry of Foreign Affairs (MOFA), naturally with a focus "to further contribute to the peace and stability of the Indo-Pacific region…" as one of the three pillars of Japanese cyber diplomacy. [59]

Recommendation 11 – Bring the use of offensive cyber operations into public debate

While it must inevitably play a secondary role to cyber diplomacy, the place of offensive cyber operations is very important. So far, offensive cyber has remained a completely classified arena outside the scope of public debate. The stakes are far too high to risk the militarisation of cyberspace with capabilities that have not been subject to oversight in a democratic society.

While the specific capabilities and methods of offensive cyber must remain classified, we should welcome debate on exactly what the newly established National Cyber Force (NCF) will do as part of its mission focus. If actions are to be taken in a proactive, preventative manner rather than in a defensive manner, debate is a necessity. Otherwise, major precedents may occur that undermine broader efforts to safeguard the free and open internet, and risk negatively shaping international norms in cyberspace.

Offensive cyber operations have been over-classified for far too long; as the NCF is built to full operational capacity, its role and place in UK national security needs to be carefully considered in public debate. If the NCSS omits the role, activities and place of the NCF within its considerations, this will be a huge mistake on the part of the UK Government. Such a mistake risks leaving a powerful component of UK cyber power without firm alignment to established national security goals, which would risk undermining the attainment of objectives by other means.

[58] Interview carried out by Dr Danny Steed with representative of the Estonian Ministry of Foreign Affairs (MFA) in Tallinn (13 May 2021).

[59] The three pillars of Japanese cyber diplomacy are: "1) the promotion of the rule of law in cyberspace, 2) the development of confidence-building measures and 3) cooperation on capacity building…" Email communication by Dr Danny Steed with the Japanese Ministry of Foreign Affairs (MOFA) (10 May 2021).

Conclusion – Future Directions for the National Cyber Security Strategy

The UK is ready to graduate from the pursuit of national domestic resilience to a place of international leadership in shaping the future international order to secure a free and open cyberspace. Resilience must be categorised as a necessary but not sufficient requirement in protecting and promoting UK interests in and through cyberspace. Achieving cyber security cannot be a zero-sum game where one nation has it and others do not; securing cyberspace for all is the surest route not only for reinforcing resilience, but also for safeguarding a free and open internet that continues to reflect democratic values.

The challenges highlighted throughout this report – digital authoritarianism, the UK and its allies, challenging wrongdoing through attribution, establishing deterrence through political red lines, and ways to develop Global Britain in cyberspace – are all essential elements for the UK to confront in the next NCSS. While the *IR* made much of the UK's position as the world's third ranked cyber power, it offered no concrete approach for how the UK can develop into the responsible, democratic cyber power it envisions itself to be. Not only does the UK need to conceptualise this blueprint carefully, but it also needs to do so while addressing the significant external challenges highlighted in this report.

Should the UK's next strategy not directly address these areas, there are significant risks. If resilience remains the UK Government's overriding objective, then the opportunity for British international leadership will be missed at a crucial juncture, potentially allowing digital authoritarianism to gain further ground against the free and open internet. This would cement an increasingly insecure cyberspace that forces democratic nations to focus internally on damage control and become tempted to engage in securitised actions in response. As former-NCSC Chief Executive Ciaran Martin warns: "We weaponise the internet at our peril. We militarise the internet at our peril." [60]

Through this report, my primary aim has been to introduce some imaginative leaps into the minds of UK policymakers at the helm of crafting the new NCSS. Above all, the next strategy needs internationalism at its heart; previous strategies have achieved many commendable goals in addressing the skills gap and building ever stronger resilience. Yet the international situation has continued to deteriorate, and the growing threat simply outpaces what any resilience effort can match or mitigate alone. Bold UK leadership in the international policy arena is the logical next step in its cyber security ambitions; it is also a clear and present opportunity for the world's third most powerful cyber power to lead actions and dialogue in safeguarding a free and open internet for all. The 11 recommendations offered in this report – and restated below for the reader's convenience – are a modest attempt to contribute to that process.

Recommendation 1 – Explicitly declare UK opposition to cyber sovereignty

Recommendation 2 – The UK should lead international cyber diplomacy wherever possible

Recommendation 3 – UK embassy missions to challenge data localisation laws

Recommendation 4 – FCDO and DIT to monitor data localisation laws

Recommendation 5 – Establish an Industry 100 for internet governance

Recommendation 6 – Establish political thresholds for attribution

[60] Ciaran Martin, "Cyber-weapons are called viruses for a reason: Statecraft and security in the digital age" (Inaugural lecture, King's College London, November 2020), 14, https://thestrandgroup.kcl.ac.uk/event/ciaran-martin-cyber-weapons-are-called-viruses-for-a-reason-statecraft-security-and-safety-in-the-digital-age/.

Recommendation 7 – Establish Tier 1 Red Lines in the NCSS

Recommendation 8 – Convene a working group on additional tiers

Recommendation 9 – Codify the operating concept and doctrine of cyber power

Recommendation 10 – Increase cyber security capacity building efforts overseas

Recommendation 11 – Bring the use of offensive cyber operations into public debate

Annex 1 – Examples of data localisation laws worldwide [61]

Country	Legislation	Year	Proposed Legislation
Australia	Federal Privacy Act	1988	
Bangladesh	Digital Security Act	2018	
Belarus	Data Protection Law No.455-Z	2008	
Brazil	Brazilian General Data Protection Law (LGPD)	2020	
Canada	Personal Information Protection and Electronic Documents Act (PIPEDA)	1983	Consumer Privacy Protection Act (CPPA)
China	Cybersecurity Law of the People's Republic of China	2017	Personal Information Protection Law
Egypt	Personal Data Protection Law No.151	2020	
EU	General Data Protection Regulation (GDPR)	2018	
India	Information Technology Act	2000	Personal Data Protection Bill
Indonesia	Indonesia Government Regulation No. 71	2019	Protection of Private Personal Data
Israel	Protection of Privacy Law	1981	
Japan	Act on the Protection of Personal Information (APPI)	2003	Amended APPI
Mexico	Federal Law on the Protection of Personal Data held by Private Parties	2010	
Nigeria	Guidelines for Nigerian Content Development in Information and Communication Technology	2013	Nigeria Data Protection Regulation
Pakistan	Prevention of Electronic Crimes Act	2016	Personal Data Protection Bill
Philippines	Data Privacy Act	2012	
Russia	Federal Law No. 242-FZ	2014	
Singapore	Personal Data Protection Act	2012	
South Africa	Protection of Personal Information Act	2013	
South Korea	Personal Information Protection Act	2001	
Thailand	Personal Data Protection Act	2019	
Turkey	Law on the Protection of Personal Data	2016	
Ukraine	Federal Law No.2297 VI 'On Personal Data Protection'	2010	
Vietnam	Law No.24/2018/QH14 on Cybersecurity	2018	

[61] Note – this list is not exhaustive, merely indicative to highlight the range of legislative differences encountered.

Title: "THE FUTURE NATIONAL
CYBER SECURITY STRATEGY:
DEFENDING VALUES IN CYBER"
By Dr Danny Steed

The Henry Jackson Society
Millbank Tower, 21-24 Millbank
London SW1P 4QP, UK

www.henryjacksonsociety.org

HJS
Henry
Jackson
Society

DEMOCRACY | FREEDOM | HUMAN RIGHTS

CENTRE
ON CYBER
SECURITY
AND ONLINE
THREATS

June 2021