National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

CANADA’S FORAY INTO OFFENSIVE CYBER: A JOINT CAF-CSE ENDEAVOUR

Maj Guillaume Corriveau

JCSP 43 DL	PCEMI 43 AD
Exercise *Solo Flight*	Exercice *Solo Flight*

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

Avertissement

Les opinons exprimées n’engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES
JCSP 43 DL – PCEMI 43 AD
2017 – 2018

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

CANADA'S FORAY INTO OFFENSIVE CYBER: A JOINT CAF-CSE ENDEAVOUR

Maj Guillaume Corriveau

"This paper was written by a student attending the Canadian Forces College in fulfilment of one of the requirements of the Course of Studies. The paper is a scholastic document, and thus contains facts and opinions, which the author alone considered appropriate and correct for the subject. It does not necessarily reflect the policy or the opinion of any agency, including the Government of Canada and the Canadian Department of National Defence. This paper may not be released, quoted or copied, except with the express permission of the Canadian Department of National Defence."

Word Count: 3097

"La présente étude a été rédigée par un stagiaire du Collège des Forces canadiennes pour satisfaire à l'une des exigences du cours. L'étude est un document qui se rapporte au cours et contient donc des faits et des opinions que seul l'auteur considère appropriés et convenables au sujet. Elle ne reflète pas nécessairement la politique ou l'opinion d'un organisme quelconque, y compris le gouvernement du Canada et le ministère de la Défense nationale du Canada. Il est défendu de diffuser, de citer ou de reproduire cette étude sans la permission expresse du ministère de la Défense nationale."

Compte de mots: 3097

CANADA'S FORAY INTO OFFENSIVE CYBER:
A JOINT CAF-CSE ENDEAVOUR

INTRODUCTION

Canada's National Defence Policy, *Strong, Secure, Engaged*, recognizes that cyberspace is essential for the conduct of modern military operations.[1] It also acknowledges that a purely defensive cyber posture is no longer sufficient and must be accompanied by active cyber operations, a capability that Canada commits to develop and employ against potential adversaries.[2] In declaring its intention to develop an active cyber operation capability[3], Canada is joining a cyber club of approximately a dozen countries that have openly declared their involvement – with various degrees of maturity ranging from early development to sophisticated employment – as perpetrators of Offensive Cyber Operations (OCO).[4] Because of the relative novelty of OCO and its significant reliance on intelligence, many of these countries have nested the development and employment of this capability jointly between their intelligence community (IC) and their military.[5] For example, the United States practices a close partnership between its National Security Agency (NSA) and its U.S. Cyber Command, allowing for maximization of talent and capabilities, leveraging of respective authorities, and a higher degree of effectiveness.[6] Similarly, the United Kingdom's National Offensive Cyber Programme (NOCP) is a partnership,

[1] Government of Canada, *Strong, Secure, Engaged: Canada's Defence Policy* (Ottawa: Department of National Defence, 2017), 72.

[2] *Ibid*.

[3] Initiative number 88 tasks the Canadian Armed Forces to "develop active cyber capabilities and employ them against potential adversaries in support of government-authorized military missions."

[4] James A. Lewis, "The Role of Offensive Cyber Operations in NATO's Collective Defence," *NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)*, 2015, 7.

[5] Aaron Franklin Brantly, *The Decision to Attack – Military and Intelligence Cyber Decision-Making* (Athens, GA: The University of Georgia Press, 2016, 108-109.

[6] Government of the United States of America, *Department of Defense Strategy for Operating in Cyberspace* (Washington D.C.: Department of Defense, 2011), 6.

between their Ministry of Defence and the Government Communications Headquarters (GCHQ), through which both organizations are responsible to develop offensive cyber and through which the skills and techniques of both organizations are harnessed.[7] However, recently within the five eyes community[8] there is growing momentum towards disaggregation of OCO resources between the IC and military. For example, the U.S. Department of Defense is considering the cessation of the dual-hat relationship between NSA and US Cyber Command, in which a single leader is currently at the helm of both organizations, with the seriousness of such consideration warranting its presence in the 2017 National Defense Authorization Act (NDAA).[9] The division of labour, between the IC and military, for the planning and execution of OCO thus remains an open question, one of particular relevance to Canada in light of recent policy announcements.

This paper argues that Canada's foray into OCO ought to be jointly conducted by both the Canadian Armed Forces (CAF) and the Communications Security Establishment (CSE), Canada's signal intelligence agency, until a certain degree of maturity is achieved, after which both organizations ought to be assigned clearer, mutually-exclusive areas of responsibility and separate resources. Joint execution of OCO will, in the short and medium terms, enable Canada to surmount two obstacles inherent to the nascent development and employment of cyber weapons: (1) knowledge barriers; and (2) technical, operational and intelligence barriers.[10]

[7] Government of the United Kingdom, *Intelligence and Security Committee of Parliament – Annual Report 2016-2017* (London: Her Majesty's Government, 2017), 43. Government of the United Kingdom, *National Cyber Security Strategy 2016-2021* (London: Her Majesty's Government, 2016), 51. David J. Lonsdale, "Britain's Emerging Cyber-Strategy," The RUSI Journal 161, no. 4 (August/September 2016), 54. Government of the United Kingdom, *National Security Strategy and Strategic Defence and Security Review 2015* (London: Her Majesty's Government, 2015), 41.

[8] Five eyes is an intelligence alliance comprising of Australia, Canada, the United Kingdom, the United States and New Zealand.

[9] Government of the United States of America, *National Defense Authorization Act for Fiscal Year 2017* (Washington D.C.: House of Representatives), 606-607.

[10] Max Smeets, "What it Takes to Develop a Cyber Weapon," in *Tech & Policy Initiative, Working Paper Series I*, ed. Merit E. Janow (Columbia: School of International and Public Affairs, 2016), 63.

Subsequent disaggregation will enable alleviation of concerns with regards to force employment, use of force escalation and mandate overlap.

KNOWLEDGE CONSIDERATIONS

One of the most significant obstacles to independently achieving, in short and medium terms, the aforementioned objective is the inadequacy of human resources, specifically with regards to knowledge. Indeed, the importance of personnel having the right skills and the difficulties in recruiting and retaining these personnel are nowhere more acute than in the cyber domain, in particular within the area of OCO. Skills are distinctly important due to the 'use and lose' nature of cyberweapons: indeed, "unlike physical weapons, [they] are readily defeated once they are revealed as weapons" due to their dependency on vulnerability exploitation and their victims' ability to fix such vulnerabilities upon discovery of a compromise.[11] To avoid such cyberweapon obsolesce, an OCO programme requires a workforce comprised of skilled hackers capable of continuously developing new surprises.[12] The knowledge required is less of the explicit type (knowledge that can be formally and systematically transferred as, for example, programming in a certain language) and more of the tacit type (knowledge "embedded in a hacker's experience or a cyber command's (implicit) operational processes").[13] Such tacit knowledge is in short supply, as it can only be acquired through experience and is not easily transferrable. The importance of knowledge in the successful prosecution of OCO is consistent with the economics of cyber weapons, in particular with how they differ with conventional

[11] Rebecca Slayton, "What is the Cyber Offense-Defense Balance," *International Security* 41, no. 3 (Winter 2016/17), 86. Karlis Podins and Christian Czosseck, "A Vulnerability-Based Model of Cyber Weapons and its Implications for Cyber Conflict," in *Proceedings of the 11th European Conference on Information Warfare and Security*, ed. Eric Filiol and Robert Erra (Laval: Academic Publishing International Limited, 2012), 200.

[12] *Ibid*.

[13] Smeets, "What it Takes to Develop a Cyber Weapon," 64.

weapons. Indeed, in contrast with conventional weapons, of which the cost mostly accrues to physical production and manufacturing, the cost of cyberweapons "comes from the skilled workers who research, develop, and deploy the technology" rather than from reproduction, the cost of which is negligible.[14] Hence, knowledge comprises a significant ingredient in the successful development and employment of an offensive cyber capability.

Unfortunately, fulfilling the knowledge requirement is difficult due to a significant supply-demand imbalance in the labour market for cyber operators. Both the private and public sector face a persistent shortage of cybersecurity talent: the current global cybersecurity workforce shortfall is estimated to number approximately two million positions, with the skills shortfall being even more acute within the subset of cybersecurity that is relevant to this paper, cyber offense.[15] The labour shortfall is no less present in militaries. Even the United States, whose foray into OCO began much earlier – its defense establishment first discussed cyberwar in 1977, began planning OCO in 1981, and made use of malicious code as early as the 1991 Gulf War – still recognized the insufficiency of its cyber attack personnel in 2010.[16] More recently, its Department of Defense acknowledged the "high demand and relative scarcity of cyber resources" and the U.S. Cyber Command, despite its relative maturity and proximity to the well-established National Security Agency, identified human resources – which it characterizes as

[14] Slayton, "What is the Cyber Offense-Defense Balance", 86.

[15] Government of the United States of America, *Report to Congressional Committees – Cybersecurity Workforce* (Washington D.C.: Government Accountability Office, 2018), 35-36. McAfee, *Hacking the Skills Shortage – A Study of the International Shortage in Cybersecurity Skills* (Santa Clara: McAfee, 2016), 5. Antoine Lemay et al., "Affecting Freedom of Action in Cyber Space: Subtle Effects and Skilled Operators," in *12th International Conference on Cyber Warfare and Security*, ed. Adam R. Bryant, Juan R. Lopez and Robert F. Mills (Reading: Academic Conferences and Publishing International Limited, 2017), 224.

[16] Derek S. Reveron, "An Introduction to National Security and Cyberspace," in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron (Washington D.C.: Georgetown University Press, 2012), 13. William A. Owens, Kenneth W. Dam, and Herbert S. Lin, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington D.C., National Research Council of the National Academies, 2009), S-6.

"high-demand, low-density" – as one of its areas of risk.[17] These cybersecurity labour shortfalls are no less present within Canada's Department of National Defence, whose personnel establishment with regards to defensive cyber operations has a 42% vacancy rate and whose Defence Policy affirms the need to build "the *future* cyber force [emphasis added].[18] In fact, having only recently been tasked, through the release of *Strong, Secure, Engaged* in June 2017, with developing offensive cyber capabilities, it is reasonable to deduce, when considering the higher scarcity of offensive cyber skills relative to defensive cyber skills, that the CAF offensive cyber capability remains in a nascent, non-mature state.

In contrast, the CSE has reached a high degree of maturity with regards to the collective human knowledge held by its cyber workforce, as can be inferred from classified documents leaked by Edward Snowden. If the content of the classified documents is authentic,[19] then indications are that CSE has possessed a Computer Network Exploitation (CNE) capability involved in target development, active collection, and higher-end cyber security exploitation as early as 2010.[20] Additionally, it can be inferred from these documents that CSE's cyber security operations capability was, in 2010, "sophisticated[21], expansive and drove [*sic*] ambitious

[17] Government of the United States of America, *The Department of Defense Cyber Strategy* (Washington D.C.: Department of Defense, 2015), 15. Government of the United States of America, *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command* (Washington D.C.: Department of Defense, 2018), 10.

[18] Government of Canada, *Defence Human Resources Information Management (DHRIM),* (Ottawa: Department of National Defence, 2018). Government of Canada, *Strong, Secure, Engaged*, 72.

[19] The author failed to find evidence of CSE refuting the authenticity of the documents. Conversely, without going so far as to explicitly acknowledging the authenticity of the documents, CSE indicated that the disclosure of the classified documents diminished its short term and long term advantages and caused a cumulative detrimental effect on its operations. Jim Bronskill, "CSE Claims Snowden Leaks Eroding Spy Agency's Advantages," *The Canadian Press*, June 25, 2015, LexisNexis Acadmic.

[20] Government of Canada, *Pay Attention to that Man Behind the Curtain: Discovering Aliens on CNE Infrastructure*, (Ottawa: Communications Security Establishment Canada, 2010), 5-6. Wesley Wark, *CSE and Lawful Access After Snowden*, (Ottawa: University of Ottawa Centre for International Policy Studies, 2016), 18.

[21] Sophisticated, in the context of OCO, describes the exploitation of zero-day vulnerabilities, the use of obfuscation techniques, the ability to establish difficult access to targets, and the in-house development of customized malware. Max Smeets, "Organisational Integration of Offensive Cyber Capabilities: A Primer on the

planning and visions that looked to merge CSE's SIGINT and cyber security functions."[22] The degree of capability maturity being inferred would not be dissimilar from that of the National Security Agency (NSA), with whom CSE has a very close relationship.[23] Only by incubating its nascent offensive cyber capability within CSE will the CAF be capable of fulfilling the tacit knowledge requirements without which the development and employment of offensive cyber capability is not possible.

TECHNICAL, OPERATIONAL, AND INTELLIGENCE CONSIDERATIONS

Second, close integration is required between the CAF's offensive cyber capability and CSE's cyber exploitation capability due to congruencies in the technical, operational and intelligence foundations of each capability. On the surface, both capabilities do not appear, due to their disparate objectives, to be congruent. Indeed, the former seeks to compromise the confidentiality of an adversary's information, whereas the latter seeks, as a direct effect, a loss of integrity, authenticity or availability.[24] However, an in-depth analysis of significant technical, operational and intelligence considerations ought to compel Canada's policy makers to closely integrate both capabilities, at least in the short and medium term until the country's OCO capability reaches maturity.

Benefits and Risks," in *2017 9th International Conference on Cyber Conflict*, ed. H. Roigas, R. Jakschis, L. Lindstrom, and T. Minarik (Tallinn: *NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)*, 2017), 6.

[22] Wesley Wark, *CSE and Lawful Access After Snowden*, 19.

[23] *Ibid.,* 12.

[24] Herbert S. Lin, "Offensive Cyber Operations and the Use of Force," *Journal of National Security Law & Policy* 4, no. 63 (2010): 67.

Technical Considerations

With regards to technical considerations, both OCO and cyber exploitation require three enablers: "a vulnerability, access to that vulnerability, and a payload to be executed."[25] A vulnerability is "an aspect of the system that can be used to compromise that system" and can exist accidentally (through design or implementation defects) or intentionally.[26] Access enables an actor to take advantage of a vulnerability and to deliver a payload. It can take the form of remote access (the launch of a compromise from a distance, e.g. through the Internet) or close access (the launch of a compromise in close proximity, e.g. through local software or hardware).[27] A payload comprises the actions that can be undertaken within an adversary's cyber domain once a vulnerability has been exploited, and it seeks to fulfill the objectives of the cyber exploitation or offensive cyber operation.[28] For example, in a physical world analogy of sensitive paper documents contained in a safe, the vulnerability may be the hinges on the safe and poor building security, the access to that vulnerability would be a particular physical path to that safe, and the payload would be the fire used to destroy the documents, in the case of an attack, or the photocopier used to copy the documents, in the case of an exploitation.

There are important conclusions to be drawn from the fact that within the cyber realm, the first two enablers – a vulnerability and access to that vulnerability – are the same for both capabilities, leaving the third enabler – the payload – as the only difference.[29] First, because much of the technology required to execute both capabilities is the same, there are significant

[25] *Ibid.,* 64.
[26] *Ibid.,* 65.
[27] *Ibid.,* 66.
[28] *Ibid.,* 67.
[29] Herbert S. Lin, "Operational Considerations in Cyber Attack and Cyber Exploitation," in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron (Washington D.C.: Georgetown University Press, 2012), 51.

efficiencies to be gained from jointly conducting OCO and cyber exploitation.[30] Such efficiencies, for example, may be so compelling that cyber exploitation tools are sometimes outfitted with OCO capabilities prior to being launched, or they are designed in such a way that they can be modified in real-time for possible OCO use.[31] In fact, in many cases cyber exploitation is a precursor to OCO.[32] The efficiencies gained can be well understood when considering that "breaking into a particular network may be cheap after the tools and infrastructure are in place [but] building and maintaining the infrastructure for a program of sustained operations requires targeting, research, hardware engineering, software development, and training [which is] not cheap."[33] Second, the technology employed in both capabilities is detectable by an adversary, with the impetus to avoid such detection varying significantly between OCO and cyber exploitation. Indeed, the requirement for its activities to remain covert are much greater for cyber exploitation due to the likelihood, in the event of a known compromise, of an adversary implementing countermeasures and of the loss of that intelligence collector, which could have been used for a prolonged time to conduct multiple exfiltrations of intelligence data.[34]

Operational Considerations

Operational considerations that justify the need to jointly plan and execute OCO are well illustrated when distilling the options available to governments that contemplate what action to undertake against an adversary's cyber capabilities. In essence, on a case-by-case basis there are

[30] *Ibid.*

[31] *Ibid.,* 52.

[32] Barton Gellman and Ellen Nakashima, "U.S. Spy Agencies Mounted 231 Offensive Cyber Operations in 2011, Documents Show," *Washington Post*, August 31, 2013, LexisNexis Academic, 2.

[33] Rebecca Slayton, "What is the Cyber Offense-Defense Balance," 90.

[34] Derek S. Reveron, "An Introduction to National Security and Cyberspace," 51.

only two, often mutually exclusive, options available: render the adversary's cyber capabilities unavailable for serving its purposes (OCO) and "exploit it to gather useful information" (cyber exploitation).[35] These options are often mutually exclusive due to cyber capabilities, by virtue of having been destroyed, being no longer available for exploitation, and due to vulnerabilities and access possibly being disclosed to the adversary as a result of the OCO activities.[36] Evaluating the trade-offs between both options would best be achieved through joint collaboration between the organizations possessing those capabilities. Another operational consideration is the need to deconflict OCO from cyber exploitation. Such deconfliction is made necessary even when, within the context of a particular operation, both activities employ different vulnerabilities and accesses. For example, coding from an OCO tool targeted against an adversary may interfere with the coding from a cyber exploitation tool used against that same adversary. In fact, deconfliction of this nature is required not only between the OCO and cyber exploitation capabilities of individual states, but also between allied states.[37] Such technical and operational considerations ought to compel policy makers to promote organizational constructs that optimize the aggregate OCO and cyber exploitation value. In the case of Canada, the argument would call for OCO to be jointly conducted by the CAF and CSE.

Intelligence Considerations

Intelligence is a critical ingredient for the successful prosecution of OCO; consequently, it will be necessary for the CAF, if it is to successfully develop and execute OCO in the short or

[35] *Ibid.,* 50.

[36] *Ibid.*

[37] *Ibid.*

medium term, to leverage CSE's mature cyber intelligence capabilities.[38] The dependency of OCO on cyber intelligence is well established, with the Offensive Cyber Effects Operations (OCEO)[39] described in the U.S. Presidential Policy Directive – 20 (PPD-20) assessed as unachievable without "significant and ongoing cyber intelligence planning, collection, processing, and reporting."[40] Indeed, OCO require "significant cyber intelligence about target networks and systems, the potential consequences/collateral damage, the operating systems, and anything concerning the related cyber environment including the people, processes, and location."[41] In addition to cyber intelligence about the targets, OCO requires significant intelligence to develop and sustain the *access* to those targets. Such intelligence requirements – with regards to both the target itself and the access to that target – increases proportionally as the degree of OCO sophistication rises. For example, if an offensive cyber operation is intended to be very precise (for example, one for which the target is Iran's uranium-enrichment centrifuges) or is dependent on close (as opposed to remote) access, then substantial intelligence information will be required.[42] Intelligence "informs the decision-making of policy-makers when engaging in covert cyber action directed against a potential adversary."[43] The acute dependency of OCO on intelligence and the greater length of time required to gather such intelligence is succinctly captured by Lin, a renowned cyber security scholar:

[38] Cyber Intelligence, also referred to as Cyber Exploitation, is defined as "prior knowledge of threats and vulnerabilities to information communications systems through a variety of technical means." Aaron Franklin Brantly, *The Decision to Attack – Military and Intelligence Cyber Decision-Making*, 104.

[39] Offensive Cyber Effects Operations are operations intended to produce cyber effects. Constance Uthoff, "Strategic Cyber Intelligence: An Examination of Practices Across Industry, Government, and Military," in *Current and Emerging Trends in Cyber Operations: Policy, Strategy and Practice*, ed. Frederic Lemieux (New York: Palgrave Macmillan, 2015), 216.

[40] *Ibid.*

[41] *Ibid.*

[42] Derek S. Reveron, "An Introduction to National Security and Cyberspace," 44.

[43] Aaron Franklin Brantly, *The Decision to Attack – Military and Intelligence Cyber Decision-Making*, 101.

> *"Information collection for cyber-attack planning differs from traditional collection for kinetic operations in that it may require greater lead time and may have expanded collection, production, and dissemination requirements because specific sources and methods may need to be positioned and employed over time to collect the necessary information and conduct necessary analyses."*[44]

More importantly, sophisticated OCO will likely require "continued and uncontested access to a target [that] takes time to develop and sustain, which again indicates collaboration with cyber intelligence functions."[45] Further, due to a global competition analogous to the arms and space races, the relationship between cyber intelligence and OCO is evolving towards a greater degree of dependency, with "cyber intelligence methodologies [becoming] increasingly essential, sophisticated, and integrated more closely with cyber operations."[46] Due to other challenges specifically inherent to the use of cyber weapons, such as the complexity of collateral effects, OCO requires practitioners of cyber intelligence to have the "resources and specific targets identified and then prepared long before the need to strike."[47]

The aforementioned knowledge, technical, operational, and intelligence foundations justify, especially during early OCO capability development stages, the joint development of OCO between the organization formally tasked with its development and execution and the organization tasked with cyber exploitation, CAF and CSE respectively. Such an arrangement would mirror the close intertwinement of cyber intelligence and military operations observed south of the border with the dual-hat nature of Commander US CYBERCOM and Director

[44] Derek S. Reveron, "An Introduction to National Security and Cyberspace," 44.

[45] Constance Uthoff, "Strategic Cyber Intelligence: An Examination of Practices Across Industry, Government, and Military," 216.

[46] *Ibid.,* 213.

[47] *Ibid.,* 217.

NSA.[48] CSE possesses advanced cyber exploitation capability that ought to be leveraged for the CAF's OCO capabilities, similar to how the NSA and US CYBERCOM arrangement has enabled the latter to "leverage the capability development, personnel, facilities, infrastructure, testing capabilities, and business processes of NSA/CSS to support CYBERCOM operations."[49]

DISAGGREGATION IN THE LONG TERM

Having established the need for OCO to be jointly conducted by the CAF and the CSE, this paper argues that this arrangement should end when a certain degree of maturity is achieved, likely several years from now, after which both organizations ought to be assigned clearer, mutually-exclusive areas of responsibility and separate resources. Such disaggregation would alleviate concerns with regards to force employment, use of force escalation and mandate overlap.[50]

With regards to force employment, as Canada develops its OCO capability, eventually it will possess the means to harness the kinetic potential of cyber to achieve strategic effects. The wielding of such use of force rests squarely within the CAF, as opposed to the CSE, with concerns during the initial stages of Canada's OCO development being attenuated due to kinetic effects being within the grasp of OCO only during its advanced stages of maturity.[51] The disaggregation would also render clearer that OCO ought to be prosecuted by militaries, with some scholars advocating that "the use of cyber as an intelligence asset should be separated from

[48] *Ibid.,* 215.

[49] Government of the United States of America, *Report to Congressional Committees – Defense Cybersecurity* (Washington D.C.: Government Accountability Office, 2017), 14.

[50] Frank J. Cilluffo and Joseph R. Clark, "Preparing for NetWars: Repurposing Cyber Command," *Parameters* 43, no. 4 (Winter 2013-14), 116.

[51] *Ibid.,* 112.

the use of cyber as a military asset."[52] Indeed, "once the intelligence community identifies a target and the national command authority makes the decision to act, [the armed forces should] 'pull the trigger'."[53]

Disaggregation would also reduce the risk of unintended escalation. Some of the effects of OCO would, under current bodies of law such as the United Nations Charter, as well as customary international law, are considered to constitute use of force, while other effects are regarded as a threat of the use of force, with such actions justifying retaliatory use of force responses.[54] Since it is very easy, due to their technical similarities, to mistaken cyber exploitation for OCO, a nation targeted in a cyber exploitation is unlikely to know the operation's intent and can hence easily misconstrue it as OCO.[55] One of the means with which the risk of misinterpretation could be reduced is conducting OCO "in such a way that cyberexploitations are clearly distinguishable in a technical sense from cyber attack."[56] Further distinctions regarding the author of the attack that go beyond the nation and include the specific agency would further reduce the risk of misinterpreting OCO for cyber exploitation. Disaggregation in the conduct of OCO between CSE and CAF would support that intent.

Lastly, disaggregation may promote the necessity to more clearly delineate the roles assigned to CAF and CSE in the realm of OCO and active cyber operations, which currently overlap. Indeed, the active cyber operations mandate currently being considered for CSE go beyond the cyber exploitation role and encroach upon use of force, which is the military's responsibility. While such a mandate will be useful for the short and medium term joint

[52] *Ibid.,* 115.
[53] *Ibid.*
[54] Herbert S. Lin, "Offensive Cyber Operations and the Use of Force," 71-72.
[55] *Ibid.* 82. Steven G. Bradbury, "The Developing Legal Framework for Defensive and Offensive Cyber Operations," *Harvard National Security Journal* 2 (2011), 17.
[56] Herbert S. Lin, "Offensive Cyber Operations and the Use of Force," 82.

collaboration between CSE and CAF, in the long term a CSE mandate constriction that more clearly provides for OCO as a mutually-exclusive area of responsibility for the CAF is recommended.

CONCLUSION

In the short and medium term, Canada's foray into OCO ought to be jointly conducted by both the CAF and CSE. Such joint execution will enable Canada to surmount two obstacles inherent to the nascent development and employment of cyber weapons: (1) knowledge barriers; and (2) technical, operational and intelligence barriers. Due to the relative immaturity of the CAF's OCO capabilities and the technical and operational requirements that underlie its employment, the CAF will only successfully accomplish initiative number 88 of Canada's Defence Policy if it joins forces with CSE in jointly developing and employing OCO. Such jointness in organization, resourcing and accountability should only endure until Canada's OCO capabilities reach a yet undefined level of maturity, at which point the CAF ought to independently prosecute OCO, albeit still in close collaboration with CSE. Such disaggregation will alleviate concerns with regards to force employment, use of force escalation and mandate overlap.

BIBLIOGRAPHY

Bradbury, Steven G. “The Developing Legal Framework for Defensive and Offensive Cyber Operations.” *Harvard National Security Journal* 2 (2011).

Brantly, Aaron Franklin. *The Decision to Attack – Military and Intelligence Cyber Decision-Making.* Athens, GA: The University of Georgia Press, 2016.

Bronskill Jim. “CSE Claims Snowden Leaks Eroding Spy Agency’s Advantages.” *The Canadian Press*, June 25, 2015. LexisNexis Acadmic.

Cilluffo, Frank J. and Clark, Joseph R. “Preparing for NetWars: Repurposing Cyber Command.” *Parameters* 43, no. 4 (Winter 2013-14), 111-118.

Gellman, Barton and Nakashima, Ellen. “U.S. Spy Agencies Mounted 231 Offensive Cyber Operations in 2011, Documents Show,” *Washington Post*, August 31, 2013, LexisNexis Academic.

Government of Canada. *Strong, Secure, Engaged: Canada's Defence Policy*. Ottawa: Department of National Defence, 2017.

Government of Canada. *Defence Human Resources Information Management (DHRIM).* Ottawa: Department of National Defence, 2018.

Government of Canada. *Pay Attention to that Man Behind the Curtain: Discovering Aliens on CNE Infrastructure*. Ottawa: Communications Security Establishment Canada, 2010. Available at: available at: https://christopher-parsons.com/Main/wp-content/uploads/2015/02/cse-pay-attention-to.pdf

Government of the United Kingdom. *Intelligence and Security Committee of Parliament – Annual Report 2016-2017*. London: Her Majesty’s Government, 2017.

Government of the United Kingdom. *National Cyber Security Strategy 2016-2021*. London: Her Majesty’s Government, 2016.

Government of the United Kingdom. *National Security Strategy and Strategic Defence and Security Review 2015*. London: Her Majesty’s Government, 2015.

Government of the United States of America. *Report to Congressional Committees – Cybersecurity Workforce*. Washington D.C.: Government Accountability Office, 2018.

Government of the United States of America. *Department of Defense Strategy for Operating in Cyberspace*. Washington D.C.: Department of Defense, 2011.

Government of the United States of America. *The Department of Defense Cyber Strategy* (Washington D.C.: Department of Defense, 2015.

Government of the United States of America. *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command*. Washington D.C.: Department of Defense, 2018.

Government of the United States of America. *Report to Congressional Committees – Defense Cybersecurity.* Washington D.C.: Government Accountability Office, 2017.

Government of the United States of America. *National Defense Authorization Act for Fiscal Year 2017*. Washington D.C.: House of Representatives.

Lemay, Antoine *et al*. "Affecting Freedom of Action in Cyber Space: Subtle Effects and Skilled Operators," in *12th International Conference on Cyber Warfare and Security*, ed. Adam R. Bryant, Juan R. Lopez and Robert F. Mills. Reading: Academic Conferences and Publishing International Limited, 2017.

Lewis, James A. "The Role of Offensive Cyber Operations in NATO's Collective Defence." *NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)*, 2015.

Lin, Herbert S. "Operational Considerations in Cyber Attack and Cyber Exploitation," in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron. Washington D.C.: Georgetown University Press, 2012.

Lin, Herbert S. "Offensive Cyber Operations and the Use of Force." *Journal of National Security Law & Policy* 4, no. 63 (2010): 63-86.

Lonsdale, David J. "Britain's Emerging Cyber-Strategy." The RUSI Journal 161, no. 4 (August/September 2016): 52-62.

McAfee. *Hacking the Skills Shortage – A Study of the International Shortage in Cybersecurity Skills*. Santa Clara: McAfee, 2016.

Owens, William A., *et al. Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities.* Washington D.C., National Research Council of the National Academies, 2009.

Podins, Karlis and Czosseck, Christian. "A Vulnerability-Based Model of Cyber Weapons and its Implications for Cyber Conflict," in *Proceedings of the 11th European Conference on Information Warfare and Security*, ed. Eric Filiol and Robert Erra. Laval: Academic Publishing International Limited, 2012.

Reveron, Derek S. "An Introduction to National Security and Cyberspace," in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron. Washington D.C.: Georgetown University Press, 2012.

Slayton, Rebecca. "What is the Cyber Offense-Defense Balance." *International Security* 41, no. 3 (Winter 2016/17): 72-109.

Smeets, Max. "What it Takes to Develop a Cyber Weapon," in *Tech & Policy Initiative, Working Paper Series I*, ed. Merit E. Janow. Columbia: School of International and Public Affairs, 2016, 49-67.

Smeets, Max. "Organisational Integration of Offensive Cyber Capabilities: A Primer on the Benefits and Risks," in *2017 9th International Conference on Cyber Conflict*, ed. H. Roigas, R. Jakschis, L. Lindstrom, and T. Minarik. Tallinn: *NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)*, 2017.

Uthoff, Constance. "Strategic Cyber Intelligence: An Examination of Practices Across Industry, Government, and Military," in *Current and Emerging Trends in Cyber Operations: Policy, Strategy and Practice*, ed. Frederic Lemieux. New York: Palgrave Macmillan, 2015.

Wark, Wesley. *CSE and Lawful Access After Snowden*. Ottawa: University of Ottawa Centre for International Policy Studies, 2016.