Research Paper

International Security Programme

September 2023

Offensive cyber operations

States' perceptions of their utility and risks

Juliet Skingsley

CHATHAM HOUSE

Chatham House, the Royal Institute of International Affairs, is a world-leading policy institute based in London. Our mission is to help governments and societies build a sustainably secure, prosperous and just world.

Contents

	Summary	2
01	Introduction	3
02	Perceptions of utility	7
03	Risk perception in cyberspace	14
04	Conclusion and recommendations	26
	Annex 1	31
	Annex 2	32
	About the author	33
	Acknowledgments	33

Summary

- Until recently, understanding the nature and utility of offensive cyber operations from the perspective of individual states has been hampered by high levels of secrecy. This has hindered the development of a more informed and open discussion as to how offensive cyber can be used responsibly. This paper seeks to further the conversation on offensive cyber by studying the new or revised national cyber strategies, authorization mechanisms and legislation of nine NATO states, alongside interviews with cyber experts from these states.

- In particular, how states view the utility and risks of use of offensive cyber warrants more detailed analysis, and is often missing from the broader cyber discourse. How some states perceive the utility of offensive cyber can, for example, help to inform the accuracy of the portrayal of offensive cyber capabilities as versatile 'silver bullets', providing a solution to a wide variety of challenges. Their limitations are often ignored, masking a better understanding of where the true utility of offensive cyber may lie. Generalizations also persist concerning the deterrent value of offensive capabilities. How states themselves perceive the broader utility of such capabilities is therefore important.

- Perceptions of utility are closely interlinked with perceptions of risks of use, as enthusiasm for the perceived operational versatility of offensive cyber 'tools' may serve to overshadow the equally important element of how they are used, and how states manage or mitigate risks of use. Again, this can help to inform the broader cyber discourse which remains divided over risks associated with using offensive cyber. How and at what level states authorize the use of offensive cyber operations is a key – but as yet under-studied – indicator of perceptions of risk, which can inform the degree to which some states retain concerns over the nature and the scale of risk in using offensive cyber.

- The paper concludes with seven key policy recommendations to support the responsible use of offensive cyber. It calls for states to give more detail on how they manage their deployment of offensive cyber, and it is hoped that states will continue to shed more light on these matters themselves, moving away from the historic secrecy that has clouded a more informed understanding of offensive cyber activity. It is also hoped that this focused study will contribute to the broader discussion on responsible state behaviour in cyberspace, helping states to meaningfully articulate how the development and use of offensive cyber capabilities aligns with a commitment to a secure cyberspace for all.

01 Introduction

Cyberspace has emerged as a major new domain of national and international security. Some states are now communicating more openly on their approaches to offensive cyber.

The number of public avowals by states of their intent to develop and, where necessary, use offensive cyber capabilities is on the rise.[1] A 2022 study reported that 37 states have established cyber units or commands,[2] albeit each with different mandates and composition. There may of course be more that are yet to publicly acknowledge these capabilities. 'Cyber' is also now a warfighting domain for several states, as well as for NATO.[3] States clearly recognize the importance of cyberspace as an arena of state competition, and the potential it holds for strategic gain.[4] In 2015, for example, China's State Council stated in a white paper that 'cyberspace has become […] a new domain of national security',[5] and in 2018 the commander

[1] In 2017 the US Senate Armed Services Committee reported that as of 2016 more than 30 states were 'developing offensive cyber attack capabilities'. See United States Senate Committee on Armed Services (2017), 'Joint Statement for the Record to the Senate Armed Services Committee: Foreign Cyber Threats to the United States', [Clapper, Lettre and Rogers], 5 January 2017, https://www.armed-services.senate.gov/download/clapper-lettre-rogers_01-05-17.

[2] Smeets, M. (2022), *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force*, London: Hurst, p. 27.

[3] At the 2016 NATO Summit in Warsaw cyberspace was recognized as an operational domain. See NATO Association of Canada (2016), 'NATO Adds Cyber to Operational Domain', 4 July 2016, https://natoassociation.ca/nato-adds-cyber-to-operational-domain. By 2021, at least eight NATO states had standalone cyber commands or services within their militaries: see Pernik, P. (2018), *Preparing for Cyber Conflict – Case Studies of Cyber Command*, report, Tallinn: International Centre for Defence and Security, https://icds.ee/wp-content/uploads/2018/12/ICDS_Report_Preparing_for_Cyber_Conflict_Piret_Pernik_December_2018-1.pdf.

[4] A 2021 report by the International Institute for Strategic Studies found that 'for many countries, cyber policies and capabilities have moved to centre stage in international security'. See *Cyber Capabilities and National Power: A Net Assessment*, Research Paper, London: International Institute for Strategic Studies, p. i, https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power.

[5] The State Council, The People's Republic of China (2015), *China's Military Strategy*, white paper, 27 May 2015, http://english.www.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm.

of United States Cyber Command (USCYBERCOM) remarked that 'the locus of the struggle for power has shifted towards cyberspace'.[6] In the United Kingdom, the 2021 *Integrated Review*[7] referred to the UK concept of 'cyber power'.[8]

Hyperbole and militaristic rhetoric continues to hinder a better understanding of the utility and risks of offensive cyber activity.

Yet, as Kello has found, 'there is perhaps no other domain of security in which researchers know so little about so much activity',[9] as 'much relevant cyber activity occurs beyond the ability of researchers to [analyse] or even observe'.[10] At the same time, hyperbole and militaristic rhetoric, not only on the part of the media and government officials but also within academic circles, continues to hinder a better understanding of the utility and risks of offensive cyber activity.[11] For example, the high end of the spectrum in terms of the damage and destruction that may be caused is regularly in focus, even where there is evidence that such operations are rare. This focus may also serve to overemphasize the risks of escalation and conflict (which some have argued can become a self-fulfilling prophecy) due to its simplistic nature and the ease with which it is accepted.[12] Much has been written about the 'militarization of cyberspace', but less has been said about the militarization of the conversation itself.[13] Continuing references to offensive cyber capabilities as a deterrent also persist, notwithstanding repeated challenges to the application of deterrence theory as an inappropriate and ineffective paradigm through which to inform cyber policy.[14] At the same time, the risks to international security posed by use of offensive cyber remain contested in the wider cyber discourse, with a stark divide between those who argue for cyber restraint[15] and those who advocate for cyber persistence.[16]

[6] MeriTalk (2018), 'Gen. Nakasone Lays Out Vision for "5th Chapter" of U.S. Cyber Command', 7 September 2018, https://www.meritalk.com/articles/nakasone-cyber-command-vision.
[7] HM Government (2021), *Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy*, https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy.
[8] See more at Devanny, J. (2021), 'The Review and Responsible, Democratic Cyber Power', King's College London, 11 October 2021, https://www.kcl.ac.uk/the-review-and-responsible-democratic-cyber-power#:~:text=Defining%20Responsible%2C%20Democratic%20Cyber%20Power&text=Such%20behaviour%20includes%20the%20use,public%20and%20private%20sector%20targets. Joseph Nye defines 'cyber power' as 'the ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyber domain'. See Nye, J. S. (2010), *Cyber Power*, essay, Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf, pp. 3–4.
[9] Kello, L. (2017), *The Virtual Weapon and International Order*, New Haven, CT: Yale University Press, p. 40.
[10] Ibid., p. 39.
[11] Brantly, A. F. (2020), 'Beyond Hyperbole: The Evolving Subdiscipline of Cyber Conflict Studies', *The Cyber Defense Review*, 5(3): pp. 99–120, https://cyberdefensereview.army.mil/Portals/6/Documents/2020_fall_cdr/CDR%20V5N3%2007_Brantly.pdf.
[12] Valeriano, B. and Maness, R. C. (2015), *Cyber War versus Cyber Realities: Cyber Conflict in the International System*, Oxford: Oxford University Press.
[13] For more on the use of military language in the cyber discourse and the impact it may have on cyber security strategies, see Dunn Cavelty, M. (2012), 'From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse', *International Studies Review*, 15(1), pp. 105–22, https://doi.org/10.1111/misr.12023.
[14] See more, alongside an alternative paradigm, in Fischerkeller, M. P., Goldman, E. O. and Harknett, R. J. (2022), *Cyber Persistence Theory: Redefining National Security in Cyberspace*, Oxford: Oxford University Press.
[15] Martin, C. (2020), 'Cyber-weapons are called viruses for a reason: Statecraft and security in the digital age', Inaugural Strand Group lecture at King's College London, 10 November 2020, https://s26304.pcdn.co/wp-content/uploads/Cyber-weapons-are-called-viruses-for-a-reason-v2-1.pdf.
[16] Fischerkeller, Goldman and Harknett (2022), *Cyber Persistence Theory*.

Recently, however, some states have sought to shed more light on their approaches in this area, marking an important step in lifting the veil on offensive cyber.[17] A more in-depth exploration of how some democratic states currently assess the utility and risks of their own use of offensive cyber is therefore now possible. In the author's view, these two elements of the debate are pivotal, given the divide in the discourse over escalation risks in cyberspace, and the regular – and largely untested – platitudes employed to describe the utility of offensive cyber. At the same time, the perceived utility of using or maintaining offensive cyber capabilities can inform risk appetite, so the two issues go hand in hand.

This paper therefore seeks to explore these two core issues through a series of interviews with cyber experts from nine NATO states,[18] alongside an analysis of the existing cyber literature and of national cyber strategies which have been made public. In particular, this study will also assess an important but as yet under-studied indicator: how and at what level states authorize the use of offensive cyber operations. This can help to shed light on how states perceive the risks of use.

It is hoped that this paper can serve as a resting place in which we can take stock of what we now know of these key matters at this stage in offensive cyber history, and how some states seek to manage offensive cyber activity. A study of more states also helps to broaden the debate beyond the US-centric context of much of the cyber discourse.[19] At the same time, it is hoped that states will continue to shed more light on these matters themselves, moving away from the historic secrecy that has clouded a more informed understanding of offensive cyber activity. As has been revealed in the parallel processes at the United Nations' Group of Governmental Experts (GGE) and Open-Ended Working Group (OEWG),[20] taking stock, at a given point in time, of where there are similarities in states' approaches can be instructive in revealing whether and how states have matured in identifying and addressing certain issues, and where there may be a reluctance to adapt over time. An assessment of this nature can also contribute to strengthening efforts to shape responsible state behaviour in cyberspace.

More detail on the interview process and the core question set for the interviews is included in Annexes 1 and 2. As is often the case with research papers, the interview process was at times as revealing as the answers provided. Some of the interviewees remarked how the question set had 'stretched them to their limit' in terms of considering and framing their responses, while others reported that the questions had been distributed to others in their respective departments in an effort to engender more informed discussion and consideration of the issues.

[17] For example, HM Government (2022), *UK Cyber Strategy 2022: Pioneering a cyber future with the whole of the UK*, https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022; US Cyber Command (2018), *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command*, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf; and Government of France, Ministry of the Armed Forces (2019), *Doctrine militaire de lutte informatique offensive (LIO)*, https://www.defense.gouv.fr/sites/default/files/ministere-armees/Lutte%20informatique%20offensive%20%28LIO%29.PDF.
[18] Belgium, Canada, the Czech Republic (Czechia), Denmark, Finland, Netherlands, Norway, the UK and the US.
[19] See, for example, Liebetrau, T. (2022), 'Cyber conflict short of war: a European strategic vacuum', *European Security*, 31(4): pp. 497–516 at p. 498, https://doi.org/10.1080/09662839.2022.2031991.
[20] See more at Geneva Internet Platform Digwatch (2022), 'UN OEWG', https://dig.watch/processes/un-gge.

Terminology

The author defines 'offensive cyber operations' as any cyber activity which can have an effect on a computer system or network, or the information held on it. For example, this effect could be realized by manipulating data, or by denying access to, disrupting, degrading or destroying the computer system or its data. It is acknowledged that the branding of such activity as 'offensive' may not reflect the true intent or nature of such operations, since, as others have pointed out, there is a vast difference between offensive cyber activity to *thwart* an ongoing or impending harm and offensive cyber activity which is used to *initiate* hostilities or harm.[21] For simplicity's sake, however, the author adopts the overarching term of 'offensive cyber activity' in which the above range of activity is included, whether above or below the threshold of armed conflict.

This paper is not concerned with cyber-enabled espionage or computer network exploitation (CNE), both of which are passive operations that seek to observe or obtain information without having an 'effect' *per se*. Indeed, misunderstandings and misplaced rhetoric about 'cyberattacks' in relation to espionage operations often obstruct a properly informed understanding of this area.[22] That is not to say that cyber-enabled espionage cannot have a significant effect, for example if used for intellectual property theft, or for the release of information which may undermine the institutions of rival states or economic security. However, that is beyond the scope of this paper.

[21] Goldsmith, J. (ed.) (2022), *The United States' Defend Forward Cyber Strategy: A Comprehensive Legal Assessment*, Oxford: Oxford University Press.
[22] Skingsley, J. (2021), 'The SolarWinds hack: A valuable lesson for cybersecurity', Chatham House Expert Comment, 2 February 2021, https://www.chathamhouse.org/2021/02/solarwinds-hack-valuable-lesson-cybersecurity.

02 Perceptions of utility

The rapid development of cyber capabilities for a range of purposes, including for offensive cyber operations, risks leaving behind considerations of how they can be effectively managed.

How states perceive the utility or value of developing and maintaining offensive cyber capabilities is critical, as this informs not only how states may seek to use them, but also how they may manage or mitigate any associated risks of use. For example, where the utility of a capability is very high, the user may take a more risk-acceptant attitude to using it. And in many instances, cyber capabilities have been rapidly developed before policy or doctrine can catch up.[23] This is a concern, as enthusiasm for the perceived operational versatility of offensive cyber 'tools' may serve to dominate the demand for capability development, while methods for ensuring effective management of their use are deprioritized.[24]

Versatility

Some states highlight the utility of offensive cyber primarily for military purposes: to preserve the ability to counter-attack or retaliate in cyberspace.[25] Norway, for example, emphasizes its use in supporting tactical operations, including contributing

[23] Kello (2017), *The Virtual Weapon and International Order*, p. 16.
[24] The Belfer Center has analysed the range of national objectives pursued by states using cyber means, which include surveillance, controlling or manipulating the information environment, intelligence collection for national security purposes, destroying or disabling an adversary's infrastructure and capabilities, and commercial gain. See Voo, J., Hemani, I. and Cassidy, D. (2022), *National Cyber Power Index 2022*, report, Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, https://www.belfercenter.org/publication/national-cyber-power-index-2022.
[25] Author interviews with representatives from Dutch Defence Cyber Command, 21 June 2021, and Belgian Cyber Defence Directorate, 2 August 2021.

to NATO operations or coalitions with allies.[26] Other states explicitly highlight the utility of offensive cyber for a broad range of purposes, including following, attributing, warning about and actively counteracting digital threats before incidents occur, in situations of peace, crisis and armed conflict.

In addition, cyber capabilities were cited as an 'enabler' for information operations. Aside from military use, in the case of two states in particular that were considered in the research for this paper, offensive cyber is also used to counter criminal activity. In the UK, the National Cyber Force (NCF) states, for example, that it may engage in offensive cyber activity in order to interfere with a terrorist's mobile phone, or to help prevent cyberspace from being used for serious crime such as fraud and child sexual abuse, while also keeping UK military aircraft safe from being targeted.[27] In the US, USCYBERCOM can also use offensive cyber operations against foreign ransomware actors.[28]

Foreign cyber operations are depicted as having considerable utility, both as a focused and a supporting activity for a wide range of threats.

The range of potential targets and activities is particularly clear in Canada's legislation. Canada's Communications Security Establishment (CSE) is mandated to conduct foreign cyber operations, both 'active' and defensive.[29] The CSE Act reveals that the CSE has the power to conduct 'active cyber operations', 'to degrade, disrupt, influence, respond to or interfere with the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group as they relate to international affairs, defence or security [interests]'.[30] Canadian active cyber operations can be used 'to disrupt the capabilities of foreign threats to Canada, such as: foreign terrorist groups, foreign cyber criminals, hostile intelligence agencies [or] state-sponsored hackers'.[31] Defensive cyber operations can be used to defend Government of Canada systems, as well as systems of importance to the Government of Canada, against foreign cyber threats by taking online action.[32] Such foreign cyber operations may include 'any other activity that is reasonable in the circumstances and reasonably necessary in aid of any other activity'.[33] Foreign cyber operations are depicted as having considerable utility, both as a focused and a supporting activity for a wide range of threats.

[26] Government of Norway, Ministry of Defence (2019), *Proposition to the Storting for a parliamentary resolution: Investments in the Armed Forces and other matters*, Prop. 60 S (2018– 2019), section 5.3, https://www.regjeringen.no/no/dokumenter/prop.-60-s-20182019/id2638198; and author correspondence with senior scientist at Forsvarets forskningsinstitutt (FFI) [Norwegian Defence Research Establishment], July 2023.
[27] HM Government (2021), *Global Britain in a Competitive Age*, p. 42.
[28] US Cyber Command Public Affairs (2021), '2021: A Year in Review', news release, 29 December 2021, http://www.cybercom.mil/Media/News/Article/2885401/2021-a-year-in-review.
[29] Government of Canada, Communications Security Establishment (2023), 'Cyber operations', https://www.cse-cst.gc.ca/en/mission/cyber-operations.
[30] Parliament of Canada, House of Commons (2019), 'Statutes of Canada Chapter 13, Part 3', *Communications Security Establishment Act*, section 19.
[31] Government of Canada, Communications Security Establishment (2023), 'Cyber operations'.
[32] Ibid.
[33] Parliament of Canada, House of Commons (2019), 'Statutes of Canada Chapter 13, Part 3', section 31(d).

Another key theme in the responses to the interviews conducted for this paper was that cyber operations are often viewed as a substitute for the use of force in peacetime, in that they can be used to affect national sources of power without conducting an armed attack or triggering conflict. This is in keeping with much of the literature on the subject.[34] The ability this affords many states to pursue foreign policy objectives is perceived as one of the key reasons why offensive cyber has real value for some states. An interview with a representative from USCYBERCOM confirmed this view, for example: the utility of offensive cyber capabilities lies in enabling strategic effect without entitling the adversary to use force in self-defence, coupled with a unique ability to modulate the level of impact in a way that is not possible with kinetic operations.[35] Similarly, an interview with the then commander of UK Strategic Command (UK STRATCOM), offensive cyber was explained as a means by which a message can be sent, so as to manage strategic rivalries.[36] Sally Walker, former cyber director at the UK's Government Communications Headquarters (GCHQ), reported in a Sky News podcast that the UK sees cyber operations as being 'about what you can do from a distance at relatively low risk […] you can have impact in the real world and you can do it at scale'.[37] Offensive cyber activity is thus often viewed both as a strategic alternative to war and as having value on the battlefield.

Further, the UK has recently given more public detail on how the NCF seeks to deliver a 'doctrine of cognitive effect' through cyber operations which seeks to affect adversaries' abilities in three main ways. First, to affect their 'ability to acquire, analyse and exploit the information they need to advance their objectives', second, to 'limit their ability to communicate and coordinate with others', and third, to 'affect their confidence in their digital technology and the information it is providing them'.[38] The UK is clear that offensive cyber activity can also achieve effects in more subtle ways, below the level of the use of force.

Cyber limits

While states rightly highlight the value of offensive cyber in the ways set out above, less attention is publicly paid to its limitations – or, to put it another way, what offensive cyber is not. It is important that any perception of the versatility of offensive cyber capabilities as 'silver bullets' does not diminish awareness of their limitations. While offensive cyber operations may have utility in armed conflict, and in peacetime, as a means of projecting both hard and soft power, understanding their limitations is important so as to avoid an over-reliance on offensive cyber capabilities at the expense of other levers of power.

[34] See Harknett, R. J. and Smeets, M. (2020), 'Cyber campaigns and strategic outcomes', *Journal of Strategic Studies*, 45(4): pp. 534–67, https://doi.org/10.1080/01402390.2020.1732354; and Smeets (2022), *No Shortcuts*.
[35] Author interview with Lt Col. Kurt Sanger, then Deputy General Counsel of US Cyber Command, 23 June 2021.
[36] Interview with commander of UK Strategic Command, 11 August 2021.
[37] Walker, S., interviewed in Haynes, D. (2021), 'Into the Grey Zone', Sky News podcast, episode 5, 10 February 2021, https://news.sky.com/story/into-the-grey-zone-podcast-episode-five-cyber-power-part-ii-12212228.
[38] National Cyber Force (2023), *Responsible Cyber Power in Practice*, https://www.gov.uk/government/publications/responsible-cyber-power-in-practice, p. 15.

For example, as Smeets has highlighted, while many more states now publicly avow their offensive cyber capabilities, very few are actively using them to any significant effect, suggesting that in fact their utility may be more limited than previously assumed.[39] The requirement for highly tailored, target-specific capabilities, dependent on reliable and often painstaking intelligence, also makes effective offensive cyber capabilities a challenge, particularly in wartime.[40] The few publicly known examples of offensive cyber operations used in conjunction with conventional kinetic activity on the battlefield are difficult to assess in terms of how decisive they have been in determining the outcome of an operation.[41] For example, according to Maschmeyer, four out of the five cyber operations conducted by Russia in Ukraine between 2014 and 2022 produced no measurable strategic value, and Russia's resort to kinetic, conventional war in 2022 was in part precisely because its ongoing cyber activity against Ukraine was failing to achieve strategic goals.[42] There are also a number of other views which seek to highlight the limits to the *military* potential of offensive cyber.[43] As the UK chief of the General Staff noted, for example, in 2022, 'you can't cyber your way across a river'.[44]

Offensive cyber capabilities are also not a 'one size fits all' capability, and can take considerable time, effort and intelligence to construct and employ effectively. For example, offensive cyber capabilities used by the UK are reported to have been 'highly tailored and system specific'.[45] Successful cyber operations appear in reality to be the work of painstaking, highly tailored operations with only a brief opportunity for success. Their military utility therefore remains an open question. And below the level of armed conflict, other studies have argued that 'empirical evidence for this cyber revolution remains scarce' as cyber operations are hampered by a so-called 'operational trilemma' that restricts their value, making them 'too slow, too low in intensity, or too unreliable to provide significant utility'.[46]

[39] Smeets (2022), *No Shortcuts*.
[40] Rovner, J. (2021), 'Warfighting in Cyberspace', War on the Rocks, 17 March 2021, https://www.warontherocks.com/2021/03/warfighting-in-cyberspace.
[41] See, for example, Valeriano and Maness (2015), *Cyber War versus Cyber Realities*, and Melikishvili, A. (2008), 'The Cyber Dimension of Russia's Attack on Georgia', *Eurasia Daily Monitor*, 5(175), https://jamestown.org/program/the-cyber-dimension-of-russias-attack-on-georgia on cyberattacks in Georgia in 2008. See also an evaluation of the US cyber operations against Islamic State (ISIS) in 2016 at Temple-Raston, D. (2019), 'How the U.S. Hacked ISIS', NPR News, 26 September 2019, https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis. Finally, see assessments of Russia's cyber activity in Ukraine in 2022–23 at Willett, M. (2022), 'The Cyber Dimension of the Russia–Ukraine War', *Survival*, 64(5), https://doi.org/10.1080/00396338.2022.2126193; and Kaminska, M., Shires, J. and Smeets, M. (2022), *Cyber Operations during the 2022 Russian invasion of Ukraine: Lessons Learned (so far)*, Tallinn Workshop Report, European Cyber Conflict Research Initiative, https://eccri.eu/wp-content/uploads/2022/07/ECCRI_WorkshopReport_Version-Online.pdf.
[42] Maschmeyer, L. (2021), 'The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations', *International Security*, 46(2): pp. 51–90, https://doi.org/10.1162/isec_a_00418.
[43] Bronk, J. and Watling, J. (2021), *Necessary Heresies: Challenging the Narratives Distorting Contemporary UK Defence*, research paper, London: Royal United Services Institute, https://rusi.org/explore-our-research/publications/whitehall-papers/necessary-heresies-challenging-narratives-distorting-contemporary-uk-defence.
[44] British Army (2022), 'General Sir Patrick Sanders, Chief of the General Staff, Opens the RUSI Land Warfare Conference with his speech', 28 June 2022, https://www.army.mod.uk/news-and-events/news/2022/06/rusi-land-warfare-conference-cgs-speech.
[45] HM Government (2017), *Intelligence and Security Committee of Parliament: Annual Report 2016–17*, https://www.gov.uk/government/publications/intelligence-and-security-committee-annual-report-2016-2017, p. 43.
[46] Maschmeyer (2021), 'The Subversive Trilemma'.

Deterrence

Several states have published cyber strategies which mention the deterrent value of offensive cyber capabilities. The Netherlands, for example, bases its *Defence Cyber Strategy* on deterrence, as 'the operational capabilities of the Defence Cyber Command contribute to the arsenal of deterrence means available to the government'.[47] Belgium and Denmark also cite deterrence as a key justification for developing offensive cyber capability,[48] while the Norwegian Defence Commission reported in 2021 that both 'defensive and offensive cyber operations can act as a deterrent and affect an adversary's perception of vulnerability and opportunity for retaliation'.[49] Yet most states give little detail as to *how* or *why* offensive cyber capabilities may serve as a deterrent in or through cyberspace. While public statements to this effect may be scarce for a variety of reasons, a more nuanced internal understanding of this area is important, as assumptions about the deterrent value of offensive cyber may serve, for example, to downplay the importance of cyber resilience.

There has also been rigorous academic challenge to the application of deterrence theory to cyberspace. For example, Harknett's conclusions that 'using a legacy construct of deterrence, whose measure of effectiveness is the absence of action, to explain an environment of constant action will not prevent adverse actions in cyberspace' are now well rehearsed among cyber experts.[50] It is clear that conventional deterrence theory does not sit well in cyberspace and there is significant evidence and scholarship that offensive cyber operations do not, on their own, necessarily deter, particularly below the threshold where most day-to-day cyber competition takes place.

It is also challenging to establish metrics as to whether deterrence is working. States may refrain from conducting more destructive offensive cyber operations due to a combination of fears which may include other concerns, such as risks of collateral damage and/or strategic blowback. The inherent uncertainties of cyber operations in terms of second- and third-order effects is also likely to constrain activity.[51] Examples may include the US reluctance to retaliate against Iran in response to the 2013 distributed denial-of-service (DDoS) attacks on US banks[52] and the US decision not to conduct offensive cyber operations against Libya in 2011

[47] Author interview with Peter Pijpers, Associate Professor Cyber Operations, Netherlands Defence Academy, 17 June 2021. See also Government of the Netherlands, Ministry of Defence (2018), *Defensie Cyber Strategie 2018: Investeren in digitale slagkracht voor Nederland* [Defence Cyber Strategy 2018: Investing in cyber striking power for the Netherlands], https://english.defensie.nl/binaries/defence/documenten/publications/2018/11/12/defence-cyber-strategy-2018/NLD+MoD+cyber+strategy+2018_web.pdf, p. 8.
[48] The Danish Government (2021), 'The Danish National Strategy for Cyber and Information Security', Copenhagen: Danish Ministry of Finance, https://www.cfcs.dk/globalassets/cfcs/dokumenter/2022/ncis_2022-2024_en.pdf, p. 50. For Belgium, author's interview with Director, Belgian Cyber Defence, 2 August 2021.
[49] Government of Norway (2023), *Forsvarskommisjonen av 2021: Forsvar for fred og frihet* [The Defence Commission of 2021: Defence for peace and freedom], https://www.regjeringen.no/contentassets/8b8a7fc642f44ef5b27a1465301492ff/no/pdfs/nou202320230014000dddpdfs.pdf, p. 142 (original Norwegian text: 'Evne til defensive og offensive cyberoperasjoner kan være avskrekkende og påvirke en motstanders oppfatning av sårbarhet og mulighet for gjengjeldelse'.)
[50] Harknett, R. J. and Nye, J. S. (2017), 'Is Deterrence Possible in Cyberspace?', *International Security*, 42(2): pp. 196–9, https://doi.org/10.1162/ISEC_c_00290.
[51] Kello (2017), *The Virtual Weapon and International Order*, p. 6. Entanglement – the idea that networks and systems are extensively interlinked and interdependent – also reflects this difficulty, as an operation by one state may inadvertently end up causing harm to that state. See Nye (2010), *Cyber Power*, pp. 16–17.
[52] Waterman, S. (2017), 'Clapper: U.S. shelved "hack backs" due to counterattack fears', Cyberscoop, 2 October 2017, https://www.cyberscoop.com/hack-back-james-clapper-iran-north-korea.

given fears of the precedent this would set.[53] According to Kaminska, the muted responses of the UK to the WannaCry attacks of early 2017 also show how states seek to minimize risk in their responses.[54]

It is likely that, in what has been termed the 'deterrence gap',[55] states may increasingly realize that deterrence in cyberspace works, but only above a certain threshold of harm. In other words, deterrence works to prevent widespread destructive cyberattacks by nation-states, but day-to-day low-level harmful cyber activity below this level continues undeterred, as most offensive cyber activity takes place below the threshold of armed conflict and '[falls] well short of threats to infrastructure'.[56] While there have been some known cases of malicious state-sponsored cyber activity on critical infrastructure, for example during the Iran–Israel so-called 'tit-for-tat' cyberattacks in 2020 (which included cyberattacks on water management facilities[57] and port facilities[58]), on the whole targets are of minor value and/or the disruption or harm is only temporary.[59] Offensive cyber operations that amount to a use of force under international law remain scarce.[60]

Deterrence works to prevent widespread destructive cyberattacks by nation-states, but day-to-day low-level harmful cyber activity below this level continues undeterred.

A more rigorous analysis of the deterrent value of offensive cyber capabilities is therefore important. The UK's *National Cyber Strategy 2022* acknowledges that 'our approach to cyber deterrence does not yet seem to have fundamentally altered the risk calculus for attackers'.[61] The US 'defend forward' strategy, set out in a case study below, is also premised on the notion that deterrence does not work in cyberspace below the threshold of armed conflict.[62] The US *2022 National Defense Strategy* speaks of 'integrated deterrence', focusing on using diplomatic, economic and military tools in combination rather than as standalone mechanisms, hinting

[53] Schmitt, E. and Shanker, T. (2011), 'U.S. Debated Cyberwarfare in Attack Plan on Libya', *New York Times*, 17 October 2011, https://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html.
[54] Kaminska, M. (2021), 'Restraint under conditions of uncertainty: Why the United States tolerates cyberattacks', *Journal of Cybersecurity*, 7(1): pp. 1–15 at p. 8, https://doi.org/10.1093/cybsec/tyab008.
[55] Daniel, M. (2021), *Closing the Gap: Expanding Cyber Deterrence*, Cyberstability Paper Series, The Hague: The Hague Centre for Strategic Studies and the Global Commission on the Stability of Cyberspace, https://hcss.nl/report/closing-the-gap-expanding-cyber-deterrence.
[56] Rovner, J. (2020), 'The Intelligence Contest in Cyberspace', Lawfare, 26 March 2020, https://www.lawfareblog.com/intelligence-contest-cyberspace.
[57] *Times of Israel* (2020), 'Cyber attacks again hit Israel's water system, shutting agricultural pumps', 17 July 2020, https://www.timesofisrael.com/cyber-attacks-again-hit-israels-water-system-shutting-agricultural-pumps.
[58] Warrick, J. and Nakashima, E. (2020), 'Officials: Israel linked to a disruptive cyberattack on Iranian port facility', *Washington Post*, 18 May 2020, https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html.
[59] Lindsay, J. R. (2015), 'Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack', *Journal of Cybersecurity*, 1(1), pp. 53–67 at p. 62, https://doi.org/10.1093/cybsec/tyv003.
[60] Stuxnet being an exception to this according to some international lawyers: see Buchan, R. (2012), 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?', *Journal of Conflict & Security Law*, 17(2), pp. 211–27, https://doi.org/10.1093/jcsl/krs014.
[61] HM Government (2021), *National Cyber Strategy 2022*, London: Cabinet Office, https://www.gov.uk/government/publications/national-cyber-strategy-2022, p. 25.
[62] Fischerkeller, M. P. and Harknett, R. J. (2017), 'Deterrence is Not a Credible Strategy for Cyberspace', *Orbis*, 61(3), pp. 381–93, https://doi.org/10.1016/j.orbis.2017.05.003.

at a shift in how some states are perceiving the deterrent value of cyber capabilities on their own.[63] The UK has also outlined a more detailed position recently on the relationship between cyber activity and deterrence, stating that its NCF 'may also potentially contribute to deterrence',[64] but highlighting that it is important to distinguish 'between deterring cyber activity, or using cyber effects to deter other activities' and that '[while] evidence is limited for cyber operations being a primary contributor to deterrence, they can form a secondary or supporting element in an integrated approach'.[65] There is a need for a more nuanced approach, which addresses what it is that states seek to deter and by whom, and which incorporates other levers of power and influence outside cyberspace. The US *2018 Department of Defense Cyber Strategy*, for example, specifically refers for example to deterring 'malicious cyber activities that constitute *a use of force* against the United States' (emphasis added).[66]

In conclusion, a better understanding of the utility of offensive cyber capabilities should be fostered within states. Despite all the rhetoric as to versatility and possible range of effect, we are essentially none the wiser as to where offensive cyber activity may have best effect or may be best utilized. Overly blunt interpretations of the advantages of offensive cyber may increase the likelihood that such activity becomes a default or 'go-to' offensive method of choice, particularly in the context where these capabilities become 'normalized' as more states adopt them.[67] A more complex balancing act may be required to assess the trade-offs or benefits the cyber operation may bring, set against the risks of use,[68] as explored in the following chapter. This would not only help to avoid any complacency as to their power and utility, but also can help, for example, to reinforce the need to consider other 'tools in the toolbox', as different strategic contexts will demand different capabilities and responses. Offensive cyber may not always be the best answer to a given problem. In this way, states can also ensure they consider how offensive cyber can be used in line with a commitment to responsible state behaviour in cyberspace.

Finally, national cyber strategies should also account for the limitations surrounding the application of deterrence theory in cyberspace, rather than making broad generalizations as to the value of offensive cyber as a deterrent in its own right. Whatever conclusions one may reach as to the efficacy of deterrence in or through cyberspace, it is also important that they do not come at the expense of other critical aspects of cyber strategy such as enhanced cyber resilience and/or cyber defence. An over-reliance on the deterrent value of offensive cyber capabilities may bring a false sense of security, or perpetuate the so-called 'cybersecurity dilemma'.[69]

[63] United States Department of Defense (2022), *2022 National Defense Strategy of the United States of America: Including the 2022 Nuclear Posture Review and the 2022 Missile Defense Review*, Washington, DC: US Department of Defense, https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF.

[64] National Cyber Force (2023), *Responsible Cyber Power in Practice*, p. 5.

[65] Ibid., p. 10.

[66] United States Department of Defense (2018), *Summary: 2018 Department of Defense Cyber Strategy*, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.pdf, p. 2.

[67] For more on the false perception that offensive cyber has advantage over defence, see Lindsay, J. R. (2013), 'Stuxnet and the Limits of Cyber Warfare', *Security Studies*, 22(3), pp. 365–404, https://doi.org/10.1080/09636412.2013.816122; and Slayton, R. (2017), 'What Is the Cyber Offense–Defense Balance? Conceptions, Causes, and Assessment', *International Security*, 41(3), pp. 72–109, https://doi.org/10.1162/ISEC_a_00267.

[68] Maschmeyer (2021), 'The Subversive Trilemma'.

[69] Buchanan, B. (2017), *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*, London: Hurst.

03 Risk perception in cyberspace

Given the wider concerns over the risks associated with using offensive cyber, how states perceive and manage these risks is critical. States' authorization mechanisms help to give clarity on their perceptions.

The last chapter referred to the risks of using offensive cyber capabilities. This paper explores ways in which states' perceptions of risk can be assessed when conducting offensive cyber operations, not only because of the wider concerns about inadvertent harm in the context of a well-rehearsed discourse on risks of escalation in cyberspace, but also because enthusiasm for the advantages of offensive cyber explored hitherto may serve to mask these concerns. Given the divide in the debate – explored below – about risks of escalation in cyberspace, how states *themselves* perceive, mitigate and manage these issues is therefore critical and deserving of more attention in the discourse. Yet only very few states openly address the risks of *own* use in their cyber strategies. For example, France's military cyber strategy mentions escalation and the risks of hacking back,[70] while Germany refers to the 'especially large risk of uncontrolled escalation' in cyberspace due to the problem of attribution in its 2016 defence white paper.[71] The 2021 German *Cybersicherheitsstrategie* [Cybersecurity Strategy] also focuses on risk and the importance of reducing the latter to an acceptable level.[72]

[70] Government of France, Ministry of the Armed Forces (2019), *Éléments publics de doctrine militaire de lutte informatique offensive*, p. 9. See also Government of France, General Secretariat for Defence and National Security (SGDSN) (2018), *Revue stratégique de cyberdéfense*, https://www.sgdsn.gouv.fr/publications/revue-strategique-de-cyberdefense, pp. 34–5.
[71] Federal Government of Germany (2016), *White Paper on German Security Policy and the Future of the Bundeswehr*, https://www.bundeswehr.de/resource/blob/4800140/fe103a80d8576b2cd7a135a5a8a86dde/download-white-paper-2016-data.pdf, p. 38.
[72] German Federal Ministry of the Interior and Community (2021), *Cybersicherheitsstrategie für Deutschland 2021*, https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf, p. 109.

Yet, aside from these two examples, cyber strategies largely focus on the risks of harm posed by external actors using offensive cyber for malign purposes; less is said about internal perceptions of risk, in terms of the extent to which a state considers that its own use of offensive cyber may cause harm in a variety of ways – both to its strategic interests and to international security more broadly, as well as physical harm. More detail in this regard could fill in some of the gaps in understanding what 'responsible cyber' means.[73]

The risks of using offensive cyber: a precis

As more states develop offensive cyber capabilities, this is said to open up more vectors for escalation. The rise in the number of players in the game, and lack of transparency as to what responsible cyber may look like, suggest an unstable future for cyberspace. Some experts still argue that offensive cyber capabilities run the risk of a dangerous escalation and inadvertent spread, due to the inherent complexities of cyberspace.[74] For example, Stuxnet, a highly sophisticated cyber operation, ultimately spread across the world unintentionally,[75] while the NotPetya cyberattack is said to have spread far further than perhaps was intended and serves as a strong example of how quickly malicious code can spread.[76] Others argue that cyberspace can favour offensive action[77] or is 'offence-dominant',[78] and that use of offensive cyber capabilities is likely to produce an overall increase in cyber conflict.[79]

Meanwhile, some studies have shown that the same methods that are used to conduct espionage in cyberspace are used in the initial stages of an offensive cyber operation, since effective offensive cyber operations are not possible without prior reconnaissance of the target.[80] Cyber operations are often characterized

[73] Shires, J. and Smeets, M. (2021), 'The UK as a Responsible Cyber Power: Brilliant Branding or Empty Bluster?', Lawfare, 23 November 2021, https://www.lawfareblog.com/uk-responsible-cyber-power-brilliant-branding-or-empty-bluster.

[74] Escalation has been defined as 'an increase in the intensity or scope of conflict that crosses threshold(s) considered significant by one or more of the participants'. See Morgan, F. E., Mueller, K. P., Medeiros, E. S., Pollpeter, K. L., and Cliff, R. (2008), *Dangerous Thresholds: Managing Escalation in the 21st Century*, Santa Monica, CA: RAND Corporation, p. 8.

[75] Sanger, D. (2018), *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*, London: Scribe UK.

[76] Greenberg, A. (2018), 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History', Wired, 22 August 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world.

[77] Libicki, M. C. (2009), *Cyberdeterrence and Cyberwar*, Santa Monica, CA: RAND Corporation, pp. 32–3. Rid counters the offence-dominance theories, however, by pointing out the costs and difficulties in cyber offence, which limits the number of states who are capable of sophisticated and highly destructive cyber offence, and the fact that, once used, destructive code will be rendered useless as defences are upgraded to guard against it. See Rid, T. (2017), *Cyberwar Will Not Take Place*, London: Hurst, pp. 167–9.

[78] Kello, L. (2013), 'The Meaning of the Cyber Revolution: Perils to Theory and Statecraft', *Quarterly Journal: International Security*, 38(2), pp. 7–40, https://www.belfercenter.org/publication/meaning-cyber-revolution-perils-theory-and-statecraft.

[79] Klimburg, A. (2020), 'Mixed Signals: A Flawed Approach to Cyber Deterrence', *Survival*, 62(1), pp. 107–30, https://doi.org/10.1080/00396338.2020.1715071, p. 123.

[80] Several examples have shown that the same cyber methods that are used to steal data can also be used to effect an attack. Malware such as Duqu, Flame and Gauss, for example, has the same characteristics as Stuxnet. See Chien, E., O'Murchu, L., and Falliere, N. (2012), 'W32.Duqu: The Precursor to the Next Stuxnet', paper presented at LEET '12, 24 April 2012, San Jose, CA, https://www.usenix.org/system/files/conference/leet12/leet12-final11.pdf; and Zetter, K. (2011), 'Son of Stuxnet Found in the Wild on Systems in Europe', Wired, 18 October 2011, https://www.wired.com/2011/10/son-of-stuxnet-in-the-wild. For detail on Flame, see Kaplan, F. (2017), *Dark Territory: The Secret History of Cyber War*, New York: Simon & Schuster, pp. 205–6. For more on Gauss, see Lindsay (2013), 'Stuxnet and the Limits of Cyber Warfare', pp. 370–1.

as '90 per cent espionage and 10 per cent hacking' for this reason.[81] This overlap therefore is said to have the potential to cause significant instability in cyberspace, due to the critical challenge of distinguishing between straightforward espionage and more harmful activity so as not to misinterpret an adversary's intentions.[82] These concerns have been brought to the fore as some states have integrated intelligence operations from civilian intelligence agencies with military cyber units, due to the high dependency of offensive cyber activity on accurate, timely and reliable intelligence.[83]

Cyberspace is unique in that offensive activity can directly undermine one's own defensive interests.

Cyberspace is also unique in that offensive activity can directly undermine one's own defensive interests, for example by propagating malware, or establishing 'back doors' into other systems, or not disclosing software vulnerabilities.[84] One former senior retired British official interviewed for this paper also highlighted that as more states develop cyber commands and offensive cyber capabilities, there is also a greater risk of 'fratricide' as more states start to operate in cyberspace.[85] While this may be mitigated to a certain extent by way of deconfliction between close allies, it may not always be the case that even close allies want to disclose the nature or location of their cyber operations to one another.[86]

The US's more assertive 'defend forward' and persistent engagement posture in cyberspace has come under close scrutiny as the US seeks to operate routinely outside its own networks, triggering some of the concerns cited above. This scrutiny has been particularly intense as other states may seek to emulate this posture in future as their capabilities and strategic priorities develop over time.[87]

[81] It is said that this is why arms control agreements in cyberspace are not feasible. See Lindsay (2015), 'Tipping the scales', p. 55.
[82] Brown, G. D. (2016), 'Spying & Fighting in Cyberspace: What is Which?', *Journal of National Security Law & Policy*, 8(3), https://jnslp.com/wp-content/uploads/2017/10/Spying-and-Fighting-in-Cyberspace_2.pdf. See also Healey, J. and Jervis, R. (2020), 'The Escalation Inversion and Other Oddities of Situational Cyber Stability', *Texas National Security Review*, 3(4), pp. 30–53, https://doi.org/10.26153/tsw/10962.
[83] For example, the UK's National Cyber Force (NCF) and US Cyber Command.
[84] The International Institute for Strategic Studies assesses that 'state cyber operations to reconnoitre and gain a presence on relevant networks are occurring every second and are now a permanent feature of cyberspace'. See International Institute for Strategic Studies (2021), *Cyber Capabilities and National Power,* p. 1. Malware placed on the Russian electrical grid by the US in 2018 was said, for example, to be a warning for Russia not to interfere with the US mid-term elections in the same year. See Sanger, D. and Perlroth, N. (2019), 'U.S. Escalates Online Attacks on Russia's Power Grid', *New York Times*, 15 June 2019, https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html.
[85] Author interview, 28 June 2021.
[86] See more on this issue at Liles, S. and Kambic, J. (2014), 'Cyber Fratricide' in Brangetto, P., Maybaum, M. and Stinissen, J. (eds) (2014), *2014 6th International Conference on Cyber Conflict: Proceedings*, Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, pp. 329–38.
[87] For example, Norway's defence plan for 2021–24 outlines an intent to develop Norway's ability to 'follow, attribute, warn and actively counter digital threats before incidents occur' – see Government of Norway, Ministry of Defence (2020), *Proposisjon til Stortinget (forslag til stortingsvedtak),* Prop. 14 S (2020–2021), section 1, https://www.regjeringen.no/contentassets/81506a8900cc4f16bf805b936e3bb041/no/pdfs/prp202020210014000dddpdfs.pdf, p.13 (original wording: 'til å følge, attribuere, varsle og aktivt motvirke digitale trusler før hendelser inntreffer. Forsvarssektorens evne til å forebygge, avdekke og håndtere trusler i det digitale rom styrkes for å beskytte Forsvarets egen virksomhet'). Similarly, the Netherlands outlines that: 'Proper defence and security alone are not […] sufficient to prevent malicious parties from carrying out cyber attacks. An increasing number of allies are therefore taking a more active approach in the cyber domain (active defence)'. See Government of the Netherlands, Ministry of Defence (2018), *Defence Cyber Strategy 2018*, p. 6.

Box 1. 'Defend forward' and persistent engagement

US policy underwent a notable shift between 2015, when the Department of Defense (DoD) released its updated cyber strategy, and 2018, when the US Cyber Command Strategic Vision was published and USCYBERCOM became a unified combatant command. While the 2015 strategy sought to preserve the status quo and to exercise restraint in cyberspace, taking the 'least action necessary to mitigate threats' and prioritizing defence,[88] by 2018 it had been decided that maintaining the status quo was no longer possible in light of the actions of US adversaries in cyberspace.[89] Hence, the US confirmed that it would undertake cyber operations outside its own networks in order to 'defend forward'[90] under the umbrella of persistent engagement. This marked a significant change in how the US employs its cyber capabilities, indicating a much more assertive posture in cyberspace. In essence, rather than remaining in a defensive posture within its own networks, USCYBERCOM would 'defend forward' in day-to-day competition, 'to expose adversaries' weaknesses, learn their intentions and capabilities, and counter attacks close to their origins' through 'persistent action' and 'removing constraints on (our) speed and agility'.[91] The architects of this new 'defend forward' vision outlined the need for 'cyber persistence' rather than 'operational restraint that is supporting a strategy of deterrence'.[92] The US Cyberspace Solarium Commission (CSC) report of March 2020 sums up 'defend forward' as a proactive rather than reactive response to cyber threats.[93] Importantly, although the CSC report states that 'defend forward' is 'inherently defensive', it nonetheless involves offensive action at the tactical and operational levels.[94] Critically, the US has not shied away from advertising this new posture, as in many respects the very idea of 'defend forward' was deliberately orchestrated to send a strong message to US adversaries.

The 'defend forward' approach has, however, been defended as both necessary and successful. In March 2021, General Paul Nakasone, the commander of USCYBERCOM, confirmed in a statement to the US Senate Armed Services Committee that the cyber command had conducted 'more than two dozen operations to get ahead of foreign threats before they interfered with or influenced our elections in 2020', which proceeded unaffected by cyberattacks.[95] The success of the US in countering the activities of the Russian-sponsored Internet Research Agency in 2018 has also been highlighted as validation of the US's defend forward posture.[96]

[88] Executive Office of the President of the United States (2013), 'Fact Sheet on Presidential Policy Directive 20', https://irp.fas.org/offdocs/ppd/ppd-20-fs.pdf.
[89] Kollars, N. and Schneider, J. (2018), 'Defending Forward: The 2018 Cyber Strategy is Here', War on the Rocks, 20 September 2018, https://warontherocks.com/2018/09/defending-forward-the-2018-cyber-strategy-is-here.
[90] See US Cyber Command (2018), *Achieve and Maintain Cyberspace Superiority*. Noting that some have argued persistent engagement and defend forward are not strategies in the strict sense, as neither 'seeks to match ways and means to achieve stated ends' – see more at Corn, G. (2021), 'SolarWinds Is Bad, but Retreat From Defend Forward Would Be Worse', Lawfare, 14 January 2021, https://www.lawfareblog.com/solarwinds-bad-retreat-defend-forward-would-be-worse.
[91] US Cyber Command (2018), *Achieve and Maintain Cyberspace Superiority*, pp. 2 and 6.
[92] Fischerkeller and Harknett (2017), 'Deterrence is Not a Credible Strategy for Cyberspace'.
[93] US Cyberspace Solarium Commission (2020), *Report*, https://www.solarium.gov/report, p. 24.
[94] Ibid., p. 33.
[95] United States Senate Committee on Armed Services (2021), 'Full Committee Hearing: United States Special Operations Command and United States Cyber Command', 25 March 2021, https://www.armed-services.senate.gov/hearings/21-03-25-united-states-special-operations-command-and-united-states-cyber-command.
[96] Nakashima, E. (2019), 'U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms', *Washington Post*, 27 February 2019, https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html.

While there is no evidence at present that the persistent engagement strategy has contributed to significant instability in cyberspace, 'defend forward' and persistent engagement have not been without criticism.[97] In cyberspace there is no such thing as no man's land. Analogies with patrolling in no man's land therefore do not transfer across well to cyberspace in terms of justifying offensive cyber activity beyond one's own networks.[98] Persistent engagement has been criticized as a 'very high-risk approach' which 'ignores the potential for unwanted effects that could prove to be highly destabilizing in an already volatile international security environment'.[99] The commander of the French Cyber Defence Command (Comcyber) also recently warned of concerns over 'relatively aggressive' US cyber operations on European networks to counter Russian intrusions.[100] Goldsmith and Loomis argue that 'defend forward' could provoke bilateral escalation, leaving the US worse off given its high digital dependencies, or even global escalation, as it uses methods which mirror the very same operations it seeks to counter.[101]

Persistent engagement has been criticized as a 'very high-risk approach' which 'ignores the potential for unwanted effects that could prove to be highly destabilizing in an already volatile international security environment'.

Yet those who advocate for persistent engagement hope that cyber operations will become a normal and agreed part of state competition, as 'a doctrine of active mitigation may be less escalatory than one of restraint'.[102] As Schneider explains, defend forward is based on the assumption that the 'constant use of cyber operations inures states to cyber incidents and, therefore, decreases emotional or strategic incentives to respond to cyber operations with escalation'.[103] In an interview in 2021, the then commander of UK STRATCOM presented persistent engagement as legitimate activity which can contribute to stability in cyberspace, as long as it is moderated and modulated effectively and a continuing internal dialogue as to its effectiveness or otherwise is maintained.[104]

[97] It is important to distinguish between the two concepts, as they do not amount to the same thing. Persistent engagement is a strategy or paradigm that guides operations, while defend forward is an operational activity. Defend forward advances the persistent engagement 'strategy' or falls into the persistent engagement 'paradigm'. In simple terms, defend forward is an action, not an idea, whereas persistent engagement is an idea, not an action. See Corn (2021), 'SolarWinds Is Bad, but Retreat From Defend Forward Would Be Worse'. See also Goldman, E. O. (2020), 'From Reaction to Action: Adopting a Competitive Posture in Cyber Diplomacy', *Texas National Security Review*, 3(4), pp. 84–101, https://doi.org/10.26153/tsw/10950.

[98] For more on the confusion and misunderstanding around red, blue, and grey 'space' in respect of cyber operations, see Smeets, M. (2019), 'Cyber Command's Strategy Risks Friction with Allies', Lawfare, 28 May 2019, https://www.lawfareblog.com/cyber-commands-strategy-risks-friction-allies.

[99] Klimburg (2020), 'Mixed Signals', p. 108.

[100] Elise Vincent (2023), 'France's cyber defense force questions role of US support in Europe', *Le Monde*, 15 January 2023, https://www.lemonde.fr/en/international/article/2023/01/15/france-s-cyber-defense-force-questions-the-role-of-us-support-in-europe_6011684_4.html.

[101] Goldsmith, J. and Loomis, A. (2022), 'Defend Forward and Sovereignty', in Goldsmith, J. (ed.) (2022), *The United States' Defend Forward Cyber Strategy: A Comprehensive Legal Assessment*, Oxford: Oxford University Press, p. 167.

[102] Fischerkeller and Harknett (2017), 'Deterrence is Not a Credible Strategy for Cyberspace', p. 382.

[103] Schneider, J. (2020), 'A Strategic Cyber No-First-Use Policy? Addressing the US Cyber Strategy Problem', *The Washington Quarterly*, 43(2), pp. 159–75 at p. 160, https://doi.org/10.1080/0163660X.2020.1770970.

[104] Author interview with Commander UK STRATCOM, 11 August 2021.

It is also important to note that many experts do not share the view that cyberspace presents an environment that is inherently escalatory.[105] Escalation dynamics in cyberspace remain contested, and some maintain that in fact offensive cyber operations may have de-escalatory functions, for a variety of reasons. For example, the covert nature of offensive cyber operations is said to provide 'escalatory off-ramps'.[106] Cyber operations can also be used to act as a pressure-release valve – unlike overt kinetic operations, which result in destruction to one degree or another – and can also be reversible (unlike the physical effects of a kinetic strike) by restoring denied access to a system or network, or by removing malicious code, making them less likely to cause escalation.[107] In mid-2019, for example, after Iranian forces shot down a US Navy Global Hawk surveillance drone, the Trump administration chose to respond using offensive cyber capabilities rather than airstrikes.[108] Cyber activity is also said to be more akin to attrition as opposed to being escalatory.[109]

As for states themselves, however, it is not always clear to what extent they consider or assess these risks. To that end, this paper considers two key indicators to explore whether and how states not only perceive risk but seek to manage it.

A measure of last resort?

One method of analysing how states observe risk of use of offensive cyber may be perceived in the way in which some states have indicated that offensive cyber activity may only be used as a measure of last resort, although this is not always communicated officially.[110] The Netherlands sees use of offensive cyber capabilities as the exception, rather than the rule.[111] An interview with a representative of the Dutch Defence Cyber Command revealed how a key consideration is based on political risk, which may be much harder to determine than physical

[105] Borghard, E. D. and Lonergan, S. W. (2019), 'Cyber Operations as Imperfect Tools of Escalation', *Strategic Studies Quarterly,* 13(3), pp. 122–45, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-13_Issue-3/Borghard.pdf.

[106] Jensen, B. and Valeriano, B. (2019), *What do we know about cyber escalation? Observations from simulations and surveys*, Scowcroft Center for Strategy and Security Brief, Washington, DC: Atlantic Council, https://www.atlanticcouncil.org/wp-content/uploads/2019/11/What_do_we_know_about_cyber_escalation_.pdf. A contrary view is also put forward by Fischerkeller, however – see Fischerkeller, M. P. (2022), *What Do We Know About Cyber Operations During Militarized Crises?,* Scowcroft Center for Strategy and Security Brief, Washington, DC: Atlantic Council, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/what-do-we-know-about-cyber-operations-during-militarized-crises.

[107] Estonia in 2007, Georgia in 2008, and Sony Pictures in 2014 are all examples of targeted distributed denial-of-service (DDoS) attacks which had a temporary effect but did not result in long-term physical damage. See more at Smeets, M. and Lin, H. S. (2018), *Offensive cyber capabilities: To what ends? 2018 10th International Conference on Cyber Conflict (CyCon)*, pp. 55–72, https://doi.org/10.23919/CYCON.2018.8405010. But note also Fischerkeller's contrary view that the reversibility of some cyber operations should not always be deemed a virtue, and much will depend on context as they may in fact communicate weakness – see Fischerkeller (2022), *What Do We Know About Cyber Operations During Militarized Crises?*.

[108] In 2019 the US conducted offensive cyber operations against Iranian computer systems that controlled rocket and missile launchers. See Barnes, J. E. and Gibbons-Neff, T. (2019), 'U.S. Carried Out Cyber Attacks on Iran', *New York Times*, 22 June 2019, https://www.nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html, and Chesney, R. (2019), 'The Legal Context for CYBERCOM's Reported Operations Against Iran', Lawfare, 24 June 2019, https://www.lawfareblog.com/legal-context-cybercoms-reported-operations-against-iran.

[109] A point made by Sally Walker in Haynes, D. (2021), 'Into the Grey Zone'.

[110] Author interview with strategic adviser to Dutch Defence Cyber Command, 21 June 2021.

[111] Ibid. Offensive cyber activity outside the context of an armed conflict would be viewed as a breach of sovereignty of the target state.

or collateral risk in the style of conventional military planning.[112] Belgium's offensive cyber aspirations are still in their relative infancy, with the government having only announced its intention to integrate offensive cyber capabilities into its military in 2020, but its 2021 *Cybersecurity Strategy* states that the Belgian military will deploy offensive cyber capabilities during 'national crises' to 'neutralize' attacks, suggesting a specifically defence-oriented approach, in which such tools are only used in extremis[113] – for example in an armed conflict, or for counter-attack purposes outside an armed conflict.[114]

Similarly, Canada's legislation contains a notable provision that foreign cyber operations will only be used where the 'objective of the cyber operation could not reasonably be achieved by other means',[115] indicating that foreign cyber operations are seen as a strategic capability to achieve outcomes that other tools could not achieve in a sufficiently timely or effective manner, for example against cybercriminals or terrorist groups that are beyond the jurisdiction or reach of Canadian law enforcement agencies.[116] Lastly, the Czech Republic's Act No. 150/2021 on Military Intelligence states that the Czech Military Intelligence Service can carry out 'active intervention in cyberspace' if there is a 'threat to important interests of the state to a large extent' and the cyberattack or threat is 'imminent' and 'cannot be averted in cooperation with the armed forces […] and [is] the only possible way to avert them'.[117] These approaches suggest that some states remain cautious as to the conditions under which offensive cyber may be used.

Authorization mechanisms

Examining several states' authorization mechanisms for use of offensive cyber – where these have been made public – can also be instructive in illustrating the extent to which states consider offensive cyber operations to carry political and/or operational risk, both in peacetime and in armed conflict.

Table 1 indicates that the nine NATO states investigated for this paper maintain authorization for offensive cyber operations at the highest levels. This may reflect an anticipation of risk from conducting offensive cyber activity, as these states appear to retain a close hold over their offensive cyber capabilities. Specific articulated recognition of risks in cyber strategies is lacking, but Table 1 suggests it remains.

[112] Ibid.
[113] Centre for Cyber Security Belgium (2021), *Cybersecurity Strategy Belgium 2.0 2021–2025*, Brussels: Centre for Cyber Security Belgium, https://ccb.belgium.be/sites/default/files/CCB_Strategie%202.0_UK_WEB.pdf, p. 37.
[114] Author interview with representative from Belgian Cyber Defence Directorate, 2 August 2021.
[115] Parliament of Canada, House of Commons (2019), 'Statutes of Canada Chapter 13, Part 3', section 34(4).
[116] Author correspondence with commanding officer, Combined Cyber Unit (Canadian Armed Forces), and then special adviser to the Deputy Chief of Operational Policy, June 2023.
[117] Czech Republic (2021), Act No. 150/2021 Act amending Act No. 289/2005 on Military Intelligence, as amended, and certain other acts, https://www.zakonyprolidi.cz/cs/2021-150, section 16(g).

Table 1. Known authorization mechanisms by country

State	Authorization mechanism
Belgium	Belgium is currently in the process of updating its legislation to include offensive cyber operations in the context of counter-attack cyber operations. Legislation at present only covers counter-attacks in respect of military networks. If used in support of military operations, cyber operations require a cabinet-level decision, involving the defence minister.[118]
Canada	Foreign cyber operations conducted by the CSE under its mandates require the involvement of both the ministers of national defence and of foreign affairs. The minister of national defence must approve foreign cyber operation authorities, and the minister of foreign affairs must also give consent in the case of 'active cyber operations' authorities or be consulted in the case of 'defensive cyber operations' authorities.[119] Canadian legislation also allows the CSE to provide technical and operational assistance to the Canadian Armed Forces (CAF). As for peacetime cyber operations, CAF operations are also subject to all applicable domestic and international law. When conducted under military authorities, offensive cyber operations are subject to a similar level of governance 'rigour' as military 'uses of force', and such offensive cyber operations will be 'subject to all applicable domestic and international law, and proven checks and balances such as rules of engagement, targeting and collateral damage assessments'.[120] Military uses of offensive cyber capabilities require a cabinet-level decision to use force, and will be authorized in the cabinet decision to exercise Crown prerogative to authorize the military operation which they will support.[121] Importantly, Canada's foreign cyber operations carried out by the CSE are bounded, in that they cannot rise to the level of causing (intentionally or negligently) death or bodily harm, nor can they obstruct, pervert or defeat the course of justice or democracy.[122] However, these limitations do not apply to the CAF when, with the operational assistance of the CSE, offensive cyber operations are carried out by the military.[123] Rather, the cyber operations will be approved and controlled by the chief of the Defence Staff through targeting processes and rules of engagement, as would any other 'use of force'.
Czech Republic	The defence minister must authorize offensive cyber operations, and Military Intelligence must also immediately inform the government, the chief of the General Staff of the Czech Armed Forces, the National Office for Cyber and Information Security and other intelligence services once 'active intervention' in cyberspace has commenced.[124]
Denmark	All aspects of Denmark's offensive cyber capability, other than cyber-enabled espionage,[125] are under the authority of the Danish chief of defence (CHOD) and directed by unit J5C of the Danish Defence Command (a specialized unit responsible for cyberspace operations). On order from the CHOD, the actual operations are conducted by the Danish Defence Intelligence Service. The ministry of defence can authorize the CHOD to conduct an offensive cyber operation. In principle, if the damage is estimated to be akin to a conventional attack (that is, physical destruction and/or casualties) then parliament must also give authorization. In practice, it is likely that parliamentary authorization will be sought before any cyberspace attack.[126]
Finland	The Finnish president, as commander-in-chief of the armed forces, has the authority to approve cyberspace operations as for any other operations. In addition, he/she now has the authority to approve military operations where necessary outside of a 'war' due to recent changes in legislation designed to meet the challenges of so-called 'grey zone' threats.[127] The president can delegate this authority as commander-in-chief to a military officer (although this has never happened in peacetime).[128]

[118] Author interview with representative from Belgian Cyber Defence Directorate, 2 August 2021.

[119] Parliament of Canada, House of Commons (2019), 'Statutes of Canada Chapter 13 Part 3', sections 29(1) and (2), 30(1) and (2). Author interview with commanding officer, Combined Cyber Unit (Canadian Armed Forces), and then special adviser to the Deputy Chief of Operational Policy, 16 July 2021, and correspondence in June 2023.

[120] Government of Canada, National Defence (2017), *Strong, Secure, Engaged: Canada's Defence Policy*, https://www.canada.ca/en/department-national-defence/corporate/policies-standards/canada-defence-policy.html, p. 72.

[121] Author interview with commanding officer, Combined Cyber Unit (Canadian Armed Forces), and then special adviser to the Deputy Chief of Operational Policy, 16 July 2021, and correspondence in June 2023.

[122] Parliament of Canada, House of Commons (2019), 'Statutes of Canada Chapter 13 Part 3', section 32.

[123] As provided for in Parliament of Canada, House of Commons (2019), 'Statutes of Canada Chapter 13 Part 3', section 20.

[124] Interview with representative from Ministry of Defence of the Czech Republic, 2 Sep. 2021. See also Czech Republic (2021), *Act No. 150/2021 Act amending Act No. 289/2005 on Military Intelligence, as amended, and certain other Acts*, https://www.zakonyprolidi.cz/cs/2021-150, section 16(2).

[125] Cyber-enabled espionage is conducted in accordance with a special set of laws directing the Danish Defence Intelligence Service.

[126] Interview with Mikkel Storm Jensen, Royal Danish Defence College, 22 June 2021.

[127] Author interview with Director, Cyber Policy Institute, 29 June 2021, and correspondence June 2023.

[128] Author interview with Director, Cyber Policy Institute, 29 June 2021.

State	Authorization mechanism
Netherlands	Article 97 of the Dutch constitution guides the use of offensive cyber capabilities, in stating that the armed forces can be deployed to 'maintain and promote the international legal order'.[129] The process for authorization, as per Article 100, involves a set of questions concerning the financial implications, collateral risks and length of the operation, among other matters. The Dutch Intelligence and Security Services Act 2017 (known as the WIV)[130] was amended in June 2021 to expand the powers of the civilian General Intelligence and Security Service (AIVD)[131] and the Military Intelligence and Security Service (MIVD)[132] to disrupt certain targets in cyberspace, applying a strict proportionality test.[133] The WIV's content and oversight regime also apply to the AIVD and the MIVD. Special operations, which may include offensive cyber operations, are approved by the Ministerial Core Group for Special Operations (MCGS), which comprises the minister of foreign affairs, the minister of defence and the prime minister,[134] on the grounds of national security. Given the national security element, such operations are said to be reserved for occasions when they can generate a strategic effect.[135] The Dutch intelligence agencies are subject to stringent rules and oversight. The AIVD's activities are overseen by two independent committees before, during and after an operation.[136] A new Temporary Cyber Operations Act went before the House of Representatives in December 2022, and remained pending at July 2023.[137] It will allow for more effective and rapid 'hacking', albeit with tighter supervisory controls, prior to, during and after an operation.[138] The cabinet decides on use of offensive cyber capabilities by the military, which must have a mandate for their use, such as acting in self-defence or under the authority of the United Nations. Offensive military cyber operations in peacetime, similar to other offensive military operations, would be exceptional, since the Dutch Defence Cyber Command is primarily mandated to act in an armed conflict. Parliament is then informed prior to use. On informing parliament (i.e. the House of Representatives), pursuant to Article 100 of the constitution, Article 97 – see above – becomes operative. Article 97 states that the Netherlands has armed forces for the defence and protection of the country's interests and to maintain and promote the international legal order.[139] Parliament need only be informed of activity in the second case (to protect the international legal order), and not in a case of self-defence. That said, in practice the Netherlands will inform parliament prior to a mission and will often seek support from a majority in the House.[140] For 'special operations' in the Netherlands where there is no Article 100 mandate, a different authorization process applies. In these cases, the MCGS must give authorization for an offensive cyber operation, reflecting the perceived level of risk and the possible repercussions involved. The MCGS determines when and to what extent the rest of the government should be involved or informed, as well as how and when parliament should be informed.[141]

[129] Government of the Netherlands, *The Constitution of the Kingdom of the Netherlands 2008*, https://www.government.nl/documents/regulations/2012/10/18/the-constitution-of-the-kingdom-of-the-netherlands-2008.

[130] In Dutch, *Wet op de inlichtingen- en veiligheidsdiensten 2017*.

[131] In Dutch, Algemene Inlichtingen- en Veiligheidsdienst.

[132] In Dutch, Militaire Inlichtingen- en Veiligheidsdienst.

[133] Government of the Netherlands (2017), 'Intelligence and Security Services Act 2017', https://wetten.overheid.nl/BWBR0039896/2021-07-15#Hoofdstuk5.

[134] This changes with the accession of each new government, however, and other ministers can be invited to join on a case-by-case basis. Author interview with strategic adviser to Dutch Defence Cyber Command, 21 June 2021.

[135] Author interview with strategic adviser to Dutch Defence Cyber Command, 21 June 2021.

[136] Government of the Netherlands, Ministry of the Interior and Kingdom Relations, General Intelligence and Security Service (2022), 'Wet op de inlichtingen-en veiligheidsdiensten' [Intelligence and Security Services Act], https://www.aivd.nl/onderwerpen/wet-op-de-inlichtingen-en-veiligheidsdiensten.

[137] Government of the Netherlands, Ministry of the Interior and Kingdom Relations, General Intelligence and Security Service (2022), 'Tijdelijke wet cyberoperaties' [Temporary Cyber Operations Act], https://www.aivd.nl/onderwerpen/wet-op-de-inlichtingen-en-veiligheidsdiensten/tijdelijke-wet-cyberoperaties.

[138] Government of the Netherlands, Ministry of the Interior and Kingdom Relations, General Intelligence and Security Service (2022), *AIVD Annual Report 2022*, https://english.aivd.nl/publications/annual-report/2023/06/16/aivd-annual-report-2022, p. 31.

[139] Government of the Netherlands, *The Constitution of the Kingdom of the Netherlands 2008*.

[140] Author interviews with Peter Pijpers, Associate Professor Cyber Operations, Netherlands Defence Academy, 17 June 2021 and 10 July 2023.

[141] Ducheine, P. A. L., Arnold, K. and Pijpers, P. B. M. J. (2020), *Decision-Making and Parliamentary Control for International Military Cyber Operations by the Netherlands Armed Forces*, Amsterdam Law School Legal Studies Research Paper No. 2020-07, https://doi.org/10.2139/ssrn.3540732, p. 1.

State	Authorization mechanism
Norway	The Norwegian Intelligence Service (NIS) directs and controls all offensive cyber operations, in both the military and civilian contexts.[142] The ministry of defence made clear in 2018 that, given the importance of intelligence in offensive cyber operations, the responsibility for conducting offensive cyber operations must be assigned to the NIS. Only the NIS is authorized by law to obtain target information, which is an integral part of offensive cyber operations.[143] The ability to conduct offensive cyber operations necessitates a good understanding of the target, achieved through communications intelligence in conjunction with the use of other intelligence capabilities.[144] The focal point for all offensive cyber in Norway is therefore the head of the NIS. During military operations, the NIS will coordinate activity with the Norwegian Joint Headquarters, and cyber operations will be under political direction and control in line with other kinds of operations.[145]
UK	The UK has made clear that NCF operations are conducted in line with a well-established legal framework, which includes the Intelligence Services Act 1994 and the Investigatory Powers Act 2016. The UK has consistently emphasized that it develops and deploys capabilities in accordance with international law, including the law of armed conflict where applicable. Its activities are subject to ministerial approval, judicial oversight and parliamentary review, 'making the UK's governance regime for cyber operations one of the strongest in the world'.[146] The investigatory powers commissioner keeps the statutory powers used in the conduct of cyber operations under review.[147] The Intelligence and Security Committee of Parliament also provides oversight of the NCF's activities.[148] For the NCF, which is a joint civilian–military entity, the secretaries of state for defence and for foreign, Commonwealth and development affairs have joint accountability for offensive cyber operations, depending on the personnel involved and the location of the target.[149]
US	In August 2018 the US implemented a significant change to the constraints imposed during the Obama administration on conducting offensive cyber operations.[150] Under Obama, Presidential Policy Directive 20 (PPD-20) meant that the president held the authority to decide that offensive cyber activity can be conducted.[151] The Trump administration subsequently delegated authority to the defence secretary to use cyber methods to disrupt or degrade adversary networks,[152] removing the usual authorization process overseen by the National Security Council.[153] The classified National Security Presidential Memorandum 13 (NSPM-13) on United States Cyber Operations Policy is said to have given the DoD authority to engage in cyber activity which falls below the use of force. Reportedly, NSPM-13 therefore enabled more rapid decision-making in conducting cyber operations.[154] The Biden administration is said to have refined NSPM-13 in 2022 to ensure that the 'White House and State Department have more visibility into sensitive military cyber operations' while ensuring that the Pentagon can no longer 'override the State Department's objection to an operation without explanation and without the White House's knowledge'.[155]

[142] The NIS is both a civilian and military intelligence service. See EOS Committee (2023), 'EOS Committee: Norwegian Parliamentary Oversight Committee on Intelligence and Security Services', https://eos-utvalget.no/en/home/about-the-eos-committee/the-eos-services.
[143] Government of Norway, Ministry of Defence (2019), *Proposition to the Storting for a parliamentary resolution*, section 5.3; additional detail from author correspondence with senior scientist at FFI, 2023.
[144] Government of Norway, Ministry of Defence (2019), *Proposition to the Storting for a parliamentary resolution*, section 5.3.
[145] Ibid.
[146] HM Government (2021), *National Cyber Strategy 2022*, p. 15.
[147] Investigatory Powers Commissioner's Office (2019), 'What we do', https://www.ipco.org.uk/what-we-do.
[148] HM Government (2021), *National Cyber Force Explainer*, London: HM Government, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1041113/Force_Explainer_20211213_FINAL__1_.pdf, p. 2.
[149] Ibid.
[150] National Security Presidential Memorandum 13 (NSPM-13) is classified, but several public reports have alluded to its contents. See Nakashima, E. (2018), 'White House authorizes "offensive cyber operations" to deter foreign adversaries', *Washington Post*, 20 September 2018, https://www.washingtonpost.com/world/national-security/trump-authorizes-offensive-cyber-operations-to-deter-foreign-adversaries-bolton-says/2018/09/20/b5880578-bd0b-11e8-b7d2-0773aa1e33da_story.html.
[151] Freedburg, S. J. (2018), 'Trump Eases Cyber Ops, But Safeguards Remain: Joint Staff', Breaking Defense, 17 September 2018, https://breakingdefense.com/2018/09/trump-eases-cyber-ops-but-safeguards-remain-joint-staff.
[152] Nakashima, E. (2018), 'Trump gives the military more latitude to use offensive cyber tools against adversaries', *Washington Post*, 16 August 2018, https://www.washingtonpost.com/world/national-security/trump-gives-the-military-more-latitude-to-use-offensive-cyber-tools-against-adversaries/2018/08/16/75f7a100-a160-11e8-8e87-c869fe70a721_story.html.
[153] The US Cyber Command Vision of 2018 states that 'removing constraints on speed and agility' was necessary to compete and deter in cyberspace. See Jensen, B. and Work, J. D. (2018), 'Cyber Civil–Military Relations: Balancing Interests on the Digital Frontier', War on the Rocks, 4 September 2018, https://warontherocks.com/2018/09/cyber-civil-military-relations-balancing-interests-on-the-digital-frontier.
[154] Lin, H. (2022), 'President Biden's Policy Changes for Offensive Cyber Operations', Lawfare, 17 May 2022, https://www.lawfareblog.com/president-bidens-policy-changes-offensive-cyber-operations.
[155] Nakashima, E. (2022), 'The Biden Administration is refining a Trump era cyber order', *Washington Post*, 13 May 2022, https://www.washingtonpost.com/politics/2022/05/13/biden-administration-is-refining-trump-era-cyber-order.

State	Authorization mechanism
US	The *National Defense Authorization Act for Fiscal Year 2019* (NDAA) authorized the DoD to conduct 'military cyber activities or operations in cyberspace, including clandestine military activities or operations in cyberspace, to defend the United States and its allies' in situations 'short of hostilities […] or in areas in which hostilities are not occurring'.[156] The DoD cannot *direct* specific operations, however: only the US president can do that. The NDAA for 2019 also confirmed that military cyber operations were classed as 'traditional military activity' which do not therefore require the usual approval and oversight required for covert activity.[157] The US Congress has, however, retained oversight for 'sensitive military cyber operations' (SMCOs) through a transparency rule for the defence secretary in which he or she must send a written notification to the Senate Armed Services Committee within 48 hours of any such operation.[158] An operation will be classed as an SMCO if it is intended to have an effect on a foreign terrorist organization or foreign government, outside the context of an ongoing US military operation, and entails one of five specified risk scenarios.[159] Further reporting requirements under the NDAA for fiscal year 2020 require notification within 15 days of any delegation by the president to the defence secretary for military operations in cyberspace that would otherwise be at the National Command Authority[160] level (i.e. for cyber operations outside the DoD's information network against China, Iran, North Korea or Russia).

Clear authorization mechanisms at the highest levels should be maintained for offensive cyber operations to demonstrate a measurable commitment to control over the use of such capabilities. The invisibility of cyber activity also increases the importance of robust independent oversight of these activities. This would go a long way towards enhancing understanding of the balance between the need to ensure an open and secure cyberspace for all and the need to use offensive cyber capabilities. This approach would also lend greater credibility to those states who support responsible state behaviour in cyberspace.

Clear authorization mechanisms at the highest levels should be maintained for offensive cyber operations to demonstrate a measurable commitment to control over the use of such capabilities.

All offensive cyber activity should be assessed in terms of how it supports or undermines norms of responsible state behaviour in cyberspace more broadly. For example, while levels of authorization suggest that concerns over the risk of harm and/or escalation from offensive cyber capabilities exist, it is hoped that planning also includes assessments of how such operations can contribute to strategic

[156] *One Hundred Fifteenth Congress of the United States of America at the Second Session, John S. McCain National Defense Authorization Act for Fiscal Year 2019*, Public Law 115–232, https://www.congress.gov/115/bills/hr5515/BILLS-115hr5515enr.pdf, section 1632.
[157] Ibid. This would normally require a written presidential 'finding' and reporting to the House and Senate Select Committees on Intelligence.
[158] United States Code, Title 10, Section 130f(a), https://uscode.house.gov. See also *One Hundred Fifteenth Congress of the United States of America at the Second Session, John S. McCain National Defense Authorization Act for Fiscal Year 2019*, section 1632.
[159] These are: involving a medium or higher collateral effects estimate; intelligence gain/loss; risk of political retaliation; probability of detection; or actual collateral effects. See Chesney, R. M. (2022), 'The Domestic Legal Framework for US Military Cyber Operations', in Goldsmith, J. (ed.) (2022), *The United States' Defend Forward Cyber Strategy*, p. 84. For more detail on what has been termed a 'grey area' in this respect, see Bailey, C. E. (2020), 'Offensive Cyberspace Operations: A Gray Area in Congressional Oversight', *Boston University International Law Journal*, 38(2), pp. 240–85, https://www.bu.edu/ilj/files/2020/08/10.-Article_Bailey.pdf.
[160] The National Command Authority is a 'term used to collectively describe the President and the SecDef [Secretary of Defense]' from which 'directions for military operations emanate'. See The Judge Advocate General's Legal Center and School (2022), *Operational Law Handbook,* https://tjaglcs.army.mil/documents/35956/56931/2022+Operational+Law+Handbook.pdf, pp. 133–4.

goals rather than limited short-term tactical objectives. As the commander of USCYBERCOM made clear in 2019, 'superiority in cyberspace is temporary; we may achieve it for a period of time, but it's ephemeral'.[161] Showing whether and how states seek to measure the positive and the possible negative effects of any offensive cyber activity can help to shine a light on how states manage perceived risk in this area. As states are unlikely to publish how they seek to measure effect even where such formal metrics do exist, very little is publicly known as to whether, let alone how, states conduct measures of effect. Clear, ongoing methods to measure both short and long-term effects, including but not limited to strategic, political and physical effects, should therefore be established and publicly acknowledged, even if the details remain closed.

[161] Joint Force Quarterly (2019), 'Defending Forward: An Interview with Paul M. Nakasone', *Joint Force Quarterly*, 92, pp. 4–9, https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-92.aspx.

04 Conclusion and recommendations

The development and use of offensive cyber capabilities requires a sophisticated and appropriately tailored strategy, with consideration for how both effect and risk are measured and mitigated, and clear links to legal authorities. States must also do more to assess where the true utility of offensive cyber operations lies.

A historical lack of transparency, combined with ongoing 'cyber hyperbole' relating both to the utility and risks of use of offensive cyber operations, has clouded a more informed understanding of such operations. Many states have at last started to take steps to alleviate concerns over the invisibility of cyberspace by publishing details of *why* they seek to develop these capabilities, and in what circumstances they may have been used thus far. National laws can also reveal how their use is authorized and governed, helping to shed light on their circumstances for use and states' perceptions of risk in this area. Given the broader concerns and divide in the discourse over risks of inadvertent harm and escalation, these details are important.

How responsible actors set the scene going forward will not just set precedents for adversaries. In addition, smaller states whose current focus may be restricted to cyber counter-attacks and defensive capabilities are likely to observe and learn from the actions of bigger cyber powers when developing their own offensive cyber capabilities. Even if one concludes that offensive cyber capabilities are not inherently escalatory, cyberspace is nonetheless fundamentally different to other so-called 'domains'. As explored in this paper, offensive action in cyberspace carries a very different nature and scale of risk, and may have consequences that reach much further, such that the development and use of offensive cyber capabilities require a sophisticated and appropriately tailored strategy. How both effect and risk are measured and mitigated constitutes a critical element of a well-defined, meaningful cyber strategy, together with clear links to legal authorities for cyber activity.

Given the residual ambiguity on the true utility of using offensive cyber capabilities, set against a significant divide in the discourse as to risks of escalation, offensive cyber tools may be better understood and portrayed as one lever of state power among others, rather than a magical solution to a whole range of challenges. In some situations they may be the least risky or the least damaging option, but in others they may be highly destabilizing or escalatory, depending on the context and the nature of the target. Further, offensive cyber operations in peacetime may have utility as a versatile means of projecting both hard and soft power, and may sometimes demonstrate clear advantages over other methods, but too few states have yet publicly articulated this in sufficient detail. There is a risk that the 'silver bullet' of offensive cyber is touted as a possible solution to a wide variety of challenges, and its versatility asserted to be sufficient justification for use, while downplaying the reality – that successful cyber operations are the work of long-term, tailor-made operations with only a brief window for success and with considerable associated risks. While offensive cyber operations may become more routine or 'normalized', states should also be wary of using them as a tool of choice, or the default option. An overzealous acceptance of the supposed benefits of offensive cyber as a 'silver bullet' solution does not account for the fact that different contexts require very different responses and/or alternative tools.[162]

States must therefore do more to assess where the true utility of offensive cyber operations lies, so as to justify their use when it matters, moving away from overly broad generalizations in relation to versatility and employability. At the same time, complacency as to the power and effect of the chosen operations should be avoided. This is particularly important, as offensive cyber gradually becomes 'normalized' as more states establish military cyber commands or units, or publicly avow their offensive cyber capabilities. Reliance on offensive cyber capabilities must also not be at the expense of other means of soft power including restraint and influence, which may prove more effective depending on context. Consideration of other tools or methods is all the more important in light of the lack of clarity in whether and how states measure the short- and long-term effects of offensive cyber operations.

Possession of offensive cyber capabilities, in and of itself, does not appear to have effective deterrent value in cyberspace below the level of a use of force – the arena in which the majority of today's cyber activity takes place. Assumptions about the deterrence value of offensive capabilities in cyberspace must therefore not be at the expense of ensuring effective cyber defence and resilience. Cyber strategies must provide meaningful assessment of the value of offensive cyber capabilities, avoiding default references to poorly understood 'deterrence'.

[162] For example, Daniel Moore proposes two distinct types of offensive cyber operations ('presence-based' and 'event-based'), each with very different utility, advantages and disadvantages, rather than combining all offensive cyber into one basket. See Moore, D. (2022), *Offensive Cyber Operations: Understanding Intangible Warfare,* London: Hurst, p. 71.

This study has shown that many democratic states continue to keep a firm hold over their use of offensive cyber, and require authorization at high levels, suggesting that how and when these capabilities are used are likely to be only in extremis. This may be due to several reasons, not least a reluctance to reveal the nature or extent of states' offensive cyber capabilities, but it nonetheless appears that concerns over risks of use remain. Clear authorization mechanisms at the highest levels are important to project a clear commitment to control over and responsible use of these capabilities. Clarity remains critical in respect of authorities, including how, and under what circumstances, they may be delegated – if at all.

States can, and should still, do more to give meaningful detail as to how they manage and measure risks of use, to inform the broader discourse on responsible state behaviour in cyberspace. Specifically addressing the risks of use publicly in this way can boost the credibility of those states whose stated intentions are to adhere to international law and norms of responsible state behaviour in cyberspace. This would also enable a better understanding of the meaning of 'responsible use' of cyber capabilities.

While cyber strategies rightly focus on cyber threats stemming from adversaries, internal measures of effect stemming from states' own use of offensive cyber are equally important. The extent to which states have clear methods to measure the effectiveness of cyber activity in pursuing strategic aims is therefore important. States could add transparency in this regard by making clear the importance of adopting measures of effect, even if their content is not made public. This is particularly important for those states who routinely (or seek to routinely) use offensive cyber capabilities in peacetime, particularly in the long term.[163] For those states which may seek to adopt a persistent engagement posture in cyberspace, for example, it may be more challenging to establish metrics for success beyond achieving short-term 'win'. Some have suggested that there may be no way of assessing whether more engagement will reduce the likelihood of conflict, and have highlighted the dangers of 'positive feedback' in this regard.[164] States should therefore establish internal metrics that measure both short- and long-term effect, taking into account a wide range of factors and indicators.

Above all, cyber strategies must meaningfully articulate how the development and use of offensive cyber capabilities aligns with a commitment to a secure cyberspace for all.

[163] For example, the US Cyberspace Solarium Commission's 2020 *Report* called for metrics to be conducted by the Department of Defense which can measure whether defend forward operations are effective from the tactical to the strategic level. Section 1634 of the National Defense Authorization Act for 2020 also called for a report on both qualitative and quantitative metrics. See US Cyberspace Solarium Commission (2020), *Report*, p. 117.
[164] Healey, J. (2018), 'Triggering the New Forever War, in Cyberspace', The Cipher Brief, https://www.thecipherbrief.com/article/tech/triggering-new-forever-war-cyberspace.

Policy recommendations

The following recommendations are designed to assist states in establishing or developing their approaches to use of offensive cyber by outlining key priority areas. As states differ in their offensive cyber capacity and policy objectives, these are intended to be broad achievable guidelines for all democratic states.

- States must continue to move away from the historic secrecy that has clouded an informed understanding of offensive cyber activity. This will require more – and continuing – transparent communication on an ongoing basis as to the basis for use and management of offensive cyber capabilities, which can be achieved without compromising operational security.

- A more nuanced understanding of the utility and value of offensive cyber capabilities should be fostered across government at the national level. Use of offensive cyber is neither a 'silver bullet' solution nor a matter of 'one size fits all', as whether and how an offensive cyber operation should be used will depend on context. Offensive cyber activity must not become the default or 'go-to' offensive method of choice; nor must it be used to pursue lesser national interests that have little strategic importance in peacetime.

- States should prioritize where and how offensive cyber can serve deterrence postures in cyberspace, rather than relying on overly broad assumptions about this means of deterrence, which may be unrealistic in practice and may come at the expense of cyber resilience. States should determine whether deterrence through cyberspace should instead focus on specific threats in specific circumstances.

- All planning must include steps to mitigate the risk of inadvertent harm and escalation when using offensive cyber capabilities. This should include an assessment of how the intended effect will contribute to strategic goals rather than limited short-term tactical objectives, and the risk of broader effects, unintended effects or collateral damage, in cyberspace and in other domains. States should consider different methods of communicating intent appropriately to an adversary, so as to minimize misinterpretation. Policymakers must also be assisted in understanding technical risk in cyberspace.

- Clear authorization mechanisms at the highest levels should be maintained for offensive cyber operations, to demonstrate a measurable commitment to control over the use of such capabilities. Decisions as to use of offensive cyber operations should also involve broader cross-government or inter-agency input. The invisibility of cyber activity is all the more reason for robust independent oversight of these activities, with consideration being given to whether certain types of offensive cyber activity require prior notification to oversight bodies and an ongoing assessment as to whether the oversight mechanisms are fit for purpose as capabilities and strategic priorities evolve. At the same time, oversight committees must have sufficient understanding of the mechanics of offensive cyber operations.

- Clear, ongoing methods to measure both short- and long-term effects, including but not limited to strategic, political and physical effects, should be established, particularly for states which may in due course seek to engage more routinely in cyberspace, in ways akin to persistent engagement. States must also make clear that such methods exist, even if the details remain closed. Specifically addressing the risks of use more publicly can also boost the credibility of those states whose stated intentions are to adhere to international law and norms of responsible state behaviour in cyberspace. All offensive cyber activity should include an assessment of how the intended operation may support norms of responsible state behaviour in cyberspace more broadly and what precedent – good or bad – it may set for both allies and adversaries.

- Cyber strategies must include specific recognition of the need to secure a balance between an open and secure cyberspace for all, on the one hand, and the need to use offensive cyber capabilities, on the other. Maintaining a trusted and secure internet should be prioritized above using offensive cyber capabilities. Both objectives are achievable if offensive cyber capabilities are used responsibly, and if the meaning of 'responsible use' is properly articulated, defined and communicated.

Annex 1

Interviews

A comprehensive study of all states' views and positions in cyberspace at any given point in time is a steep challenge, yet an analysis of a handful of democratic states which are known to have offensive cyber capabilities can still be instructive. Research for this paper was qualitative and is based on publicly available documents such as cyber strategies, legislation and national security strategies, as well as interviews with experts in some states. It was observed that not all states have the same quality or quantity of public material on the issues addressed in this paper. This observation was in itself a key finding in relation to the overall lack of transparency as to many states' approaches to the use of offensive cyber.

Interviews were conducted with cyber experts from nine different NATO states. Some other states were not ready to be interviewed, which perhaps reveals the residual nervousness attached to public discussion about offensive cyber. Many states are still considering how best to articulate their respective positions on offensive cyber into their national strategies. Others, perhaps understandably, may wish to control their own narrative in this regard. The interviews were undertaken with cyber specialists based in a given state, using a standard question set included below at Annex 2, albeit with some variation, with specific questions being posed – for example in relation to aspects of a state's cyber history or authorization framework which were unique to that state.[165]

Finally, it is recognized that in such a fast-moving arena, there may be strands of this research which will later require refinement, as future events disrupt current findings. It is important to continually challenge perceived wisdom, particularly given that discourse on this topic is frequently characterized by hyperbole and/or oversimplification.

[165] For example, with the United States, some questions focused on defend forward and the authorities under the 2019 National Defense Authorization Act.

Annex 2

Core interview question set

Questions about [state's] specific policy/position:

- What value does [state] place on having offensive cyber capabilities?
- How does [state] prioritize defence and offence in the cyber domain?
- How does [state] mitigate risks of using offensive cyber capabilities?

Questions for wider discussion on use of offensive cyberspace more generally:

- What in your view is the longer-term impact of more states developing cyber commands and offensive cyber capabilities?
- Does having offensive cyber capabilities contribute to deterrence and if so, how? If not, why not?
- How does the development of offensive cyber align with wider goals of an open, secure and free internet?
- How should states prioritize offence and defence in cyberspace?
- Are fears of (inadvertent) escalation in cyberspace through use of offensive cyber unfounded or overhyped?
- Is cyberspace in fact characterized by a system of restraint? If so, is this likely to last?
- What does being a responsible cyber state mean in practice?
- How can states mitigate the wider risks of using offensive cyber tools?
- Are offensive cyber operations becoming 'normalized' as part of state competition? What are the risks of this or does this in fact contribute to stability?
- Do persistent engagement strategies increase stability in cyberspace? What is their likely longer-term impact? How can the 'success' or otherwise of persistent engagement be measured or assessed?
- Is the oversight and authorization process for use of offensive cyber in [state] sufficiently transparent?
- What might the impact of a joint military–intelligence organization be on stability in cyberspace? Might it contribute to the cybersecurity dilemma?
- Should states declare some areas off limits when using offensive cyber capabilities? How might this work in practice?

About the author

Juliet Skingsley commissioned into the British Army in 2012 and currently serves as a lawyer in the Army Legal Services (ALS).

She has served in Germany and the UK, and has deployed on operations overseas as a UK military legal adviser. She was the Army Chief of the General Staff Research Fellow at Chatham House during 2020–21.

Juliet's research focuses on information operations and the international law of cyber operations.

Acknowledgments

The analysis in this paper draws upon interviews and correspondence with cyber experts from nine NATO states, as well as academics and former cyber practitioners. The author would like to thank all those who gave their valuable time to share their views and their knowledge. In particular, the author would like to express her sincere thanks to John Bruce, Vera Chapman Browne, Pierre Ciparisse, Joyce Hakmeh, Christopher Horner, Hannah Hovinga, Mikkel Storm Jensen, Mika Kerttunen, Patricia Lewis, Mass Soldal Lund, Chris Painter, Henrik Palbo, Peter Pijpers, Kurt Sanger, James Shires, Aasmund Thuv, Beyza Unal and Gary Wolfman. The author would also like to thank the anonymous peer reviewers for their helpful comments on the paper.

This publication was made possible by the author's time as a visiting research fellow in Chatham House's International Security Programme, facilitated by the British Army's External Placement Programme. The views expressed in the publication are those of the author, and may not necessarily reflect the views or position of the UK Ministry of Defence.

Chatham House does not express opinions of its own. The opinions expressed in this publication are the responsibility of the author(s).

Cover image: NATO interoperability exercise at Joint Force Training Centre, Bydgoszcz, Poland, 22 June 2017.
Photo credit: Copyright © Jaap Arriens/Nur Photo/Getty Images

ISBN 978 1 78413 585 0
DOI 10.55317/9781784135850

Cite this paper: Skingsley, J. (2023), *Offensive cyber operations: States' perceptions of their utility and risks*, Research Paper, London: Royal Institute of International Affairs, https://doi.org/10.55317/9781784135850.

This publication is printed on FSC-certified paper.
designbysoapbox.com

Independent thinking since 1920

CHATHAM HOUSE

The Royal Institute of International Affairs
Chatham House
10 St James's Square, London SW1Y 4LE
T +44 (0)20 7957 5700
contact@chathamhouse.org | chathamhouse.org

Charity Registration Number: 208223