CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

The Five Eyes and Offensive Cyber Capabilities: Building a 'Cyber Deterrence Initiative'

Josh Gold

NATO CCDCOE Non-Resident Visiting Scholar

Tallinn 2020

About the author

Josh Gold is a NATO CCDCOE Non-Resident Visiting Scholar, and a research assistant at Citizen Lab, at the University of Toronto's Munk School of Global Affairs and Public Policy. Josh's research focuses on international cyberspace governance and conflict in cyberspace. Josh has previously worked various contracts including as a consultant for the Estonian Ministry of Foreign Affairs' cyber policy team, and in threat intelligence at CyberCube. He holds a bachelor's degree in peace and conflict studies from the University of Toronto. Josh is on Twitter at @joshgold3.

CCDCOE

The NATO CCDCOE is a NATO-accredited cyber defence hub focusing on research, training and exercises. It represents a community of 29 nations providing a 360-degree look at cyber defence, with expertise in technology, strategy, operations and law. The heart of the Centre is a diverse group of international experts from military, government, academia and industry backgrounds.

The CCDCOE is home to the Tallinn Manual 2.0, the most comprehensive guide on how international law applies to cyber operations. The Centre organises the world's largest and most complex international live-fire cyber defence exercise Locked Shields and hosts the International Conference on Cyber Conflict (CyCon), a unique annual event in Tallinn, joining key experts and decision-makers from the global cyber defence community. As the Department Head for Cyberspace Operations Training and Education, the CCDCOE is responsible for identifying and coordinating education and training solutions in the field of cyber defence operations for all NATO bodies across the Alliance. The Centre is staffed and financed by its member nations: Austria, Belgium, Bulgaria, Croatia, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Montenegro, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. NATO-accredited centres of excellence are not part of the NATO Command Structure.

www.ccdcoe.org
publications@ccdcoe.org

Disclaimer

The views expressed in this paper belong to the author of the paper. This publication is a product of the NATO Cooperative Cyber Defence Centre of Excellence (the Centre). It does not necessarily reflect the policy or the opinion of the Centre or NATO. The Centre may not be held responsible for any loss or harm arising from the use of information contained in this publication and is not responsible for the content of the external sources, including external websites referenced in this publication. Digital or hard copies of this publication may be produced for internal use within NATO and for personal or educational use when for non-profit and non-commercial purpose, provided that copies bear a full citation.

Acknowledgements

The author would like to sincerely thank the following people for offering their time and expertise to bounce thoughts, reviewing sections of this paper, or otherwise providing assistance: Siim Alatalu, Greg Austin, Jakob Bund, Joe Burton, Rob Mazzolin, Paul Meyer, Mark Pomerleau, Holly Porteous, Max Smeets, Maria Tolppa, Tom Uren, Adrian Venables, Mike Widmann, & Andrew Williams. Special thanks go to Amy Ertan, Jim Lewis, Chris Parsons and Piret Pernik, who generously reviewed the full-length paper and provided in-depth comments to improve the final product. Additional thanks go to NATO CCDCOE reviewers Tania Jančárková, Damjan Štrucl and Sungbaek Cho and to the several anonymous experts who verified facts and provided immensely helpful comments and advice. This paper benefitted from a presentation and subsequent discussion at the June 2020 Closing the Gap Conference; for this the author would like to thank the EU Cyber Direct team including Patryk Pawlak, Nathalie Van Raemdonck and Fabio Barbero.

Table of Contents

1. Abstract

Countries around the world are increasingly developing offensive cyber capabilities (OCCs) but there are differences in how, if at all, these are acknowledged publicly. Many democracies argue that developing and even using OCCs is not necessarily harmful or destabilising, but rather it depends on *how* they are used. Under this view, OCCs are legitimate so long as their use aligns with accepted norms and international legal obligations. This paper explores how each of the Five Eyes countries (the United States, United Kingdom, Australia, Canada and New Zealand) speaks publicly about its respective offensive cyber capabilities – including how these capabilities might be used. In other words, the paper examines how transparent these five intelligence partners are toward their OCCs. The examination indicates a move toward a collective response through the US-led Cyber Deterrence Initiative (CDI), which seeks to justify some degree of action in response to transgressions of the United Nations-based norms for responsible behaviour and international law. The paper concludes by discussing the notion of transparency, suggesting that transparency toward how the Five Eyes' OCCs will be used is important for the credibility of their collective response, while also noting potential challenges for the way forward.

2. Introduction

Everybody is moving towards developing offensive cyber capabilities.

— General Keith Alexander, Commander US Cyber Command, May 2014[1]

In July 2015, the United Nations (UN) Group of Governmental Experts (GGE) on information and communications technologies (ICTs) in the context of international security, released a consensus report which was endorsed by all members of the UN General Assembly that same year.[2] The report presented eleven non-binding norms for responsible state behaviour in cyberspace and reaffirmed the applicability of international law in cyberspace and the importance of confidence-building measures (CBMs) to increase transparency and reduce the risk of conflict. Taken together with the recommendations of previous GGEs, these norms constitute a UN-based international cyber stability framework to facilitate global peace and stability.[3]

The 2015 GGE report also recognised the development of ICT capabilities for military purposes by states and that the use of such capabilities in inter-state conflict was becoming more likely.[4] According

[1] Christopher Joye, 'Interview transcript: former head of the NSA and commander of the US cyber command, General Keith Alexander', The Australian Financial Review. May 9, 2014, https://www.afr.com/technology/interview-transcript-former-head-of-the-nsa-and-commander-of-the-us-cyber-command-general-keith-alexander-20140508-itzhw.

[2] UNGA. 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', A/70/174, July 22, 2015, https://undocs.org/A/70/174.

[3] US Department of State, 'Joint Statement on Advancing Responsible State Behavior in Cyberspace', September 23, 2019, https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/.

[4] UNGA. A/70/174, 6.

to a joint statement by three top American intelligence officials in early 2017, more than 30 countries were developing 'offensive cyberattack capabilities'.[5]

Yet there are differences in how, if at all, countries acknowledge their offensive cyber capabilities (OCCs), which has led to international contention. For example, views differ at the UN on the concept of the 'militarisation' of cyberspace. Some states such as Russia, China and Iran call for a ban on the development and use of OCCs by states and tend to avoid admitting that they use these capabilities themselves.[6] By contrast, Western countries – especially those which are capable cyber actors – advocate for acknowledging and speaking transparently about OCCs. These latter states claim that OCCs are a reality and call for clarity from states on how such capabilities are to be used. They posit that transparency leads to accountability, predictability and thus stability and do not take issue with the capabilities themselves so long as their use aligns with accepted norms of the UN cyber stability framework and international humanitarian law.

This paper looks more closely at the narrative which promotes transparency toward state OCCs. It focuses on the countries of the 'Five Eyes' intelligence-sharing alliance – the United States (US), United Kingdom (UK), Australia, Canada and New Zealand – and describes how each talks publicly about its respective OCCs, particularly in terms of rules around their use and broader strategy concerning such capabilities. The analysis is framed through US strategic moves to build and consolidate collective responses together with international partners through the Cyber Deterrence Initiative (CDI).[7]

The examination of the statements and documents of each of the five countries shows a general trend toward collective response. This collective response, represented by the CDI, seeks to justify some degree of action in response to transgressions of the UN cyber stability framework, including the norms for responsible behaviour in cyberspace and international law. While some countries argue at the UN about the dangers of 'militarising' cyberspace and demand a ban on OCCs, the Five Eyes countries generally support legitimising their development – and justifying their use – by incorporating OCCs into the international framework governing the use of force and coercion. The positions of the US and those of at least some of its Five Eyes partners indicate a desire to be able to respond forcefully to violations of the UN cyber stability framework so as to uphold it – and also makes clear that some of these responses could come in the form of offensive cyber actions.

Building on the findings of the five cases, the paper closes by returning to the notion of transparency. If indeed the Five Eyes countries are moving toward a collective response approach like the CDI, then transparency toward OCCs and how they are used will be important for making such an approach credible. As the Five Eyes and other like-minded democracies head toward a strategy of jointly imposing consequences in response to malicious state-driven cyber activity, common understandings and approaches are needed among allies to synchronise action and bolster credibility. At the same time, further study is needed of the relationships between transparency, credibility and accountability in this context.

[5] James R. Clapper, Marcel Lettre, & Michael S. Rogers, 'Foreign Cyber Threats to the United States', January 5, 2017, https://www.armed-services.senate.gov/imo/media/doc/Clapper-Lettre-Rogers_01-05-16.pdf?fbclid=IwAR3zLIXbhy-2ggxkXk4FEmJD4JkEfvWWK_-RDf3ONtesa80k9ypTEeTV90g.

[6] Josh Gold, 'A Cyberspace 'FIFA' to Set Rules of the Game? UN States Disagree at Second Meeting', *Net Politics (Blog)*, March 2, 2020, https://www.cfr.org/blog/cyberspace-fifa-set-rules-game-un-states-disagree-second-meeting.

[7] The concept of the CDI was first introduced in US 2018 National Cyber Strategy, which states that the US will work with like-minded countries to coordinate and support each other's responses to 'significant' malicious cyber incidents, including – inter alia – through 'the joint imposition of consequences against malign actors'. Further public information is scant, though this paper hopes to begin discussion of what it might look like. The CDI may be related to the 'Joint Statement on Advancing Responsible State Behavior in Cyberspace', a September 23, 2019 joint declaration by the US and 26 other countries: https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/.

3. Country Cases: The Five Eyes and Offensive Cyber Capabilities (OCCs)

The 'Five Eyes' refers to the close intelligence-sharing partnership between Australia, Canada, New Zealand, the UK and the US, which emerged from US-UK intelligence sharing during WWII. The partnership involves close cooperation between the five countries' signals intelligence (SIGINT) agencies and close ties between other security, intelligence and police services.[8] This paper focuses on the Five Eyes countries because of: their historic and closely integrated security collaboration; the fact that they include the US – which is recognised as the leading cyber-power globally[9] and the champion of the CDI; the fact that four of the five have acknowledged OCCs; their common nature as consolidated democracies; and their extensive accountability mechanisms for their intelligence agencies.[10]

Methodologically, this paper relies predominantly on unclassified open-source documents, with only a few exceptions when formerly classified, but now-public, documents are used to emphasise or clarify key points. Thus, while secrecy is routinely a challenge that authors must overcome when writing about classified government programmes, this challenge is mitigated by focusing only on what is publicly available, though with an acknowledgement that such information may not reflect the full scope of offensive doctrine and the thinking and aims behind proposed strategic measures such as the CDI. Much of the material released to the public domain may be conducted purposefully as a form of signalling, both in terms of public documents and statements and declassified documents. However, public endorsement by states of the UN norms of responsible state behaviour and international humanitarian law may be a starting point for understanding their positions.

This paper follows the definition of OCCs proposed by researchers at the Australian Strategic Policy Institute, who wrote:

> In the context of cyber operations, having a capability means possessing the resources, skills, knowledge, operational concepts and procedures to be able to have an effect in cyberspace […] Offensive cyber operations use offensive cyber capabilities to achieve objectives in or through cyberspace.[11]

While this paper takes a wide scope in assessing OCCs, it does not attempt to account for all elements of OCCs as they pertain to the Five Eyes countries.[12] Specifically, although this paper takes note of how

[8] James Cox, 'Canada and the Five Eyes Intelligence Community', *OpenCanada*, December 18, 2012, https://www.opencanada.org/features/canada-and-the-five-eyes-intelligence-community/. Note that while this paper discusses the Five Eyes partnership in the context of collective response (i.e.: the CDI), the two concepts are separate; the Five Eyes is not a deterrence nor collective defence partnership *per se*.

[9] Julia Voo et. al., 'National Cyber Power Index 2020', Belfer Center for Science and International Affairs, Harvard University, September 2020, https://www.belfercenter.org/publication/national-cyber-power-index-2020.

[10] See, for example Richard Morgan, 'Oversight through Five Eyes: Institutional Convergence and the Structure and Oversight of Intelligence Activities', in *Global Intelligence Oversight: Governing Security in the Twenty-First Century*, by Zachary K. Goldman and Samuel J. Rascoff, 2016, or Cat Barker et. al., 'Oversight of Intelligence Agencies: A Comparison of the 'Five Eyes' Nations', Library of Parliament, Canada, December 13, 2017.

[11] Tom Uren et. al., 'Defining offensive cyber capabilities', Australian Strategic Policy Institute, July 4, 2018, https://www.aspi.org.au/report/defining-offensive-cyber-capabilities. While there are also references to offensive cyber *operations* in this paper, those are of secondary importance to the analysis.

[12] Given considerations for scope, in-depth discussion is avoided on law (domestic or international), accountability mechanisms (such as oversight and review), attribution, electronic warfare and intelligence collection, despite the

each country defines OCCs, it is mainly concerned with what each country says about how OCCs might be used, particularly concerning nations' adherence to norms and international law and of the CDI. Due partly to a lack of public information, the paper does not examine the differences between OCCs used for military versus intelligence purposes, nor does it focus on the specific operations and capabilities themselves.

3.1 United States

The US has a long history of operating in cyberspace. Various American public documents and policy statements have defined the terms related to cyberspace activities and capabilities and outlining strategy and doctrine, including the decision-making process, organisational structure and rules.[13]

The US military's 2018 Joint Publication 3-12 on Cyberspace Operations is the authoritative source of US military doctrine related to Cyberspace Operations (CO) in general and Offensive Cyberspace Operations (OCO) in particular.[14] The document presents OCO in extensive detail, defining them as 'CO missions intended to project power in and through foreign cyberspace' by actions taken in support of national objectives.[15] The doctrine further elaborates that 'OCO may exclusively target adversary cyberspace functions or create first-order effects in cyberspace to initiate carefully controlled cascading effects into the physical domains'.[16] OCO missions may also comprise actions that constitute the use of force, including those actions resulting in physical damage to, or the destruction of, enemy systems.[17]

Cyberspace mission objectives are achieved by various actions, including 'cyberspace attack'. Cyberspace attack actions are conducted in foreign cyberspace and are designed to create both 'noticeable denial effects' like degradation, disruption, or destruction, and manipulation actions that result in denial effects in physical domains.[18]

The US, particularly its military, has released myriad documents which either directly describe or relate to OCCs and how these are used by the US military.[19] In this regard, the country's agencies are transparent, appearing comfortable to discuss such capabilities and their doctrine without revealing information about the capabilities themselves, nor about other sensitive specifics. Most relevant to this paper, though, is information on *how* these capabilities might be used and for what purpose.

relevance of these and other topics. Discussion around the differences between military and intelligence capabilities and operations is also largely avoided, as is close discussion of organisational structure, chains-of-command, standard operating procedures and various other operational or doctrinal points. The paper also avoids delving into the academic literature surround transparency, credibility and accountability. Moreover, the paper predominantly relies on unclassified open source documents, with some minor exceptions.

[13] In addition to many public documents, dozens of classified documents made public via Freedom of Information Act requests can be found on the website of the National Security Archives: https://nsarchive.gwu.edu/briefing-book/cyber-vault/2016-01-20/united-states-cyberspace-military-organisation-policies-activities.

[14] 'Cyberspace Operations', Joint Publication 3-12 (JP 3-12), Department of Defense (USA), 8 June, 2018, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf. This document also lists various other relevant documents and policies with which it is meant to interoperate.

[15] 'Cyberspace Operations', Joint Publication 3-12 (JP 3-12), Department of Defense (USA), II-5.

[16] Ibid.

[17] Ibid., II-4.

[18] Ibid.: JP 3-12 explains in some depth what it means by each of these terms (deny, degrade, disrupt, destruct, manipulate); see p. II-7.

[19] See, for example, a compilation of such documents on the website of the National Security Archive, especially the 'USCYBERCOM Documents Timeline': https://nsarchive.gwu.edu/news/cyber-vault/2020-05-11/uscybercom-documents-timeline.

According to the 2019 National Defence Authorization Act (NDAA):

> '[i]t shall be the policy of the United States, with respect to matters pertaining to cyberspace, cybersecurity and cyber warfare, that the United States should employ all instruments of national power, *including the use of offensive cyber capabilities*, to deter if possible and respond to when necessary, all cyberattacks or other malicious cyber activities of foreign powers that target United States interests'[20]

The document adds that the US will develop and, when appropriate, demonstrate the existence of cyber capabilities to impose costs on any foreign power targeting the US with malicious cyber activity.[21]

Significantly, the NDAA amends Title 10 of the United States Code – which clarifies the role of the armed forces – to expand US Cyber Command's (USCYBERCOM) authority to conduct traditional military activities in cyberspace and military activities that are short of hostilities and outside areas of hostilities.[22] This expansion makes it easier and more expedient for USCYBERCOM to conduct cyber operations because it removes Title 10-induced interagency friction that historically limited USCYBERCOM's ability to conduct cyber operations with effects outside of combat zones.[23] For example, the NDAA enabled clandestine military operations in 2018 by USCYBERCOM against the Russia-based 'Internet Research Agency' troll farm[24] which, presumably, would not have been permissible before the amendment of Title 10.

Section 1642 of the NDAA specifically authorises the Department of Defense (DOD) to conduct OCO against four specific adversary countries: Russia, China, North Korea and Iran.[25] It offers relatively broad parameters for doing so, stating that if one of these four countries is conducting an 'active, systematic and ongoing campaign of attacks' against the US government or people (including attempts at influencing democratic processes), USCYBERCOM may be authorised to 'take appropriate and proportional action in foreign cyberspace to disrupt, defeat and deter such attacks'.[26]

More generally, significant changes have been made to the authorities that allow the DOD to conduct CO. In August 2018, National Security Presidential Memorandum 13 (NSPM13) updated these authorities and it was reported by May 2019 that the changes allowed USCYBERCOM to conduct more CO than in the previous ten years combined.[27] NSPM13 allows the military to engage more easily in 'actions that fall below the "use of force" or a level that would cause death, destruction or significant

[20] United States House Armed Services Committee, 'H.R.5515 - John S. McCain National Defense Authorization Act for Fiscal Year 2019', Washington, D.C., U.S. GPO, 2019, https://www.congress.gov/bill/115th-congress/house-bill/5515/text, s. 1636, p.491. *Italics* added by author for emphasis.

[21] Ibid.

[22] Ibid., 489. The USCYBERCOM is a US military unified combatant command which directs, synchronises and coordinates cyberspace planning and operations to defend and advance US national interests together with domestic and international partners. See more: https://www.cybercom.mil/.

[23] Robert Chesney, 'The Law of Military Cyber Operations and the New NDAA', *Lawfare*, July 26, 2018, https://www.lawfareblog.com/law-military-cyber-operations-and-new-ndaa.

[24] Julian E. Barnes, 'Cyber Command Operation Took Down Russian Troll Farm for Midterm Elections', *The New York Times*, February 26, 2019, https://www.nytimes.com/2019/02/26/us/politics/us-cyber-command-russia.html.

[25] John S. McCain National Defense Authorization Act for Fiscal Year 2019, 497.

[26] Ibid., 497.

[27] Mark Pomerleau, 'New Authorities Mean Lots of New Missions at Cyber Command', *Fifth Domain*, May 8, 2019, https://www.fifthdomain.com/dod/cybercom/2019/05/08/new-authorities-mean-lots-of-new-missions-at-cyber-command/. However, this may have been due to a lack of capabilities and reluctance by the Obama administration to conduct these types of activities.

economic impacts'.[28] Given NSPM13's classified nature, it is unclear what specific rules guide the use of OCO but documents such as JP 3-12 are clear that the DOD must conduct CO in a way that is 'consistent with US domestic law, applicable international law and relevant USG and DOD policies'.[29]

Other recent strategy documents emphasise how the UN cyber stability framework governs how OCCs are to be used. The 2018 National Cyber Strategy (NCS), which emphasises more aggressive approaches in cyberspace such as 'defend forward' and 'persistent engagement', lists that the US will encourage universal adherence to international law and globally agreed-on norms as a priority action.[30] This priority is reiterated in the 2018 DOD Cyber Strategy, in which the DOD commits to reinforcing 'voluntary, non-binding norms of responsible State behaviour in cyberspace during peacetime'.[31]

While the US is trying to encourage adherence by all countries to the UN norms for responsible state behaviour, it seems that it does not want to politically commit itself to follow the norms. For example, the US is the only Five Eyes member which has not signed the 'Paris Call for Trust and Security in Cyberspace', a 2018 French-led initiative that calls for various stakeholders to commit to working together and to adopt a set of nine non-binding principles for a secure and responsible cyberspace.[32] The US also does not explicitly commit to adhering to the UN norms which it promotes.

At the UN, the US takes the position that threats come from the behaviour of countries and how they use cyber capabilities rather than from the technology or the capabilities themselves.[33] The US has also stated that while it prefers for all states to act together in addressing threats in cyberspace, the reality is that some states are unwilling to do so. Any UN agreement, then, 'needs to reflect the reality that individual States may need to take measures to address threats in cyberspace when collective action is not feasible'. [34]

The US position stands in contrast to an unrealistic proposition advocated by countries like Russia, China, Cuba and Iran which propose that to increase international stability in cyberspace and avoid its 'militarisation', it is necessary to conclude an international legally binding treaty.[35] Such a treaty would ostensibly prohibit or constrain the state use of OCCs among UN member states.

[28] Ellen Nakashima, 'White House authorises 'offensive cyber operations' to deter foreign adversaries', *The Washington Post*, September 20, 2018, https://www.washingtonpost.com/world/national-security/trump-authorises-offensive-cyber-operations-to-deter-foreign-adversaries-bolton-says/2018/09/20/b5880578-bd0b-11e8-b7d2-0773aa1e33da_story.html.

[29] JP 3-12, xiv-xv. JP 3-12 also states that 'the laws that regulate military actions in US territory also apply to cyberspace'. The US has made several statements clarifying how it considers various issues of domestic and international law to apply to cyberspace. See for example: https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/.

[30] The White House, 'National Cyber Strategy of the United States of America', August 1, 2018, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf, 20.

[31] Department of Defense, 'Cyber Strategy', September 18, 2018, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF, 5.

[32] Louise Matsakis, 'The US Sits out an International Cybersecurity Agreement', *Wired*, November 12, 2018, https://www.wired.com/story/paris-call-cybersecurity-united-states-microsoft/.

[33] 'United States Comments on the Chair's Pre-draft of the Report of the UN Open Ended Working Group (OEWG)', April 6, 2020, https://front.un-arm.org/wp-content/uploads/2020/04/oewg-pre-draft-usg-comments-4-6-2020.pdf. The US argues that '[t]he mere existence of a possibility to use ICTs for military purposes is not inherently a threat'.

[34] Ibid.

[35] Josh Gold, 'A Cyberspace "FIFA" to Set Rules of the Game? UN States Disagree at Second Meeting', *Net Politics (Blog)*, March 2, 2020.

At the close of the 2016-2017 UN GGE which, unlike its 2013 and 2015 iterations failed to agree on a consensus report, US representative Michele Markoff explained that the US could not accept a GGE report which did not address the question of how certain bodies of international law apply to the state use of ICTs, including international humanitarian law, the law of state responsibility and international law governing states' right to self-defence.[36] Markoff elaborated the US position further, stating that:

> A report that discusses the peaceful settlement of disputes and related concepts but omits a discussion of the lawful options States have to respond to malicious cyber activity they face would not only fail to deter States from potentially destabilising activity, but also fail to send a stabilising message to the broader community of States that their responses to such malicious cyber activity are constrained by international law.[37]

Thus, the US position is that there must be lawful ways for states to respond to malicious cyber activities, both to deter such activities and also to provide stability through a clear and firm display that international law applies to activity in cyberspace. USCYBERCOM's 2018 Command Vision is even more frank about the condemnation of US military capabilities in cyberspace and asserts that the US has a right to respond forcibly to defend itself:

> We recognize that adversaries already condemn US efforts to defend our interests and allies as aggressive and we expect they will similarly seek to portray our strategy as 'militarizing' the cyberspace domain. The Command makes no apologies for defending US interests […] in a domain already militarized by our adversaries. To the maximum extent possible, we will operate in concert with allies and coalition partners. We will also explain to oversight entities and the public the nature of threats in cyberspace, the threatening conduct of our adversaries, the limitations of passive defenses and our scrupulous regard for civil liberties and privacy.[38]

This statement shows that while the US reserves the right to respond unilaterally to defend its interests, it prefers to do so collectively. It also captures the US conclusion that military involvement in cyberspace is an unavoidable reality and that the US will not shy away from this reality.

Indeed, as the statements by both Markoff and USCYBERCOM demonstrate, current US strategic thinking in cyberspace has shifted from a defensive strategy to a more active approach that is focused on imposing costs on malicious actors who violate accepted norms for responsible state behaviour. This is clarified in the 2018 NCS as preserving peace and security by 'strengthening the ability of the United States – in concert with its allies and partners – to deter and if necessary, punish' those who behave badly in cyberspace.[39] Two approaches for imposing consequences came to the fore in 2018: persistent

[36] Michele G. Markoff, 'Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE)', June 23, 2017, accessible via U.S. Department of State: https://www.state.gov/explanation-of-position-at-the-conclusion-of-the-2016-2017-un-group-of-governmental-experts-gge-on-developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-sec/.

[37] Ibid.

[38] US Cyber Command, 'Command Vision for US Cyber Command', June 14, 2018, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010, 10.

[39] The White House, 'National Cyber Strategy of the United States of America', 19.

engagement,[40] and what James Lewis calls 'collective deterrence', which involves the development of a common approach among like-minded nations to respond collectively to malicious actions that clearly transgress existing norms.[41] While the US is one of many countries which have declared that a response to a cyberattack need not necessarily come through cyberspace,[42] existing strategy and policy suggest that responses could indeed come that way; one of USCYBERCOM's primary missions is to impose costs on adversaries which are acting maliciously and with impunity in cyberspace.[43]

The US has two main objectives for what it calls 'preserving peace through strength': enhancing cyber stability through norms for responsible state behaviour and attributing and deterring unacceptable behaviour in cyberspace.[44] While it works to promote global consensus and adherence to norms, the US also intends to formalise how it works with like-minded partners to impose 'swift, costly and transparent' consequences when it or its partners are harmed by 'irresponsible' and 'malicious' cyber activities – presumably activities that violate the UN norms.[45] To do so, the NCS announced the creation and development of the CDI under which the US will work with like-minded countries to coordinate and support each other's responses to 'significant' malicious cyber incidents, including through 'the joint imposition of consequences against malign actors'.[46] Little public information elaborates on the CDI and a significant element of it may simply be based on collective attributions rather than entailing a more active response. Yet as is shown in examining the remaining four Five Eyes country cases, their respective strategies, statements and actions align with what little is currently known.

In summary, the US has been transparent with regard to its OCCs, especially in articulating military doctrine toward how they will be used and in terms of the norms, rules and international legal principles to which OCCs will adhere. The US has affirmed that countries have the right to use OCCs, though it does not call loudly for other states to reveal how they will use them. Instead, it has led by example. The US has also been clear in its preference to work collectively with allies and partners while simultaneously insisting on the right to take unilateral action if necessary. Shifts in US strategy toward a more active approach for ensuring deterrence against malicious cyber activities may indicate its desire to be able to use OCCs as a legitimate means for responding to, or defending against, violations of existing international norms and law.

However, while the US may indeed be relatively transparent toward its OCCs in terms of its disclosure of public documents and statements, this paper avoids discussion of historical examples of the use of OCCs, for example, the Stuxnet campaign against Iranian nuclear infrastructure. If, as most commentators suspect, the US did play a significant role in the Stuxnet attacks, then they could be seen as an example of the US disregarding some of the norms and rules which it promotes. Admittedly, the Stuxnet attack occurred before the UN consensus endorsements of international law and the non-

[40] For further reading on persistent engagement, see Jason Healey, 'The Implications of Persistent (and Permanent) Engagement in Cyberspace', Journal of Cybersecurity 5, no. 1 (2019), doi:10.1093/cybsec/tyz008.

[41] James A. Lewis, 'Risk, resilience and retaliation', *Routledge Handbook of International Cybersecurity*, February 18, 2020, https://www.routledgehandbooks.com/doi/10.4324/9781351038904-25, 255.

[42] National Cyber Strategy of the United States of America, 2018, 21. 'All instruments of national power are available to prevent, respond to and deter malicious cyber activity against the United States. This includes diplomatic, information, military (both kinetic and cyber), financial, intelligence, public attribution and law enforcement capabilities'.

[43] Mark Pomerleau, 'Cyber Command Nominee: Attacks Must Come with a Cost', *Fifth Domain*, March 1, 2018, https://www.fifthdomain.com/dod/cybercom/2018/03/01/cyber-command-nominee-attacks-must-come-with-a-cost/.

[44] National Cyber Strategy of the United States of America, 20-21.

[45] Ibid., 21.

[46] Ibid. While this paper examines the Five Eyes countries, the CDI is certainly not limited to just these five countries.

binding norms but more recent offensive cyber operations may be classified and given that the US has not itself explicitly committed to adhering to the UN cyber stability framework, it may be difficult to argue that the US is, in reality, transparent about its OCCs on an operational level.

3.2 United Kingdom

In 2013, the UK announced its development of cyber capabilities, which included a 'strike capability'.[47] Five years later the director of the Government Communication Headquarters (GCHQ) revealed that his agency had been developing and using 'offensive cyber techniques' for more than a decade, meaning 'action online that has direct real-world impact'.[48] GCHQ also announced that it had conducted a 'major offensive cyber campaign' against ISIS in partnership with the Ministry of Defence (MOD).[49] This campaign was qualified as a success and GCHQ indicated that such offensive cyber operations can deny, disrupt, deter or destroy various services, activities, groups, or networks.[50]

Cyber operations are described in the MOD Joint Doctrine Note (JDN) 1/18 on Cyber and Electromagnetic Activities, as 'the planning and synchronisation of activities in and through, cyberspace to enable freedom of manoeuvre and to achieve military objectives'.[51] Offensive cyber operations (OCO) refer specifically to '[a]ctivities that project power to achieve military objectives in, or through, cyberspace'.[52] OCO further include 'activities that project force to create, deny, disrupt, degrade and destroy effects in and through cyberspace' and such operations 'may transcend the virtual domain into effects in the physical and cognitive domains'.[53] Such OCOs involve 'deliberate intrusions into opponents' systems or networks, with the intention of causing damage, disruption or destruction'.[54] OCO 'can [also] be used to inflict temporary or permanent effects, thus reducing an adversary's confidence in networks or capabilities'.[55]

According to the 2016-2017 annual report of the Intelligence and Security Committee (ISC) of Parliament which oversees GCHQ, the UK's National Offensive Cyber Programme (NOCP) involved 'the full spectrum of capabilities' and ranges from tactical measures to 'the high end of counter state

[47] James Blitz, 'UK Becomes First State to Admit to Offensive Cyber Attack Capability', *Financial Times*, September 29, 2013, https://www.ft.com/content/9ac6ede6-28fd-11e3-ab62-00144feab7de.
[48] Jeremy Fleming, 'Director's speech at Cyber UK 2018'. CyberUK18, April 12, 2018, https://www.gchq.gov.uk/speech/director-cyber-uk-speech-2018.
[49] Ibid.
[50] Ibid.
[51] Ministry of Defence (UK), 'Joint Doctrine Note 1/18: Cyber and Electromagnetic Activities', February, 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/682859/doctrine_uk_cyber_and_electromagnetic_activities_jdn_1_18.pdf, 32. Cyber operations are categorised into four distinct roles: offensive cyber operations; defensive cyber operations; cyber intelligence, surveillance and reconnaissance (ISR); and cyber operational preparation of the environment (32-33).
[52] Ministry of Defence (UK), 'Cyber Primer: Second Edition', July 20, 2016, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/549291/20160720-Cyber_Primer_ed_2_secured.pdf, 54.
[53] Ibid.
[54] UK Government, 'National Cyber Security Strategy 2016-2021', 2016, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf, 51.
[55] Ministry of Defence (UK), 'Cyber Primer: Second Edition', 54.

offensive cyber capabilities which might never be used but are the sort [of] high-end deterrents'.[56] The ISC report also revealed that the UK intelligence community, including the military, interprets OCCs to cover a range of capabilities including the ability to retaliate after a cyberattack and capabilities to attack systems or infrastructure in a way that may extend into '"real-world" damage'.[57] There is no known public elaboration on what precisely these capabilities involve, though in September 2020, General Sir Patrick Sanders of UK Strategic Command said that the UK's national OCCs could degrade, disrupt, or destroy adversaries' 'critical capabilities and infrastructure' – including strategic and tactical targets.[58]

The UK has been vocal in emphasising the alignment of its OCCs with international law and has called repeatedly for other countries to do so. GCHQ has asserted that it only uses OCCs 'in line with domestic and international law, when […] necessity and proportionality have been satisfied and with all the usual oversight in place'.[59] This is reflected in the 2016-2021 National Cyber Security Strategy (NCSS), which announced that while the UK will 'more actively disrupt' the activity of its adversaries and the infrastructures on which they rely to create deterrence and prevent impunity and will simultaneously promote the application of international law in cyberspace.[60] However, GCHQ has noted that the existing practice and precedents regarding how international legal principles apply in cyberspace are underdeveloped and therefore the application of international law can 'vary considerably'.[61]

At the UN, the UK has delivered clear rebukes to countries that are ostensibly concerned about the 'militarisation of cyberspace'. The UK holds that cyber capabilities have a dual-use nature. It has thus recognised that cyber capabilities can be developed and used 'in a manner consistent with international law' and has further called on countries to be transparent about the existence of military cyber capabilities and to provide information on the legal rules and oversight mechanisms that govern them.[62] The UK asserts that transparency around cyber capabilities leads to predictability and common understanding – and thereby also stability.[63]

The UK argues that, in many cases, the use of cyber capabilities in military contexts may even be preferable to the use of kinetic weapons, and could be de-escalatory.[64] It has stated that states 'must comply' with international law and 'should be guided' by previous UN GGE reports in their development and use of military or other cyber capabilities.[65] Yet while the UK is firm on declaring that it will use its own OCCs in line with its obligations under international law, it is softer on its degree of adherence to

[56] Interview with the GCHQ cited in: Intelligence and Security Committee of Parliament (UK), 'Annual Report 2016-2017', House of Commons, December 20, 2017, https://fas.org/irp/world/uk/isc2016-17.pdf, 44. The NOCP has reportedly been replaced by the 'National Cyber Force', yet any further detail appears lacking.
[57] Ibid., 43.
[58] Helen Warrell, 'Top general lifts lid on Britain's cyber attack capability', *Financial Times*, September 25, 2020, https://www.ft.com/content/702c4589-b4e2-4409-af33-3935b74ea27c.
[59] Jeremy Fleming, 'Director's speech at Cyber UK 2018'. CyberUK18, April 12, 2018. Furthermore, the UK has outlined how it sees international law apply to cyberspace and how it views sovereignty. See, for example: https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.
[60] UK Government, 'National Cyber Security Strategy 2016-2021', 47.
[61] Intelligence and Security Committee of Parliament (UK), 'Annual Report 2016-2017', 44.
[62] 'UK response to Chair's initial 'Pre-draft' of the report of the OEWG on developments in the field of information and telecommunications in the context of international security', April 15, 2020, https://front.un-arm.org/wp-content/uploads/2020/04/20200415-oewg-predraft-uk.pdf. The UK has also publicly outlined its position on how international law applies in cyberspace, including cyber operations.
[63] 'Contribution by United Kingdom to the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the context of International Security, February 2020'. March 3, 2020, https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/03/20200303-uk-national-contribution-oewg2.pdf, 4.
[64] Ibid.
[65] Ibid.

the UN norms of responsible state behaviour championed in the UN GGE discussions, saying only that it will take this 'into account'.[66]

Like the US, the UK holds the view that cyber capabilities are not in and of themselves a threat, but rather the threat arises when states or other actors use these capabilities 'for purposes inconsistent with international peace and security'.[67] To counter cyber threats from state actors, the UK will reinforce and promote the UN cyber stability framework alongside international partners.[68] It may also use its OCCs to respond.

The NCSS makes clear that the primary purpose of the UK's OCCs is deterrence; it declares that the UK will be a 'hard target' for aggressive action in cyberspace and notes that it reserves the right to disrupt, pursue and prosecute hostile actors through offensive action in cyberspace, should it choose to do so.[69] That said, like the US, the UK also leaves open the possibility for offensive activities unrelated to deterrence; as the NCSS affirms, the UK will ensure that it has at its disposal 'appropriate offensive cyber capabilities that can be deployed at a time and place of our choosing, for both deterrence and operational purposes, following national and international law'.[70]

Aligning with the US-led CDI, the UK also emphasises the importance of working with its allies, especially the US, Five Eyes, NATO and the EU, both in growing their offensive capabilities and in jointly attributing and responding to malicious cyber activity.[71] GCHQ supports seeking international consensus on 'rules of engagement for offensive cyber',[72] and echoes the US on the importance of working through 'collective defence' and 'cooperative security' to prevent adversaries from acting with impunity.[73]

Although the UK has released fewer documents on military and other operational details related to its OCCs and how they might be used, it joins the US in avoiding an explicit commitment to adhere to the UN cyber stability framework which it supports and promotes. The UK and the US, likely due to their size and status as major cyber powers, are the only Five Eye countries which make clear their right to act unilaterally in cyberspace if necessary, potentially in violation of agreed UN norms and international law. The fact that some parties of the CDI such as the US and UK avoid making clear commitments to adhere to the UN cyber stability framework may question the extent to which the existing public positions of the US and UK toward their OCCs are credible or meaningful.

[66] Ibid. However, the UK has been a vocal and active supporter at the UN of these norms and their implementation.
[67] Ibid.
[68] UK Government, 'National Cyber Security Strategy 2016-2021', 49. The document states that to counter hostile foreign actors the UK will, inter alia, 'reinforce the application of international law in cyberspace in addition to promoting the agreement of voluntary, non-binding norms of responsible state behaviour and the development and implementation of confidence building measures'.
[69] Ibid., 9.
[70] UK National Cyber Security Strategy 2016-2021, 51.
[71] Jeremy Fleming, 'Director's speech at Cyber UK 2018'.
[72] Intelligence and Security Committee of Parliament (UK), 'Annual Report 2016-2017', 135.
[73] UK National Cyber Security Strategy 2016-2021, 49.

3.3 Australia

In 2016, Australia released an updated Cyber Security Strategy which, for the first time, acknowledged OCCs.[74] Speaking about the Strategy, Australian prime minister Malcolm Turnbull noted that defensive cybersecurity measures 'may not always be adequate to respond to serious cyber incidents against Australian networks', and acknowledged for the first time the offensive cyber capability of the Australian Signals Directorate (ASD).[75] Later that year Turnbull told parliament that these OCCs have important military applications and are used in support of the Australian Defence Forces (ADF) and that they 'are making a real difference' in operations against Daesh.[76] Then, in June 2017, Turnbull announced that his government had directed offensive cyber capabilities to be used 'to disrupt, degrade, deny and deter organised offshore cyber criminals' in response to the growing impact of cybercrime.[77] Most recently, Australia's 2020 National Cybersecurity Strategy noted that the ASD had, in summer 2020, used OCCs to 'disrupt foreign cyber criminals' targeting Australia with COVID-19 themed attack campaigns.[78]

The Australian government defines cyberspace operations as '[o]ffensive and defensive activities designed to achieve effects in or through cyberspace'.[79] Offensive cyber operations (OCO) are defined as '[a]ctivities in cyberspace that manipulate, deny, disrupt, degrade or destroy targeted computers, information systems, or networks'.[80] This includes 'computer network attack operations to destroy an adversary's communication device' and, also, more subtle and 'sophisticated' operations that consist of highly-targeted, well-timed and proportionate actions.[81]

The ADF has been quite clear on how it approaches cyber operations and how it collaborates with the ASD on them.[82] While it has not released a cyber doctrine, it has developed a Conceptual Framework for Cyber Operations that explains offensive cyber, active cyber defence, passive cyber defence and cyber self-defence.[83] Offensive cyber means that 'the ADF will attack the systems and capabilities of actors viewed as hostile to the ADF or its operations, to ensure missions are achieved and ADF personnel and systems are safe'.[84]

[74] Australian Government, 'Australia's Cyber Security Strategy', 2016, https://cybersecuritystrategy.homeaffairs.gov.au/AssetLibrary/dist/assets/images/PMC-Cyber-Strategy.pdf, 28.

[75] Malcolm Turnbull, 'Speech at Launch of Australia's Cyber Security Strategy, Sydney', April 21, 2020, https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22media/pressrel/4513168%22.

[76] Malcolm Turnbull, 'Address to Parliament – National Security Update on Counter Terrorism', November 23, 2016, https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22media/pressrel/4951827%22.

[77] Malcolm Turnbull, 'Offensive Cyber Capability To Fight Cyber Criminals', June 30, 2017, https://www.malcolmturnbull.com.au/media/offensive-cyber-capability-to-fight-cyber-criminals. Australia thus became the first country to do so.

[78] Australian Government, 'Australia's Cyber Security Strategy 2020', August 6, 2020, https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf, 14.

[79] Australian Cyber Security Centre, 'Glossary', https://www.cyber.gov.au/acsc/view-all-content/glossary/c.

[80] Ibid.: https://www.cyber.gov.au/acsc/view-all-content/glossary/o.

[81] Mike Burgess, 'Director-General ASD speech to the Lowy Institute', Lowy Institute, Sydney, March 27, 2019, https://www.asd.gov.au/publications/speech-lowy-institute-speech.

[82] The ADF's military cyber operations fall within its Information Warfare Division (IWD). However, Australia's offensive cyber capabilities are held by the ASD and are conducted by ASD personnel in collaboration with the ADF and under the direction of the Chief of Joint Operations.

[83] Marcus Thompson & Edward Morgan, 'Information Warfare: An Emergent Australian Defence Force Capability', October 4, 2018, https://www.csis.org/analysis/information-warfare-emergent-australian-defence-force-capability, 23.

[84] Ibid.

Australia has also been clear on the rules surrounding the use of OCCs; they must be targeted, proportionate, 'subject to stringent legal oversight' and be consistent with support for the rules-based international order and both domestic and international legal obligations.[85,86]

Australia's 2017 International Cyber Engagement Strategy presents various policies regarding the conduct and authorisation of the use of OCCs in support of military operations, including clarity around authorisations, organisation and chain-of-command.[87] Conduct of OCO in support of military operations is, like all other military capabilities, governed by ADF Rules of Engagement (ROE).[88] The ROE are themselves 'informed by and consistent with domestic and international law, including the Law of Armed Conflict (International Humanitarian Law)'.[89] OCOs are also bound by the ASD's existing legislative and oversight framework, which includes domestic laws and oversight mechanisms.[90]

Internationally, Australia is a proponent of the right of states to develop OCCs but it calls attention to the different degrees of transparency of states toward them.[91] Australia agrees with the US and UK on acknowledging the 'undeniable' reality that an ever-growing number of states are developing such capabilities.[92] Like the UK, Australia holds that transparency about the fact that states possess and develop OCCs leads to accountability and denies that Australia's acknowledgement of the existence and use of OCCs contradicts its commitment to a peaceful and stable cyberspace. Instead, Australia maintains that its clarity toward how it will use OCCs sends a clear message 'that states' activities in cyberspace have limitations and are subject to obligations, just as in the physical domain'.[93]

Australia thus calls on all countries to be transparent about the development and use of their OCCs and to commit clearly to aligning these activities to domestic and international law – and to the UN norms of responsible state behaviour, with which Australia aligns its own OCCs.[94] As Australia's ambassador for cyber affairs Tobias Feakin has written, '[w]hen increased spending and developments in cyber capability are placed within a framework that is at once exceedingly clear, measured and explanatory, it lowers suspicion and the potential confrontation in cyberspace'.[95]

[85] Malcolm Turnbull, 'Speech at Launch of Australia's Cyber Security Strategy, Sydney', April 21, 2020.

[86] Mike Burgess, 'Director-General ASD speech to the Lowy Institute', March 27, 2019.

[87] Australian Government, 'Australia's International Cyber Engagement Strategy', October 2017, https://www.dfat.gov.au/sites/default/files/DFAT%20AICES_AccPDF.pdf, 55.

[88] Ibid.

[89] Ibid. Australia has outlined its positions on how international law applies in cyberspace, e.g. here: https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/2019_international_law_supplement.html.

[90] Ibid. Domestic laws include the Commonwealth Criminal Code Act 1995 and the Intelligence Services Act 2001. The Intelligence Services Act was amended in 2018, including changes to the ASD's mandate. Under the new amendments the ASD gained, inter alia, the ability to 'disrupt', which refers to the ability to use offensive cyber capabilities in support of military operations and counter-terrorism efforts and to counter espionage and cybercrime.

[91]'Australia's comments on the Initial 'Pre-draft' of the report of the UN Open Ended Working Group in the field of information and telecommunications in the context of international security (OEWG)'. April 16, 2020, https://front.un-arm.org/wp-content/uploads/2020/04/final-australia-comments-on-oewg-pre-draft-report-16-april.pdf.

[92] Tobias Feakin & Johanna Weaver, 'Cyber Diplomacy', *Routledge Handbook of International Cybersecurity*, February 18, 2020, https://www.routledgehandbooks.com/doi/10.4324/9781351038904-29, 280.

[93] Ibid., 281.

[94] Stilgherrian, 'Blaming Russia for NotPetya Was Coordinated Diplomatic Action', *ZDNet*, April 12, 2018, https://www.zdnet.com/article/blaming-russia-for-notpetya-was-coordinated-diplomatic-action/.

[95] Tobias Feakin, 'Matching rhetoric with action: cyber and the 2016 Defence White Paper', ASPI, February 25, 2016, https://www.aspistrategist.org.au/matching-rhetoric-with-action-cyber-and-the-2016-defence-white-paper/.

Such positions speak to Australia's broader strategy when it comes to OCCs, which seeks to promote the 'establishment or preservation of a legitimate rules-based order for capabilities in the information environment, especially as these are deployed or utilized by militaries'.[96] This means that Australia will push for the recognition that 'cyber capabilities are subject to the same limitations and obligations as any other military capability' through diplomatic outreach and 'defence engagement'.[97] Australia and its Five Eyes allies develop their doctrines 'while closely coordinating their strategic intent with one another',[98] and most of Australia's capabilities are closely aligned with those of its Five Eyes partners.[99]

While protective cybersecurity measures are 'at the forefront' of Australia's response to cyber threats, Australia sees its OCCs as another way to respond to malicious cyber activity in addition to law enforcement, diplomatic and economic measures.[100] According to Turnbull, acknowledgement of OCCs provides deterrence and clarity around their use raises Australia's credibility as it promotes UN norms of responsible state behaviour internationally.[101]

Aligning with both the US-led CDI and support for the UN cyber stability framework, Australia's international cyber strategy stresses the importance of an 'architecture for cooperation' among states, including 'mechanisms to respond to unacceptable behaviour in cyberspace in a timely and agile manner, within the existing framework of international law'.[102] Like the US and UK, Australia commits itself to working with its partners to strengthen 'global responses' and to counter, deter and discourage unacceptable malicious behaviour – especially by 'states and their proxies'.[103]

3.4 Canada

Though OCCs have been quietly discussed for many years,[104] Canada only publicly committed to moving in this direction in its 2017 National Defence Policy. The policy announced that Canada would 'assume a more assertive posture in the cyber domain', including by 'conducting active cyber operations against potential adversaries in the context of government-authorized military missions'. The National Defence Policy further elaborates that the Canadian Armed Forces (CAF) will invest in joint capabilities including 'the development of military-specific information operations and offensive cyber operations

[96] Marcus Thompson & Edward Morgan, 'Information Warfare: An Emergent Australian Defence Force Capability', October 4, 2018, 21.
[97] Australian Government, 'Australia's International Cyber Engagement Strategy', October 2017, 53.
[98] Thompson & Morgan, 'Information Warfare: An Emergent Australian Defence Force Capability', 20.
[99] Marcus Thompson, 'Cyber War: The ADF's New Battleground'. *No Limitations (podcast)*, Episode 19, June 12, 2019, https://www.youtube.com/watch?v=zojQiWM0pic.
[100] Malcolm Turnbull, 'Speech at Launch of Australia's Cyber Security Strategy, Sydney', April 21, 2020.
[101] Ibid.
[102] Australian Government, 'Australia's International Cyber Engagement Strategy', 54.
[103] Ibid., 55.
[104] For some of this discussion, see for example: Melanie Bernier & Joanne Treurniet, 'Understanding Cyber Operations in a Canadian Strategic Context: More than C4ISR, More than CNO', in C. Czosseck and K. Podins (ed.), *Conference on Cyber Conflict Proceedings 2010*, CCD COE Publications, 2010, https://ccdcoe.org/uploads/2018/10/Benier-Understanding-Cyber-Operations-in-a-Canadian-Strategic-Context-More-than-C4ISR-More-than-CNO.pdf.

capabilities able to target, exploit, influence and attack in support of military operations'.[105] It is unclear to what extent the CAF currently has OCCs; they may largely be in development.[106]

The Department of National Defence (DND) explains that active cyber operations are used to protect personnel and advance military objectives and will offer the government a strategic tool to 'disrupt, degrade and deny foreign and adversarial threats'.[107] Both the DND and the CAF work closely with Canada's SIGINT agency, the Communications Security Establishment (CSE), to develop these active cyber capabilities and the CSE 'assists them in their active cyber operations'.[108] For reasons unknown, the CAF refers to such operations as 'active', while nevertheless conceding that the capabilities themselves may be 'offensive'. There is no further known public detail around Canada's OCCs; while the CAF published a Joint Doctrine Note (JDN) on cyber operations in 2017, it remains classified at the time of writing.[109]

Recent legislative updates have authorised the CSE to behave more assertively in cyberspace. The July 2019 Communications Security Establishment Act (CSE Act) – which was included as part of omnibus legislation that substantively updated Canada's national security and intelligence capabilities and accountability mechanisms – authorises the CSE to conduct both defensive and 'active' cyber operations abroad.[110] 'Active cyber operations' enable the CSE to carry out activities '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'.[111] The Canadian government has not, at the time of writing, elaborated on what this means or precisely entails.

Bill C-59, the aforementioned omnibus legislation, significantly clarified the rules around how the CSE can conduct its 'active' cyber operations.[112] It also established an updated oversight body and review agency which are, respectively, tasked with authorising certain classes of activities and ensuring that the CSE is acting in compliance with the law and examining the reasonableness and necessity of its powers, including active cyber operations.[113] This is in addition to the Bill providing authorisation frameworks for both defensive and active cyber operations.

[105] National Defence (Canada), 'Strong, Secure, Engaged: Canada's Defence Policy', 2017, https://www.canada.ca/content/dam/dnd-mdn/documents/reports/2018/strong-secure-engaged/canada-defence-policy-report.pdf, 41.

[106] It is clear that developing such capabilities is a priority; the joint DND and CAF 2020-2021 Departmental Plan announces plans to 'Advance research and development in the future of cyber warfare to improve and strengthen both defensive and offensive capabilities' (7).

[107] Government of Canada, 'Joint Capabilities: Canadian Armed Forces Cyber Activities', April 7, 2020, https://www.canada.ca/en/department-national-defence/corporate/reports-publications/proactive-disclosure/cow-estimates-a-2019-20/joint-capabilities.html.

[108] Ibid.

[109] The author filed an Access to Information (ATI) request for this document in February 2020, after being denied access by the DND. As of October 2020, the ATI request has not been filled.

[110] Christopher Parsons and Josh Gold, 'A Deep Dive into Canada's Overhaul of Its Foreign Intelligence and Cybersecurity Laws', *Just Security*, June 2, 2020: https://www.justsecurity.org/70519/a-deep-dive-into-canadas-overhaul-of-its-foreign-intelligence-and-cybersecurity-laws/.

[111] Parliament of Canada, 'Bill C-59, An Act Respecting National Security Matters', 1st session, 42 parliament, June 21, 2019, https://www.parl.ca/legisinfo/BillDetails.aspx?billId=9057418&Language=E, *CSE Act*, s. 19 (p.68).

[112] Ibid.

[113] Christopher Parsons and Josh Gold, 'A Deep Dive into Canada's Overhaul of Its Foreign Intelligence and Cybersecurity Laws'.

Concerning the CAF and the DND, the 2017 Defence Policy affirms that cyber operations are subject to 'all applicable domestic law, international law and proven checks and balances such as rules of engagement, targeting and collateral damage assessments'.[114] The Defence Policy also speaks of its commitment to 'full oversight and accountability' and cites 'efforts to advance human rights and establish new international norms' as examples of how Canada could advocate for the 'highest standards for the use of cyber'.[115] Notably, however, one of the Defence Policy's introductory messages characterises cyber threats as existing in 'uncharted legal territory', though it commits to fully reflecting 'Canadian values' when it comes to challenges to the international humanitarian law governing armed conflict.[116]

Canada, like the US, UK and Australia, asserts at the UN the view that OCCs are not necessarily dangerous in and of themselves and that '[t]here are entirely appropriate uses for these capabilities'.[117] Canada supports openness and transparency and has expressed support for the UN cyber stability framework when it has publicly stated that Canada's cyber capabilities would be used in line with 'international legal obligations and with agreed norms of State behaviour'.[118] Canada encourages all countries with OCCs to reveal their existence and to 'pledge' to use them 'in accordance with international law and existing agreed norms of State behaviour'.[119]

Canada has not developed an international strategy for cyberspace. Its 2018 National Cyber Security Strategy says only that it will, alongside its allies, 'work to shape the international cyber security environment in Canada's favour'.[120] However, a secret October 2019 briefing note to the Prime Minister, released to a Canadian journalist, clearly marks Canada's position: while rules and norms in cyberspace are critical, they 'must be supplemented with measures to impose costs on hostile actors'.[121] The briefing note further mentions Canadian collaboration with 'a group of likeminded countries' and states that Canada seeks to strengthen deterrence and reinforce the international order through imposing costs on malicious activity that violates international law or the non-binding norms for responsible state behaviour. Despite significant redactions, the aforementioned points from the briefing note indicate close Canadian alignment with the CDI.

Based purely on public statements and documents, Canada appears to be behind the US, UK and Australia in terms of fully developing and operationalising its OCCs. Whether Canada is, in reality, less developed in this area or simply prefers to remain in the shadows is difficult to determine. Canada's less mature operationalisation of its OCCs may explain why it is less transparent about its intentions and capabilities, or it may simply reflect a reluctance to share information outside of the executive. Regardless, Canada's positions appear to align with those of the US, UK and Australia in terms of support for the UN cyber stability framework and the US-led CDI.

[114] National Defence (Canada), 'Strong, Secure, Engaged: Canada's Defence Policy', 15. Unlike the US, UK and Australia, Canada has not yet clarified how it considers international law to apply in cyberspace.
[115] Ibid., 55.
[116] Ibid., 8.
[117] 'Canada's response to questions in Chair's paper: February 2020 OEWG meeting', February 26, 2020, https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/03/canada-responses-to-oewg-chair-questions-Feb-26.pdf, 5.
[118] Ibid.
[119] Ibid.
[120] Public Safety Canada, 'National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age', June 12, 2018, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx - s11, 3.
[121] Contact the author for this document, or find it here: https://drive.google.com/file/d/1Q1SQEIFKwHj5JRERO-L5-IqcmM0Er3mi/view.

3.5 New Zealand

Unlike its four larger Five Eyes counterparts, New Zealand has not publicly acknowledged the development or possession of OCCs, nor are there known references to such capabilities. New Zealand's 2019 Cyber Security Strategy states that New Zealand will '[p]revent, detect, deter and respond to' malicious cyber activity, though in elaborating on how it might respond, the Strategy refers only to defensive mechanisms such as Computer Emergency Response Teams (CERTs).[122]

New Zealand's 2018 Strategic Defence Policy Statement (SDPS) does make some reference to cyber capabilities, including the recognition that the increased use of cyber capabilities 'could enhance Defence's operational effectiveness and efficiency'.[123] Given this, the SDPS identifies the development of '[e]nhanced Defence cyber capabilities to provide military commanders with a broader set of tools to achieve military objectives' as one of three capability areas to focus on in the future.[124] The SDPS also notes that 'governments' development of offensive cyber capabilities is becoming increasingly normalised' and refers directly to the publicly-acknowledged offensive capabilities of the other Five Eyes countries.[125]

The SDPS also mentions the importance of expanding New Zealand's repertoire of cyber operations, stating that in addition to focusing on protection, 'operational effects in cyberspace could provide Defence Force commanders with new tools and be a new form of valued coalition contribution'.[126] Later on, it states that in the future, the New Zealand Defence Force (NZDF) 'needs to be able to conduct a broader range of cyber operations' to maintain relevant combat capabilities – such as interoperability with close partners.[127] However, it is unclear whether or not this refers to offensive capabilities; the same paragraph then refers to the aforementioned broader capabilities as 'Defence cyber capabilities'.

Neither the Government Communications Security Bureau (GCSB), New Zealand's foreign intelligence and cybersecurity agency, nor the 2017 Intelligence and Security Act, which governs the GCSB, make any reference to an ability to conduct operations beyond protective and defensive ones. The Intelligence and Security Act stresses that the GCSB must act following New Zealand law and 'all human rights obligations recognised by New Zealand law'.[128]

Internationally, New Zealand has been more muted than its Five Eyes counterparts on the militarisation of cyberspace although in May 2020 it did subtly indicate support for the idea that militarisation in cyberspace is not a risk in and of itself, but rather only when such capabilities are used improperly.[129] New Zealand has also been quiet in terms of collective responses; its 2019 cyber security strategy

[122] New Zealand Government, 'New Zealand's cyber security strategy 2019', July 2019, https://dpmc.govt.nz/sites/default/files/2019-07/Cyber%20Security%20Strategy.pdf, 13.

[123] New Zealand Government, 'Strategic Defence Policy Statement 2018', July 2018, http://www.nzdf.mil.nz/downloads/pdf/public-docs/2018/strategic-defence-policy-statement-2018.pdf, 7.

[124] Ibid., 8.

[125] Ibid., 19.

[126] Ibid., 26.

[127] Ibid., 39. This is echoed in the 2019 NZDF strategic plan 2019-2025, which repeats that 'The NZDF will need to be able to conduct a range of cyber operations to maintain relevant and interoperable combat capabilities'. (p.11).

[128] Parliamentary Counsel Office (New Zealand), 'Intelligence and Security Act 2017', October 24, 2019, http://www.legislation.govt.nz/act/public/2017/0010/latest/whole.html#DLM6920923, section 17.

[129] 'New Zealand Comments', April 2020, https://front.un-arm.org/wp-content/uploads/2020/04/oewg-pre-draft-new-zealand-comments.pdf. See notes within document: 'Some states expressed this view. Others noted that militarisation itself is not a risk - risk arose when these capabilities were used improperly. The same states noted the importance of the application of international law and norms in this context'.

mentions only that New Zealand will respond to unacceptable behaviour in cyberspace and 'will cooperate with others to prevent and deter malicious activity that threatens peace and security'.[130] It has stated at the UN that cyber stability is threatened when states do not abide by the agreed-on norms[131] and has indicated its alignment with the other Five Eyes (and their allies more widely) in joining collective attributions and statements.[132]

Despite a lack of clarity over whether New Zealand has, or even is developing OCCs, it is clear from the documents that New Zealand sees such capabilities as a valuable coalition contribution and a way to better interoperate with its Five Eyes partners. Combined with New Zealand's desire to conduct a wider range of cyber operations to better interoperate with allies, support for the UN cyber stability framework and collective attributions of cyber activity, New Zealand appears to align with the CDI even if it might not contribute to the collective efforts of the CDI with OCCs of its own.

[130] New Zealand Government, 'New Zealand's cyber security strategy 2019', July 2019, 13.

[131] 'Position Paper on New Zealand's Participation in the February 2020 Session of the 2019-2020 Open Ended Working Group'. February 2020, https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/02/nz-position-paper-on-oewg.pdf, 2.

[132] For example, New Zealand has joined many countries on common attributions of cyber-attacks, e.g. attributing NotPetya to Russia and was one of the signatories of the September 2019 US-led Joint Statement on Advancing Responsible State Behaviour in Cyberspace. For a discussion of New Zealand and cyber threat attribution, see: William Hoverd, 'Cyber Threat Attribution, Trust and Confidence and the Contestability of National Security Policy', in Steff, R., Burton, J. and Soare, S. (eds.) *Emerging Technologies and International Security: Machines, the State and War*, 2020, https://doi.org/10.4324/9780367808846.

4. Discussion

Thus far, this paper has examined how each of the Five Eyes countries' public documents and statements address the development and use of their respective OCCs. This examination has shown how the stated use of OCCs by these countries aligns with their positions in UN cyberspace governance discussions, namely, support for the UN cyber stability framework of agreed non-binding norms, international law and CBMs. In addition, the assessment of each country's position indicates a common endorsement of the US-led CDI, which aims to further enforce and strengthen the UN cyber stability framework through the collective imposition of real-world costs to states which violate the norms and principles of that framework.

This section of the paper returns to the notion of transparency, as mentioned by many of the country cases in their public statements related to OCCs. It discusses the implications of the five countries' common approach, raising questions about the existing narrative around transparency and noting potential challenges.

The five countries adhere to a common understanding that OCCs are not necessarily problematic, so long as there is transparency around their development and use – and so long as OCCs are used in a manner consistent with the obligations of international law, including international humanitarian law. Presumably, this is modelled by the five countries themselves, which have publicly committed, to varying degrees, to aligning their own OCCs with international law, the UN norms of responsible state behaviour and other transparency and accountability mechanisms such as domestic oversight and review processes as part of the rule of law. Such transparency is intended to clarify *how* the capabilities are used, which is the main focus of the Five Eyes countries in international deliberations and what they call for therein. Transparency in releasing official information about OCCs is thus used by the countries to publicly signal commitment for agreed-on UN norms and rules, which they support and want to promote globally to foster greater predictability, peace and stability.

The Five Eyes countries and many of their allies have also concluded that such norms and rules must be backed up by the imposition of costs and consequences for those who violate them. These consequences can take various forms – some of which may be in the form of offensive cyber operations – to either respond to or to proactively disrupt significant malicious activity. They recognise that imposing consequences is best done collectively in collaboration with as many countries as possible, perhaps because having a greater number of countries on board can be seen as more credible and legitimate. At the same time, it appears that the Five Eyes countries recognise that it is difficult to obtain such coordination on a global scale and thus regional or like-minded coalitions are more viable.

The desire for the collective imposition of costs in response to violations of accepted UN norms and international law leads to a question: how can like-minded democracies build common understandings about the role of OCCs in imposing costs through, for example, the CDI? Within this question is the underlying concern of how to build such a CDI in a way that is credible and that is not contradictory or hypocritical. To do so, allies ought to synchronise how they conduct offensive cyber operations and use OCCs. The CDI or any other broad, coalition-based initiative aimed at bolstering deterrence through the imposition of costs might be undermined if certain partner countries are themselves using OCCs in ways that they would otherwise seek to deter against and impose consequences in response to.

Ensuring that the CDI is credible requires some degree of transparency; for example, clarity by different CDI members toward how they will use their OCCs. Transparency commits countries to use OCCs in certain ways such as in line with UN norms, international law and national law and exhibits this to allies and adversaries alike. This transparency allows allies to credibly call on other countries to behave in kind, while simultaneously better justifying collective response against countries which transgress the rules and norms to which the allied countries have committed themselves.

A major challenge for democracies like the Five Eyes countries is to come to an agreement on common rules and principles for the operational use of OCCs and to communicate them clearly. This is critical for avoiding hypocrisy and for building credibility through practising-what-you-preach. For example, the US and the UK might gain greater credibility in the UN cybersecurity governance deliberations, if they could show that their use of OCCs in operations against the Internet Research Agency, or against ISIS, was aligned with the accepted UN norms and international law. This may pose a particular challenge to major cyber powers like the US and UK, who do not explicitly commit to following the UN cyber stability framework in full, even though they seek to reinforce and promote this framework. Furthermore, the exceptionality of the US and UK could result in the Five Eyes partners and other CDI members across the world being seen as unreliable and hypocritical by non-CDI aligned countries.

That said, the notion that a more peaceful and stable state use of OCCs can be established if the US and UK simply commit to behaving according to the UN cyber stability framework may be overly optimistic. The calls at the UN by the five countries for states to be more transparent about their use of OCCs are vague; for example, they do not specify exactly what states should be transparent about and to what extent. The current assumption posited by the Five Eyes countries (with the possible exception of New Zealand) appears to be that what countries say is what they will do – and that this type of transparency is sufficient to constrain states in their behaviour. Yet high-level assertions about how states will use their OCCs may not necessarily reflect the reality of operational policies and how these states might really use OCCs. The more important form of transparency may be toward certain classes of offensive cyber operations themselves – for example, making clear what specific actions were conducted. Some clarity or justification may lead to a form of accountability and could enable the Five Eyes and other CDI countries to more effectively uphold and reinforce the norms of behaviour which they seek to promote, including through the imposition of consequences.

Ultimately, if countries are going to use OCCs themselves *and* take part in a CDI which punishes transgressions of accepted norms, official statements about how they will use their own OCCs may not be enough. Further research is needed to explore these and other questions related to the links between transparency, credibility and accountability in the context of OCCs and offensive cyber operations, especially as more information about the CDI emerges.

5. Conclusion

> A strategic approach to developing norms in cyberspace, based primarily on diplomacy, fails to consider the unique characteristics of cyberspace.
>
> — Michael P. Fischerkeller and Richard J. Harknett[133]

> A clearer understanding of the military use of cyberattack helps make clear that creating cyber capabilities or organising to use them effectively isn't inherently contrary to international law; nor does it create new risks to peace.
>
> — James A. Lewis[134]

These two quotations provide a generalised summary of this paper's findings of what the Five Eyes countries are saying concerning OCCs and their use. An examination of the Five Eyes' public documents and statements has shown that these close partners are leaning toward a collective response approach, the US-led CDI, whereby state cyber activity which transgresses agreed-on UN norms and international law can justify some form of a response, including through the use of OCCs.

The US and its Five Eyes partners support legitimising the development of OCCs and justifying their use within the existing international norms and rules governing the use of force and coercion, such as the UN Charter. The positions of the US, UK, Australia and Canada indicate an explicit interest in the ability to respond strongly to violations of the UN cyber stability framework, to uphold the framework and build meaningful accountability into it.

The possible exception to the general trends identified in this paper is New Zealand, which does not acknowledge the development of OCCs and may not even possess them, and is thus less vocal on these issues. But even its few statements and policies align with its four close partners. New Zealand and perhaps Canada, appear to be less developed (if developed at all) in terms of OCCs compared to the US, UK and Australia. This raises questions as to why and, particularly in the case of New Zealand, questions around the extent to which smaller alliance partners need to develop their own OCCs when their larger and better-resourced partners already have them.

As part of ensuring that OCCs and their use align with the UN cyber stability framework, the Five Eyes countries and many of their allies argue that states must be transparent toward their efforts to develop OCCs and how they will use them. In this context, transparency can be considered a confidence-building measure which provides clarity, stability and accountability. That said, what the calls for transparency actually mean, beyond UN speaking points, is unclear. Following the narrative of transparency proposed by the Five Eyes countries, this paper concluded in suggesting that to make their own collective response approach credible, they and their allies must be transparent about how their own OCCs will be used. Yet a closer examination of the transparency concept raised questions related to what transparency means and ought to mean and about how transparency is related to credibility and accountability in the context of OCCs.

Further work might more extensively explore the details of what the Five Eyes countries are transparent about and what exactly transparency means for them, as compared to others. Transparency might be

[133] Michael P. Fischerkeller, & Richard J. Harknett, 'Deterrence Is Not a Credible Strategy for Cyberspace', *Foreign Policy Research Institute*, Summer 2017, 383.

[134] James A. Lewis, 'Cyberspace and armed forces: the rationale for offensive cyber capabilities', ASPI, May 31, 2016, https://www.aspi.org.au/report/cyberspace-and-armed-forces-rationale-offensive-cyber-capabilities, 2.

used as a tool for signalling; selected information can be released, while simultaneously domestic conditions such as freedom of information processes or potential leaks might affect what information is released and when. It is also unclear how transparency can be measured; what classes or types of information countries should be transparent about and how much transparency is ‘enough’.

Additionally, work building on this paper might more critically examine the narrative of the Five Eyes countries and other countries who publicly acknowledge their OCCs, to evaluate what kind of a narrative they have crafted around doing so and the extent to which this is credible or contradictory in, for example, the context of democratic values.

Finally, to look more broadly, a like-minded approach for the collective imposition of consequences carries with it an inherent challenge related to the feasibility of seeking global ends through coalition-based means. While this paper posits that the incipient coalition-based CDI is based upon the UN cyber stability framework of norms for state behaviour, as well as international law, it is unclear how an approach reliant on opposing camps of like-minded nations can effectively uphold the purportedly global cyber stability framework.

References

Australia. 'Australia's comments on the Initial 'Pre-draft' of the report of the UN Open Ended Working Group in the field of information and telecommunications in the context of international security (OEWG)'. April 16, 2020, Accessed June 30, 2020. https://front.un-arm.org/wp-content/uploads/2020/04/final-australia-comments-on-oewg-pre-draft-report-16-april.pdf.

Australian Cyber Security Centre. 'Glossary'. Accessed June 30, 2020. https://www.cyber.gov.au/acsc/view-all-content/glossary/c.

Australian Government. 'Australia's Cyber Security Strategy'. 2016, Accessed June 30, 2020. https://cybersecuritystrategy.homeaffairs.gov.au/AssetLibrary/dist/assets/images/PMC-Cyber-Strategy.pdf.

Australian Government. 'Australia's Cyber Security Strategy 2020'. August 6, 2020, Accessed September 20, 2020. https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf.

Australian Government. 'Australia's International Cyber Engagement Strategy'. October 2017, Accessed June 30, 2020. https://www.dfat.gov.au/sites/default/files/DFAT%20AICES_AccPDF.pdf.

Blitz, James. 'UK Becomes First State to Admit to Offensive Cyber Attack Capability'. *Financial Times*, September 29, 2013. Accessed June 30, 2020. https://www.ft.com/content/9ac6ede6-28fd-11e3-ab62-00144feab7de.

Burgess, Mike. 'Director-General ASD speech to the Lowy Institute'. Lowy Institute, Sydney, Australia. March 27, 2019, Accessed June 30, 2020. https://www.asd.gov.au/publications/speech-lowy-institute-speech.

Canada. 'Canada's response to questions in Chair's paper: February 2020 OEWG meeting'. February 26, 2020, Accessed June 30, 2020. https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/03/canada-responses-to-oewg-chair-questions-Feb-26.pdf.

Chesney, Robert. 'The Law of Military Cyber Operations and the New NDAA'. *Lawfare*, July 26, 2018. Accessed June 30, 2020. https://www.lawfareblog.com/law-military-cyber-operations-and-new-ndaa.

Clapper, James R., Marcel Lettre, & Michael S. Rogers. 'Foreign Cyber Threats to the United States'. Joint Statement for the Record to the Senate Armed Services Committee. January 5, 2017, Accessed June 30, 2020. https://www.armed-services.senate.gov/imo/media/doc/Clapper-Lettre-Rogers_01-05-16.pdf?fbclid=IwAR3zLlXbhy-2ggxkXk4FEmJD4JkEfvWWK_-RDf3ONtesa80k9ypTEeTV90g.

Cox, James. 'Canada and the Five Eyes Intelligence Community'. *OpenCanada*, December 18, 2012. Accessed September 20, 2020. https://www.opencanada.org/features/canada-and-the-five-eyes-intelligence-community/.

'Cyberspace Operations'. Joint Publication 3-12, Department of Defense (United States). 8 June, 2018, Accessed June 30, 2020. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.

Department of Defense. 'Cyber Strategy'. September 18, 2018, Accessed June 30, 2020. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

Feakin, Tobias, & Johanna Weaver. 'Cyber Diplomacy'. In: Eneken Tikk & Mika Kerttunen (ed.) *Routledge Handbook of International Cybersecurity*, Routledge. February 18, 2020, Accessed June 30, 2020. https://www.routledgehandbooks.com/doi/10.4324/9781351038904-29.

Feakin, Tobias. 'Matching rhetoric with action: cyber and the 2016 Defence White Paper'. Australian Strategic Policy Institute. February 25, 2016, Accessed June 30, 2020.

https://www.aspistrategist.org.au/matching-rhetoric-with-action-cyber-and-the-2016-defence-white-paper/.

Fischerkeller, Michael P., & Richard J. Harknett. 'Deterrence Is Not a Credible Strategy for Cyberspace'. *Foreign Policy Research Institute*, Summer 2017, 381-93. Accessed July 1, 2020. doi:10.1016/j.orbis.2017.05.003.

Fleming, Jeremy. 'Director's speech at Cyber UK 2018'. CyberUK18, Manchester. April 12, 2018, Accessed June 30, 2020. https://www.gchq.gov.uk/speech/director-cyber-uk-speech-2018.

Gold, Josh. 'A Cyberspace 'FIFA' to Set Rules of the Game? UN States Disagree at Second Meeting'. *Net Politics (Blog)*, U.S. Council on Foreign Relations, March 2, 2020. Accessed June 30, 2020. https://www.cfr.org/blog/cyberspace-fifa-set-rules-game-un-states-disagree-second-meeting.

Government of Canada. 'Joint Capabilities: Canadian Armed Forces Cyber Activities'. National Defence. April 7, 2020, Accessed June 30, 2020. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/proactive-disclosure/cow-estimates-a-2019-20/joint-capabilities.html.

Intelligence and Security Committee of Parliament (UK). 'Annual Report 2016-2017'. House of Commons. December 20, 2017, Accessed June 30, 2020. https://fas.org/irp/world/uk/isc2016-17.pdf.

Joye, Christopher. 'Interview transcript: former head of the NSA and commander of the US cyber command, General Keith Alexander'. The Australian Financial Review. May 9, 2014, Accessed June 30, 2020. https://www.afr.com/technology/interview-transcript-former-head-of-the-nsa-and-commander-of-the-us-cyber-command-general-keith-alexander-20140508-itzhw.

Lewis, James A. 'A Necessary Contest: An Overview of U.S. Cyber Capabilities'. *Asia Policy* vol. 15 no. 2. April 29, 2020, Accessed June 30, 2020. https://www.nbr.org/publication/the-future-of-cybersecurity-across-the-asia-pacific/.

Lewis, James A. 'Cyberspace and armed forces: the rationale for offensive cyber capabilities. Australian Strategic Policy Institute. May 31, 2016, Accessed June 30, 2020. https://www.aspi.org.au/report/cyberspace-and-armed-forces-rationale-offensive-cyber-capabilities.

Lewis, James A. 'Risk, resilience and retaliation'. In: Eneken Tikk & Mika Kerttunen (ed.) *Routledge Handbook of International Cybersecurity*, Routledge. February 18, 2020, Accessed June 30, 2020. https://www.routledgehandbooks.com/doi/10.4324/9781351038904-25.

Markoff, Michele G. 'Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security'. Remarks made on June 23, 2017, Accessed September 20, 2020 via U.S. Department of State. https://www.state.gov/explanation-of-position-at-the-conclusion-of-the-2016-2017-un-group-of-governmental-experts-gge-on-developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-sec/.

Martelle, Michael (ed.). 'USCYBERCOM Documents Timeline'. *National Security Archive*, George Washington University. May 11, 2020, Accessed September 20, 2020. https://nsarchive.gwu.edu/news/cyber-vault/2020-05-11/uscybercom-documents-timeline.

Matsakis, Louise. 'The US Sits out an International Cybersecurity Agreement'. *Wired*. November 12, 2018, Accessed September 20, 2020. https://www.wired.com/story/paris-call-cybersecurity-united-states-microsoft/.

Ministry of Defence (UK). 'Cyber Primer: Second Edition'. Development, Concepts and Doctrine Centre. July 20, 2016, Accessed June 30, 2020. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/549291/20160720-Cyber_Primer_ed_2_secured.pdf.

Ministry of Defence (UK). ‘Joint Doctrine Note 1/18: Cyber and Electromagnetic Activities’. Development, Concepts and Doctrine Centre. February, 2018, Accessed June 30, 2020. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/682859/doctrine_uk_cyber_and_electromagnetic_activities_jdn_1_18.pdf.

Morgan, Richard. ‘Oversight through Five Eyes: Institutional Convergence and the Structure and Oversight of Intelligence Activities’. In *Global Intelligence Oversight: Governing Security in the Twenty-First Century*, by Zachary K. Goldman and Samuel J. Rascoff, 37-70. Oxford Scholarship Online, 2016. Accessed June 30, 2020. DOI:10.1093/acprof:oso/9780190458072.003.0003.

Nakashima, Ellen. ‘White House authorises ‘offensive cyber operations’ to deter foreign adversaries’. *The Washington Post*, September 20, 2018. Accessed June 30, 2020. https://www.washingtonpost.com/world/national-security/trump-authorises-offensive-cyber-operations-to-deter-foreign-adversaries-bolton-says/2018/09/20/b5880578-bd0b-11e8-b7d2-0773aa1e33da_story.html.

National Defence (Canada). ‘Strong, Secure, Engaged: Canada’s Defence Policy’. 2017, Accessed June 30, 2020. https://www.canada.ca/content/dam/dnd-mdn/documents/reports/2018/strong-secure-engaged/canada-defence-policy-report.pdf.

New Zealand Government. ‘New Zealand’s cyber security strategy 2019’. July 2019, Accessed June 30, 2020. https://dpmc.govt.nz/sites/default/files/2019-07/Cyber%20Security%20Strategy.pdf.

New Zealand Government. ‘Strategic Defence Policy Statement 2018’. July 2018, Accessed June 30, 2020. http://www.nzdf.mil.nz/downloads/pdf/public-docs/2018/strategic-defence-policy-statement-2018.pdf.

New Zealand. ‘New Zealand Comments: Initial ‘Pre-draft’ of the report of the OEWG on developments in the field of information and telecommunications in the context of international security’. April 2020, Accessed June 30, 2020. https://front.un-arm.org/wp-content/uploads/2020/04/oewg-pre-draft-new-zealand-comments.pdf.

New Zealand. ‘Position Paper on New Zealand’s Participation in the February 2020 Session of the 2019-2020 Open Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security’. February 2020, Accessed June 30, 2020. https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/02/nz-position-paper-on-oewg.pdf.

Parliament of Canada. ‘Bill C-59, An Act Respecting National Security Matters’. 1st session, 42 parliament. June 21, 2019, Accessed June 30, 2020. https://www.parl.ca/legisinfo/BillDetails.aspx?billId=9057418&Language=E.

Parliamentary Counsel Office (New Zealand). ‘Intelligence and Security Act 2017’. October 24, 2019, Accessed June 30, 2020. http://www.legislation.govt.nz/act/public/2017/0010/latest/whole.html#DLM6920923.

Parsons, Christopher & Josh Gold. ‘A Deep Dive into Canada’s Overhaul of Its Foreign Intelligence and Cybersecurity Laws’. *Just Security*. June 2, 2020, Accessed June 30, 2020. https://www.justsecurity.org/70519/a-deep-dive-into-canadas-overhaul-of-its-foreign-intelligence-and-cybersecurity-laws/.

Pomerleau, Mark. ‘Cyber Command Nominee: Attacks Must Come with a Cost’. *Fifth Domain*, March 1, 2018. Accessed June 30, 2020. https://www.fifthdomain.com/dod/cybercom/2018/03/01/cyber-command-nominee-attacks-must-come-with-a-cost/.

Pomerleau, Mark. ‘New Authorities Mean Lots of New Missions at Cyber Command’. *Fifth Domain*, May 8, 2019. Accessed June 30, 2020. https://www.fifthdomain.com/dod/cybercom/2019/05/08/new-authorities-mean-lots-of-new-missions-at-cyber-command/.

Public Safety Canada. 'National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age'. June 12, 2018, Accessed June 30, 2020. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx#s11.

Stilgherrian. 'Blaming Russia for NotPetya Was Coordinated Diplomatic Action'. *ZDNet*, April 12, 2018. Accessed July 1, 2020. https://www.zdnet.com/article/blaming-russia-for-notpetya-was-coordinated-diplomatic-action/.

The White House. 'National Cyber Strategy of the United States of America'. August 1, 2018, Accessed June 30, 2020. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

Thompson, Marcus, & Edward Morgan. 'Information Warfare: An Emergent Australian Defence Force Capability'. Center for Strategic International Studies, Washington, D.C. October 4, 2018, Accessed June 30, 2020. https://www.csis.org/analysis/information-warfare-emergent-australian-defence-force-capability.

Thompson, Marcus. 'Cyber War: The ADF's New Battleground'. *No Limitations (podcast)*, Episode 19, June 12, 2019, YouTube. Accessed June 30, 2020. https://www.youtube.com/watch?v=zojQiWM0pic.

Turnbull, Malcolm. 'Address to Parliament – National Security Update on Counter Terrorism'. Parliament of Australia. November 23, 2016, Accessed June 30, 2020. https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22media/pressrel/4951827%22.

Turnbull, Malcolm. 'Speech at Launch of Australia's Cyber Security Strategy, Sydney'. Parliament of Australia. April 21, 2020, Accessed June 30, 2020. https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22media/pressrel/4513168%22.

Turnbull, Malcolm. 'Offensive Cyber Capability to Fight Cyber Criminals'. June 30, 2017, Accessed June 30, 2020. https://www.malcolmturnbull.com.au/media/offensive-cyber-capability-to-fight-cyber-criminals.

UK Government. 'National Cyber Security Strategy 2016-2021'. 2016, Accessed June 30, 2020. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

United Kingdom. 'Contribution by United Kingdom to the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the context of International Security, February 2020'. March 3, 2020, Accessed June 30, 2020. https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/03/20200303-uk-national-contribution-oewg2.pdf.

United Kingdom. 'UK response to Chair's initial 'Pre-draft' of the report of the OEWG on developments in the field of information and telecommunications in the context of international security'. April 15, 2020, Accessed June 30, 2020. https://front.un-arm.org/wp-content/uploads/2020/04/20200415-oewg-predraft-uk.pdf.

United Nations General Assembly. (2015) 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security'. A/70/174. July 22, 2015, Accessed June 30, 2020. https://undocs.org/A/70/174.

United States Cyber Command. 'Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command'. June 14, 2018, Accessed June 30, 2020. https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010.

United States Government. Presidential Policy Directive 20/PPD-20: ‘US Cyber Operations Policy’. October 2012. Accessed June 30, 2020. https://fas.org/irp/offdocs/ppd/ppd-20.pdf.

United States, House Armed Services Committee. ‘H.R.5515 - John S. McCain National Defense Authorization Act for Fiscal Year 2019’. Washington, D.C., U.S. Government Publishing Office, 2019, Accessed June 30, 2020. https://www.congress.gov/bill/115th-congress/house-bill/5515/text.

United States. ‘United States Comments on the Chair’s Pre-draft of the Report of the UN Open Ended Working Group (OEWG)’. April 6, 2020, Accessed June 30, 2020. https://front.un-arm.org/wp-content/uploads/2020/04/oewg-pre-draft-usg-comments-4-6-2020.pdf.

Uren, Tom, Bart Hogeveen, & Fergus Hanson. ’Defining Offensive Cyber Capabilities’. International Cyber Policy Centre, Australian Strategic Policy Institute. July 4, 2018. Accessed June 30, 2020. https://www.aspi.org.au/report/defining-offensive-cyber-capabilities.

US Department of State. ‘Joint Statement on Advancing Responsible State Behavior in Cyberspace’. September 23, 2019, Accessed June 30, 2020. https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/.

Voo, Julia, Irfan Hemani, Simon Jones, Winnona DeSombre, Dan Cassidy, & Anina Schwarzenbach. ‘National Cyber Power Index 2020’. Belfer Center for Science and International Affairs, Harvard University. September 2020, Accessed October 5, 2020. https://www.belfercenter.org/publication/national-cyber-power-index-2020.

Warrell, Helen. ‘Top general lifts lid on Britain’s cyber attack capability’. *Financial Times*, September 25, 2020, https://www.ft.com/content/702c4589-b4e2-4409-af33-3935b74ea27c.