UNPACKING 'WICKED PROBLEMS' OF CYBERSPACE: CONCEPTUAL APPROACHES FOR NOVICE PRACTITIONERS

Lieutenant-Commander Kenneth Ingram

JCSP 45

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.

PCEMI 45

Solo Flight

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.

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES

JCSP 45 – PCEMI 45
2018 – 2020

SOLO FLIGHT

UNPACKING 'WICKED PROBLEMS' OF CYBERSPACE: CONCEPTUAL APPROACHES FOR NOVICE PRACTITIONERS

Lieutenant-Commander Kenneth Ingram

UNPACKING ‘WICKED PROBLEMS” OF CYBERSPACE: CONCEPTUAL APPROACHES FOR NOVICE PRACTICIONERS

INTRODUCTION

Regardless of training or vocation, every cybersecurity professional faces the difficulty of first conceptualizing cyberspace and subsequently articulating it to others. A dearth of discourse within DND/CAF specifically examines this phenomenon and it’s a dilemma because the language we use matters—especially in policy yet extendable to advisors, diplomats, and the decisions made not only by senior leaders but also everyday computer users.

Borrowed metaphors such as ‘viruses’ and ‘infections’ are often employed when describing cyber-related threats. Others, such as ‘trojans’, draw from particular histories of warfare. We are routinely warned about future dangers by references to the past. Culturally specific conflicts such as ‘cyber Pearl Harbor’, ‘cyber 9/11’, or ‘cyber Armageddon’ saturate much of the contemporary literature. Perhaps most menacing, however, is the use of ‘cyber’ as a subject, adverb, adjective, and noun; paradoxically communicating everything and nothing. Additional terms, such as ‘cyber attack’ and ‘hack’, colloquially define *any unwelcomed incident* affecting a computer, peripheral device, or data. These examples have become normative in everyday language and require astute attention.

This paper examines some of the most common language, imagery, and other non-technical factors associated with cyberspace – including intersectional policies and competing priorities. These factors are critical aspects of cybersecurity yet they are often ignored, eclipsed, or rendered invisible by other facets of the warfighting domain. This approach reveals underlying problems. If unaddressed, they will continue to impede progress towards addressing 'wicked problems' of cyberspace.

WICKED PROBLEMS OF CYBERSPACE

'Wicked problems' are an important concept in public policy[1] and are highly relevant to cyberspace – particularly from the perspective of national security. Since the term emerged in the late 1960s (its origin is discussed in detail elsewhere),[2] 'wicked problems' present "pressing and highly complex issues for policy formulation that involve many causal factors and high levels of disagreement about the nature of a problem and the best way to handle it."[3] As Bateman (2011) notes, the term 'wicked' is not to imply something is evil. Rather, it describes "a problem that is highly resistant to resolution."[4] Other examples of 'wicked problems' include the nature of poverty,[5] maritime security,[6] health inequalities,[7] and (I contend) politics of the English language.[8] These problems, whether analogous or highly relevant to cyberspace, entangle fundamental differences between stakeholders whereby effective solutions require

[1] Bateman, Sam. 2011. "Solving the "Wicked Problems" of Maritime Security: Are Regional Forums up to the Task?", *Contemporary Southeast Asia*, Vol 33(1), p 1.

[2] Skaburskis, Andrejs. June 2008. "The Origin of "Wicked Problems"', Planning Theory and Practice, Vol 9(2), 227-280.

[3] Bateman, Sam. 2011. "Solving the "Wicked Problems" of Maritime Security: Are Regional Forums up to the Task?", Contemporary Southeast Asia, Vol 33(1), p 2.

[4] *ibid*., p 2.

[5] Rittel, Horst W. and Melvin M. Webber. "Planning Problems are Wicked Problems", 1973, from "Dilemmas in a General Theory of Planning", *Policy Sciences*, 4, 155-69, retrieved 22 May 2020: https://cec.prodwebb.lu.se/sites/cec.prodwebb.lu.se/files/rittel_and_webber_1973_planning_problems_are_wicked_problems.pdf.

[6] Bateman, Sam. 2011. "Solving the "Wicked Problems" of Maritime Security: Are Regional Forums up to the Task?", Contemporary Southeast Asia, Vol 33(1), pp 1-28. P1.

[7] National Collaborating Centre for Healthy Public Policy. June 2013, "Wicked Problems and Public Policy", retrieved 24 May 2020: http://www.ncchpp.ca/docs/WickedProblems_FactSheet_NCCHPP.pdf.

[8] Orwell, George. 1968. "Politics and the English Language." In the collected essays, journalism, and letters of George Orwell, ed. Sonia Orwell and Ian Angos, vol 4(1), 127-40. New York: Harcourt, Brace, Javanovich. Retrieved 24 May 2020: https://faculty.washington.edu/rsoder/EDLPS579/HonorsOrwellPoliticsEnglishLanguage.pdf.

changes to both mindset and behaviour. Most recently, efforts are underway to eliminate the word ‘cyber’ as jargon and replace ‘cybersecurity’ with the term ‘digital security’.[9]

Pressing, Highly Complex Issues

There is no shortage of major media headlines, alerts, and other sources of disclosure to demonstrate overwhelming evidence that our data and computer networks are vulnerable. Cyber-espionage was cited as a means for “the greatest transfer of wealth in history” nearly a decade ago and remains rampant.[10] Other malicious activities – with disproportionate severity – apparently seek to degrade, deny, disrupt, or destroy critical infrastructure or influence democratic elections. A sense of urgency is palpable from news cycles, senior officials, cybersecurity professionals, advocacy groups, and alleged victims.

Underlying political, administrative, and policy elements are almost certainly present although they progress at a comparatively glacial pace (and are thus far less appealing to most audiences) compared to the more sensational aspects of cyber-related threats. Many of the complex issues we face concerning cyberspace are in fact, not new. Previous candidates of the Canadian Forces College (CFC) Joint Command and Staff Programme (JCSP) have examined more than a dozen cyber-related topics. Each paper illuminate a dimension of cyberspace from a particular DND/CAF lens, offering valuable

[9] Organisation for Economic Cooperation and Development. 2019. Digital Security and Privacy. Retrieved 24 May 2020: https://www.oecd.org/going-digital/topics/digital-security-and-privacy/.

[10] Remarks in 2012 by U.S. General Keith Alexander, then director of the National Security Agency and Commander of US Cyber Command. This quote inevitably appears in most Western literature concerning national security and cyberspace. Rogin, Josh. 9 July 2012. “NSA Chief: Cybercrime constitutes the ‘greatest transfer of wealth in history’”, *Foreign Policy*, retrieved 24 May 2020: https://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/.

insight regarding deterrence,[11] procurement,[12] decentralized military functions,[13] capability gaps,[14] broad capability development proposals,[15] environment-specific requirements such as within the Royal Canadian Navy,[16] integration of the Primary Reserve within force generation and force employment models,[17] joint offensive cyber operations with the CAF and Canada's national cryptologic agency[18] and a need for clear strategic direction including a blueprint for hiring talent,[19] amongst others.[20,21,22] These papers, including the most recent ones, also demonstrate that Canadian defence policy continues to adjust as some cited entities no longer exist and terminology remain in flux.

While beyond the scope of this paper, other 'wicked problems' presented by cyberspace that warrant further consideration include the widespread inadequacy of contemporary computer literacy skills; insider threats and also 'unintentional insiders' –

[11] Bégin, Daniel. May 2019. "More than just ones and zeros: Canadian cyber deterrence posture", JCSP 45, retrieved 16 May 2020: https://www.cfc.forces.gc.ca/259/290/308/305/begin.pdf.

[12] Turner, J.T.D.S. 2016. "Buy Cyber-Secure: Improving Cybersecurity of Procured Combat Systems", JCSP 42, retrieved 12 May 2020: https://www.cfc.forces.gc.ca/259/290/318/286/turner.pdf.

[13] Yu, Howard. 2018. "Decentralized Cyber Forces: Cyber Functions at the Operational and Tactical Levels", JCSP 44, retrieved 16 May 2020: https://www.cfc.forces.gc.ca/259/290/405/305/yu.pdf.

[14] Dias, R.F.J. 2016. 'The Institutional Cyber Gap Within the Canadian Armed Forces", JCSP 42, retrieved 12 May 2020: https://www.cfc.forces.gc.ca/259/290/318/192/dias.pdf.

[15] Chouinard-Prévost, R. 2017. "Cyber Capability Development: Considerations for Optimizing Organizational Form in the DND/CAF", JCSP 43, retrieved 16 May 2020: https://www.cfc.forces.gc.ca/259/290/402/305/chouinard-prevost.pdf.

[16] Lanouette, J.M. 2016. "Naval Cyber Warfare Capability Requirement", JCSP 42, retrieved 12 May 2020: https://www.cfc.forces.gc.ca/259/290/318/192/lanouette.pdf.

[17] Day, Malcolm. 2018. "Developing the CAF Cyber Capability: The Need to Integrate the Reserve", JCSP 43, retrieved 14 May 2020: https://www.cfc.forces.gc.ca/259/290/402/305/day.pdf.

[18] Corriveau, Guillaume. 2018. "Canada's Foray into Offensive Cyber: A Joint CAF-CSE Endeavour", JCSP 43, retrieved 22 May 2020: https://www.cfc.forces.gc.ca/259/290/402/305/corriveau.pdf.

[19] Smibert, Devon. 2019. "Building Cyber Operations in the Canadian Armed Forces: A Blueprint to Lay a Solid Foundation", JCSP 42, retrieved 12 May 2020: https://www.cfc.forces.gc.ca/259/290/318/286/smibert.pdf.

[20] Walkling, L.C. 2013. "Considerations: Canadian Forces' Efforts in the Electromagnetic Spectrum and Cyber Operating Environment", JCSP 39, retrieved 12 May 2020: https://www.cfc.forces.gc.ca/259/290/299/286/walkling.pdf.

[21] Lyttle, R.J. 2016. "Due Online: Is Canadian Cyber Culture Secure?", JCSP 40, retrieved 12 May 2020: https://www.cfc.forces.gc.ca/259/290/301/305/lyttle.pdf.

[22] Marshall, N.B. 2016. "Offensive Cyber in the Canadian Armed Forces: Opportunities from Bill C-51", JCSP 42, retrieved 12 May 2020: https://www.cfc.forces.gc.ca/259/290/318/192/marshalln.pdf.

those who elevate risk due to their own cognitive bias, routines, and behaviour that prioritizes trust[23] and convenience[24] rather than best practices and common sense. Research demonstrates that scaring people about cyber-related threats doesn't improve cybersecurity and often has the opposite intended effect.[25] Shifting away from predominantly human factors, disruptions to defence-related logistics support and tainted supply chains, including fake parts[26] or 'digital backdoors', pose risks to mission assurance, force projection, and force sustainment. At this very moment, cyber-espionage activity is probably harvesting proprietary information from cleared defence contractors who are preparing sophisticated multibillion-dollar platforms of the future (in essence, 'systems of systems').[27,28] A technological 'arms race' also exists between nations as they compete for raw materials, semiconductors,[29] telecommunications equipment and bulk data.

[23] Multiple studies have shown that employees with pick up derelict USB sticks, such as those left in parking lots, and violate basic cybersecurity policies by plugging the device into computers because they want to learn who owns the USB and return it to avoid trouble. Sterling, Bruce. 29 June 2011. "The Dropped Drive Hack", *Wired*, retrieved 11 May 2020: https://www.wired.com/2011/06/the-dropped-drive-hack/.

[24] Constant access to streaming services, voice assistants, and other internet-connected smart-devices increase the number of potential vulnerabilities and overall risk surface. Mee, Paul, and Nico Brandenburg. 14 April 2020. "Digital Convenience Threatens Cybersecurity", *MIT Sloan Management Review*, retrieved 24 May 2020: https://sloanreview.mit.edu/article/digital-convenience-threatens-cybersecurity/.

[25] Palmer, Danny. 6 June 2019. "Don't let cybersecurity be driven by fear, warns NCSC chief", *ZDNet*, retrieved 23 May 2020: https://www.zdnet.com/article/dont-let-cyber-security-be-driven-by-fear-warns-ncsc-chief/.

[26] Bogus components were discovered in Hercules C130J aircraft since at least July 2012. Weston, Greg. 9 January 2013."Fake Parts in Hercules Aircraft Called a Genuine Risk", *CBC News*, retrieved 24 May 2020: https://www.cbc.ca/news/politics/fake-parts-in-hercules-aircraft-called-a-genuine-risk-1.1345862.

[27] Singh, Abhijit. 27 August 2016. "India and the Scorpene Leak: Untangling the Knots", *The Diplomat*, retrieved 24 May 2020: https://thediplomat.com/2016/08/india-and-the-scorpene-leak-untangling-the-knots/.

[28] Ling, Justin. 24 March 2016. "Man Who Sold F-35 Secrets to China Pleads Guilty", *Vice News*, retrieved 24 May 2020: https://www.vice.com/en_us/article/kz9xgn/man-who-sold-f-35-secrets-to-china-pleads-guilty.

[29] Swanson, Ana, and Cecilia Kang. 20 January 2020. "Trumps China Deal Creates Collateral Damage for Tech Firms", *The New York Times*, retrieved 24 May 2020: https://www.nytimes.com/2020/01/20/business/economy/trump-us-china-deal-micron-trade-war.html.

By no means are these examples mutually exclusive. When considering the enormity of the problem, surmised by Major-General Loos as a domain "increasingly more complex, congested and contested",[30] we must also acknowledge the speed of technological advancements—their inclusion within our homes and workplaces whether afloat, on land or in the air—far outpacing policy formulation and implementation.[31]

At first glance, these complex problems appear to align with the type of 'wicked problems' defined by Roberts (2000) whereby "stakeholders agree on the nature of the problem, but not on the solutions".[32] Looking to a global perspective, however, further conflates the nature, urgency, and complexity of these issues. There are profound opposing perspectives about what cyberspace is and what it represents. Russia and China do not use the word 'cyber' and opt for terms such as 'informationalization' and 'digital confrontation'. These differences are not merely linguistic. They present profound ideological disparities whereby 'access to the internet and free expression' (primarily Western constructs) clashes with deeply held convictions that cast information as a threat to be highly regulated, censored, and controlled. Questions about intellectual property, state sovereignty, privacy and human rights are also part of the discourse.

[30] *The Maple Leaf Defence Stories*: DND/CAF Welcomes First Cyber Operators. 8 January 2018. Retrieved 16 May 2020: https://ml-fd.caf-fac.ca/en/2018/01/9092.

[31] DND's 2009 Integrated Capstone Concept by Chief of Force Development noted "a continuing challenge will be to ensure our policy and doctrine keep up with the pace of change in the cyberspace domain". Canada. Department of National Defence, Integrated Capstone Concept (Ottawa: Chief of Force Development, 2009), p 30.

[32] National Collaborating Centre for Healthy Public Policy. June 2013, "Wicked Problems and Public Policy", retrieved 24 May 2020: http://www.ncchpp.ca/docs/WickedProblems_FactSheet_NCCHPP.pdf.

Ongoing Limitations of Policy Formulation

The *Canada First Defence Strategy* (2008) was a milestone for introducing the word 'cyber'[33] into the lexicon of Canadian defence papers although it appears only once in the document.[34] It's lengthier 2017 successor, *Strong, Secure, Engaged* (*SSE*), mentions 'cyber' a total of 87 times using 24 different variations – all of which are undefined. The variation is noteworthy because each term conceivably conveys a different meaning and interpretation within DND/CAF, Government of Canada (GoC), and abroad including allies and potential adversaries. While the prevalence of cyber-related words in the 113-page document is unprecedented for a Canadian defence paper, *SSE* articulates very little meaning for the public or the majority of the Defence Team when it comes to cyberspace.

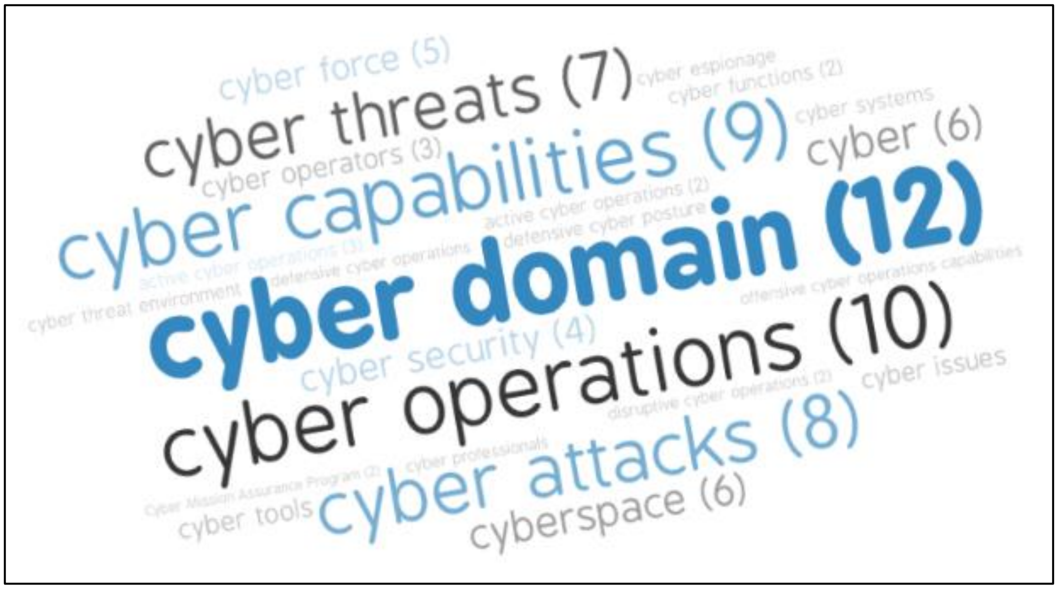


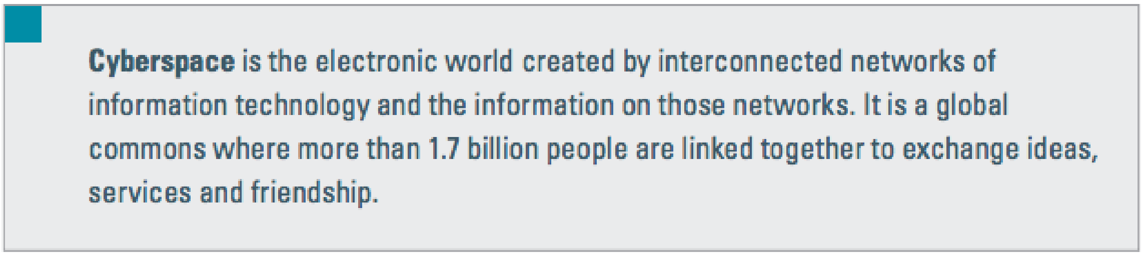
Image 1: Graphic illustration for cyber-related words, terms, and concepts in *SSE*.
Size of font is relative to the number of times a term appears (displayed as a number).
Those without a number appear in the document only once.

[33] *ibid*., p1.

[34] The word 'cyber' appears once in the term 'cyber attack' and references Canada's need to address asymmetric threats in a complex security environment along with terrorism and insurgencies. Canada. Department of National Defence, Canada First Defence Strategy (Ottawa, 2010). Retrieved 22 May 2020: https://www.canada.ca/content/dam/dnd-mdn/migration/assets/FORCES_Internet/docs/en/about/CFDS-SDCD-eng.pdf.

Note: some sums are inferred based on sentence structure in the original document.
Source: created by author using WordArt.com.

Canada's first national Cyber Security Strategy (also known as a first-generation policy) took a few years to formulate before it was release in 2010 by Public Safety Canada.[35] The document defines cyberspace as:



Cyberspace is the electronic world created by interconnected networks of information technology and the information on those networks. It is a global commons where more than 1.7 billion people are linked together to exchange ideas, services and friendship.

Image 2: Screenshot of Canada's national definition of cyberspace in 2010.
Source: *Canada's Cyber Security Strategy*, 2.

It briefly describes a three-pillar strategy without addressing the specifics of *how* progress will be made, *who* is responsible, or *what* the mandates are. It may be concluded that the document's main premise, like other first-generation policies by other like-minded countries at the time, was to characterize 'cyber' as something new and something different (a characterization since contested or abandoned).[36] It also established the sentiment that government should be organized to face cyber-related threats and prioritized federal funding.[37]

In our current *National Cyber Security Strategy*, the definition for cyberspace was amended to note "more than 3 billion people" (vice 1.7b) in 2018. While not explicit, this

[35] Canada. Public Safety Canada, Canada's Cyber Security Strategy (2010). Retrieved 24 May 2020: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/archive-cbr-scrt-strtgy/archive-cbr-scrt-strtgy-eng.pdf.
[36] The perspective that cyberspace is not new, special, or unique is not intended to be pejorative. Arguably, it fosters more important discussions about responsibility and accountability whereby 'cyber' isn't something fundamentally 'extra' that has to be added, but rather accepted. Canada. Department of National Defence, CF Cyber Force Development: Director's View, October 2012.
[37] Phone interview with Mr. Corey Michael Dvorkin, Acting Policy Director for Cyber Security in Public Safety Canada, 23 May 2020. Mr. Dvorkin has extensive experience in cyber-related policy.

change suggests that cyberspace is contingent on the number of people with access to it rather than the majority of the world's population who are excluded.[38] The document also notes other cyber security action plans that will supplement the strategy and it will align with other GoC cyber-related initiatives, including "the Canadian military's use of cyber" (this is the only reference to DND/CAF in the entire document).[39] Objectives are set, but not priorities.

The following alternative definition of cyberspace, proposed in 2016 at the Joint Terminology Panel, does not mention humans and characterizes it as "[t]he element of the operational environment that consists of interdependent networks of information technology structures – including the Internet, telecommunications networks, computer systems, embedded processors and controllers – as well as the software and data that reside within them."

While not intended to be an exhaustive examination of national or governmental policies, this brief examination aligns with the observation that "wicked problems lack agreement on both a definition and a solution" – even at the national level – yet "any fruitful attempt to tackle a wicked problem will of necessity be multisectoral".[40]

Intersectional Policies and Competing Priorities

In early 2018, the Royal Canadian Navy announced it was lifting the 'draconian' policy of prohibiting Wi-Fi coverage in warships so that sailors could achieve a better

[38] Canada. Public Safety Canada, National Cyber Security Strategy (2018), p 34. Retrieved 24 May 2020: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf.
[39] *ibid.*, p 5.
[40] National Collaborating Centre for Healthy Public Policy. June 2013, "Wicked Problems and Public Policy", p 2.

work-life balance and communicate with their families back home.[41] At around the same time yet unrelated, the U.S. military was unexpectedly forced to re-examine its security policies after the location of bases, routes, and perimeters were disclosed as part of a larger data set of approximately 13 trillion GPS points from users of a mobile personal fitness tracker.[42] These examples offer a small glimpse of intersectional policies and competing priorities (i.e. fitness, morale, recruiting and retention) that the CAF must manage moving forward as technology – and expectations – change.

Cyber Operator, a relatively new military occupation in the CAF that was created in 2017, is specifically noted in *Strong, Secure Engaged* "to attract Canada's best and brightest talent and significantly increasing the number of military personnel dedicated to cyber functions."[43] The Defence Women's Advisory Organization, created to encourage diversity in the CAF by addressing and overcoming barriers that women face, met in Ottawa during January 2019 when the Deputy Vice Chief of the Defence Staff, Major-General Frances Allen, discussed her previous experience as Director General Cyberspace and Joint Force Cyber Component Commander. The *Defence Story* notes "the rapidly growing cyber workforce has exciting opportunities for women with an interest in any aspect of the cyber field" with specific examples such as planning, policy, law, and human resources.[44] Of the 99 Cyber Operator positions in total, 76 are presently filled although the vast majority of them (73) were drawn from in-service selection

[41] Brewster, Murray. 11 January 2018. "Navy Dropping 'draconian' Policy on Warship Wi-Fi, Admiral Says", *CBC News*, retrieved 24 May 2020: https://www.cbc.ca/news/politics/navy-warship-wifi-1.4481346.
[42] Hsu, Jeremy. 29 January 2018. "The Strava Heat Map and the End of Secrets", *Wired*, retrieved 24 May 2020: https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/.
[43] Canada. Department of National Defence, Strong, Secure, Engaged: Canada's Defence Policy (Ottawa, 2017), p 111.
[44] *The Maple Leaf Defence Stories*, "MGen Allen Speaks About Cyber at the Defence Women's Advisory Organisation", 29 January 2019. Retrieved 16 May 2020: https://ml-fd.caf-fac.ca/en/2019/01/24165.

programs (personnel already in the CAF) while only three were Direct Entry (recruited from outside the military).[45] The profile of "Canada's first female Cyber Operator" appeared in a Canadian military magazine as of November 2019 - and to its credit - noted she holds an arts degree whereby technical and creative skills allow her bring the whole picture together.[46] She is presently one of only two Cyber Operators who identify as female.[47] With the objective of increasing representation of women in the CAF towards the goal of 25 percent, progress within the Cyber Operator trade—albeit one microcosm amongst roughly 90 occupations[48]—is not promising.

VISUALIZING 'CYBER'

When attempting to visualize cyberspace or cybersecurity, human factors are usually the first to be omitted. While more technical aspects such as hardware, software, and packets of information are inherent to the field, humans remain the primary actors and stakeholders as they are inevitably behind most keyboards and interfaces despite varying levels of automation.

Yet media, private vendors, and television shows continue to portray 'hackers' wearing hoodies, masks, or black balaclavas. These depictions perpetuate a particular fantasy that is deeply engrained within lay culture when in reality, these accessories are unnecessary (if not uncomfortable, unless made of merino wool perhaps). Images may also miscommunicate using gendered, xenophobic, or erroneous attribution (i.e. not all

[45] Response to information request from a reliable source in ADM(IM) D Cyber Ops, 19 May 2020.

[46] Fouchard, Steven. 1 November 2019. "Cyber Operations an Enjoyable Puzzle, says First Female", *Esprit de corps*, Canadian Military Magazine. Retrieved 12 May 2020: http://espritdecorps.ca/army-articles/cyber-operations-an-enjoyable-puzzle-says-first-female.

[47] Response to information request from a reliable source in ADM(IM) D Cyber Ops, 19 May 2020.

[48] Canada. Canadian Armed Forces. Careers, main webpage. Accessed 24 May 2020: https://forces.ca/en/careers.

‘hackers’ are malicious – some are ‘ethical hackers’).[49] While official government documents may not use these images, their prevalence elsewhere undoubtedly influences readers’ perceptions when encountering words like “hacker’ (present in official material) and absence of plausible alternatives.

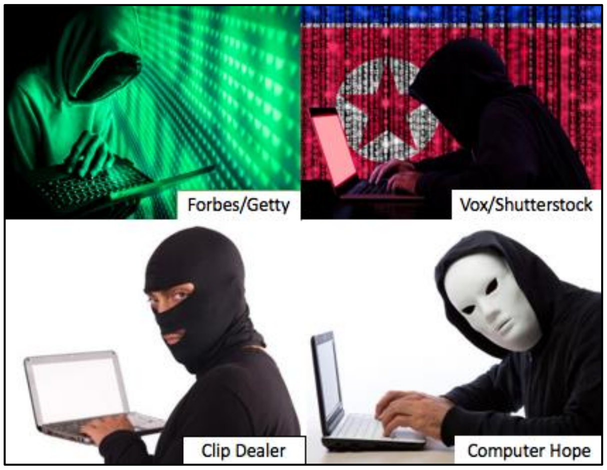


Image 3: Examples of ‘hackers’ drawn from news and stock photography webpages.

Technical VS Human Factors

In 2003, the Opte Project sought to create a static visualization for a portion of the internet – including routes and nodes – using multiple sources and tools.[50] Human factors, however, are often excluded from these depictions.

[49] Hess, Ken. 27 September 2011. “What is a Hacker?”, *ZDNet*, retrieved 24 May 2020: https://www.zdnet.com/article/what-is-a-hacker/.
[50] Lyon, Barrett. 2003. *The Opte Project*. Lyon Labs. Retrieved 24 May 2020: https://web.archive.org/web/20040824013519/http://www.opte.org/.

Image 4: An illustrated portion of the internet (left) compared to
use of mobile devices at home (top right) and workplace.
Sources (respectively): The Opte Project, Engadget, Carlo Allegri (*Reuters*).

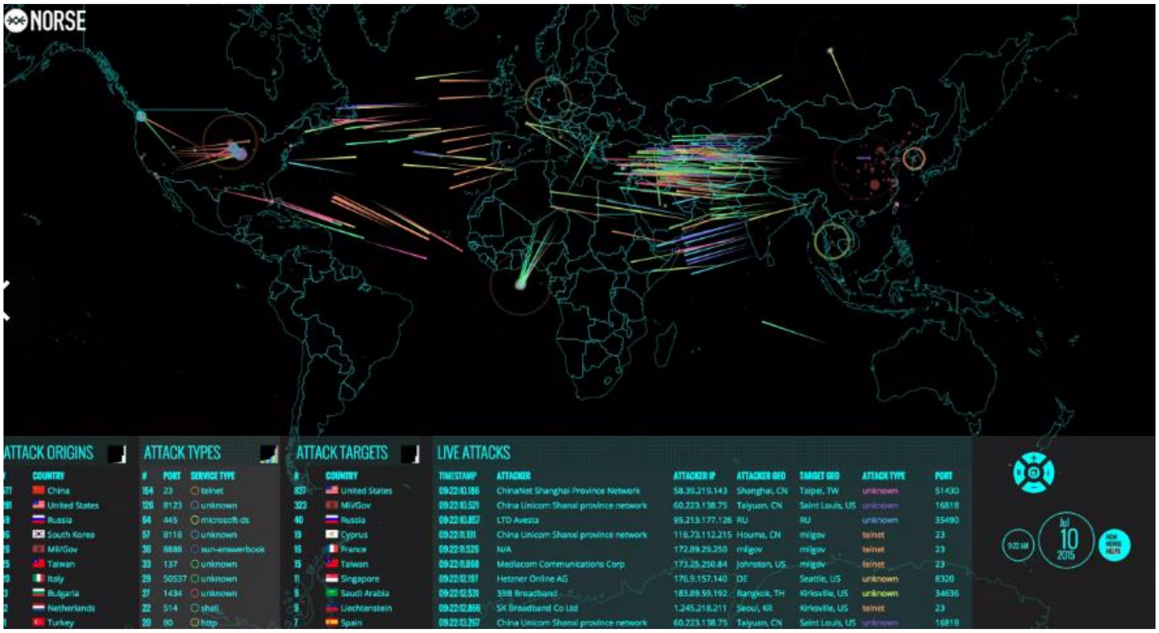
Limitations of 'Cyber' Threat Maps

Private companies such as FireEye,[51] Kaspersky,[52] and Norse[53] (among others) offer threat maps to visualize activity in cyberspace. While each of these services vary, they typically have a similar aesthetic: an overlay of bright colours representing transnational activity against a dark digital backdrop of Earth.

[51] FireEye: Cyber Threat Map. Accessed 24 May 2020: https://www.fireeye.com/cyber-map/threat-map.html.

[52] Kaspersky Cyberthreat Real-Time Map. Accessed 24 May 2020: https://cybermap.kaspersky.com/.

[53] Norse: Real-time Visibility into Global Attacks. Not functioning when accessed 24 May 2020: http://norsenet.com/.



ATTACK ORIGINS

	COUNTRY
77	China
81	United States
19	Russia
16	South Korea
26	Mil/Gov
25	Taiwan
19	Italy
3	Bulgaria
2	Netherlands
1	Turkey

ATTACK TYPES

#	PORT	SERVICE TYPE
154	23	○ telnet
126	8123	○ unknown
64	445	○ microsoft-ds
57	8118	○ unknown
36	8888	○ sun-answerbook
33	137	○ unknown
29	50537	○ unknown
27	1434	○ unknown
22	514	○ shell
20	80	○ http

ATTACK TARGETS

#	COUNTRY
837	United States
323	Mil/Gov
40	Russia
19	Cyprus
16	France
15	Taiwan
11	Singapore
9	Saudi Arabia
9	Liechtenstein
7	Spain

LIVE ATTACKS

TIMESTAMP	ATTACKER	ATTACKER IP	ATTACKER GEO	TARGET GEO	ATTACK TYPE	PORT
09:22:10.186	ChinaNet Shanghai Province Network	58.39.219.143	Shanghai, CN	Taipei, TW	unknown	51430
09:22:10.521	China Unicom Shanxi province network	60.223.138.75	Taiyuan, CN	Saint Louis, US	unknown	16818
09:22:10.857	LTD Avesta	95.213.177.126	RU	RU	unknown	35490
09:22:11.131	China Unicom Shanxi province network	118.73.112.215	Houma, CN	mil/gov	telnet	23
09:22:11.526	N/A	172.89.29.250	mil/gov	mil/gov	telnet	23
09:22:11.868	Mediacom Communications Corp	173.25.250.84	Johnston, US	mil/gov	telnet	23
09:22:12.197	Hetzner Online AG	176.9.157.140	DE	Seattle, US	unknown	8320
09:22:12.531	3BB Broadband	183.89.59.192	Bangkok, TH	Kirksville, US	unknown	34636
09:22:12.866	SK Broadband Co Ltd	1.245.218.211	Seoul, KR	Kirksville, US	telnet	23
09:22:13.267	China Unicom Shanxi province network	60.223.138.75	Taiyuan, CN	Saint Louis, US	unknown	16818

Image 5: Norse Live Attack Map. Source: *Newsweek*.[54]

Cyberspace is often conceptualized as 'borderless' yet divisions at the political, corporate, private, and individual-level exist in the form of national firewalls, state-funded censorship, or other forms of circuits and switches. Threat maps offer little value because they are devoid of context. Some offensive cyber operations, for example, leverage Command and Control (C2) infrastructure that forms a network of interconnected yet geographically dispersed endpoints. Such operations rely on multiple stages yet threat maps depict unidirectional activity that also conveys no information about the intent of the offensive cyber activity, significance of the compromise (if any), or meaningful measures (whether success or failure).

[54] Walker, Lauren. 12 July 2015. "Real-time Cyber Attack Map Shows Scope of Global Cyber War", *Newsweek*, retrieved 24 May 2020: https://www.newsweek.com/real-time-cyber-attack-map-shows-scope-global-cyber-war-352886.

Why Most Activity is Not an 'Attack'

Likely one of the strongest words in the English language, 'attack' often accompanies the word cyber; however, the majority of cyber-related incidents (including cyber-espionage and precursors such as reconnaissance, scanning, probing) are not considered attacks. Much progress remains to be seen for establishing 'norms' about the way states behave in cyberspace and how older laws, conventions, and norms such as the Law of Armed Conflict (LOAC) apply.

A website re-direct that impacted a CAF recruiting website (forces.ca) in 2016 offers a useful example. Visitors were automatically forwarded to a Chinese state-run website, according to media reporting that claimed the recruiting website was 'hacked'.[55] An initial examination revealed that the recruiting website was hosted externally by a service provider in the public sector.[56] The Public Safety Minister, acknowledging the event as "a serious matter", also noted the importance of not jumping to conclusions.[57]

Nomenclature and Taxonomy

Playful yet often unfamiliar words characterize threats in cyberspace such as phishing, malware (malicious software), ransomware, zero-days, Stuxnet, NotPetya, and WannaCry. Naming conventions for malware exist and classify it according to families and potential threats. Not too long ago, Public Safety in Ottawa maintained a giant database for malware analysis aptly named BeAVER (BEhavioural Analysis using

[55] Brewster, Murray, and John Paul Tasker. 17 November 2016. "Canadian Forces Recruiting Website Hacked", retrieved 24 May 2020: https://www.cbc.ca/news/politics/canadian-forces-website-hacked-1.3855719.

[56] *ibid*.

[57] *ibid*.

Virtualization and Experimental Research).[58] The imagination inevitably conjures images of the Containment Unit in *Ghostbusters* yet this Canadian example demonstrates there is room for creativity in cyberspace. Laymen, however well-intentioned, distill all unwelcome or inconvenient events as “hacks” or “attacks”. The use of these mental shortcuts is widespread. It is perhaps most akin to exasperated entomologists who overhear other people using the word ‘bugs’.

[58] Massicotte, Frederic, et al. December 2012. “Navigating and Visualizing the Malware Intelligence Space”, *Institute of Electrical and Electronics Engineers* (IEEE), retrieved 16 May 2020: https://ieeexplore.ieee.org/document/6375889/authors#authors.

CONCLUSION

This paper serves as a mechanism to explore language, imagery, and other non-technical factors associated with cyberspace. It reveals significant problems with the way we conceptualize and articulate the warfighting domain. These factors are as ubiquitous as cyberspace yet similarly obscure. The terms and metaphors commonly encountered, while sometimes playful, are not universal. They are frequently derived from specific historical and cultural contexts that are prone to romanticizing, politicizing, and misinterpreting.

Our increasingly interconnected world, while fostering innovation and unprecedented access to information, reveals a deepening reliance—if not dependence—on global telecommunications infrastructure for commerce, governance, and critical services. As society and militaries integrate technology, many of the challenges that plague cyberspace are not new. Yet our ability to describe nuanced threats remains relatively rudimental and inarticulate. These realities pose significant problems, particularly when faced with intersectional policies across government departments and agencies, between nation states, and competing priorities within the DND/CAF or GoC. The analysis, drawn from primary and secondary sources, also exemplifies how we face no greater 'wicked problem' than that of cyberspace. Despite its complexity, however, ample opportunity exists for improvement and collaborative solutions.

BIBLIOGRAPHY

Bateman, Sam. 2011. “Solving the “Wicked Problems” of Maritime Security: Are Regional Forums up to the Task?”, *Contemporary Southeast Asia*, Vol 33(1), 1-28.

Bégin, Daniel. May 2019. “More than just ones and zeros: Canadian cyber deterrence posture”, JCSP 45, retrieved 16 May 2020: https://www.cfc.forces.gc.ca/259/290/308/305/begin.pdf.

Brewster, Murray. 11 January 2018. “Navy Dropping ‘draconian’ Policy on Warship Wi-Fi, Admiral Says”, *CBC News*, retrieved 24 May 2020: https://www.cbc.ca/news/politics/navy-warship-wifi-1.4481346.

Brewster, Murray, and John Paul Tasker. 17 November 2016. “Canadian Forces Recruiting Website Hacked”, retrieved 24 May 2020: https://www.cbc.ca/news/politics/canadian-forces-website-hacked-1.3855719.

Canada. Canadian Armed Forces. Careers, main webpage. Accessed 24 May 2020: https://forces.ca/en/careers.

Canada. Department of National Defence, Canada First Defence Strategy (Ottawa, 2010), 1-22. Retrieved 22 May 2020: https://www.canada.ca/content/dam/dnd-mdn/migration/assets/FORCES_Internet/docs/en/about/CFDS-SDCD-eng.pdf.

Canada. Department of National Defence, CF Cyber Force Development: Director’s View, October 2012.

Canada. Department of National Defence, Integrated Capstone Concept (Ottawa: Chief of Force Development, 2009), 28–30.

Canada. Department of National Defence, Strong, Secure, Engaged: Canada’s Defence Policy (Ottawa, 2017), 1-113.

Canada. Public Safety Canada, Canada’s Cyber Security Strategy (2010). Retrieved 24 May 2020: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/archive-cbr-scrt-strtgy/archive-cbr-scrt-strtgy-eng.pdf.

Canada. Public Safety Canada, National Cyber Security Strategy (2018). Retrieved 24 May 2020: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf.

Chouinard-Prévost, R. 2017. “Cyber Capability Development: Considerations for Optimizing Organizational Form in the DND/CAF”, JCSP 43, retrieved 16 May 2020: https://www.cfc.forces.gc.ca/259/290/402/305/chouinard-prevost.pdf.

Corriveau, Guillaume. 2018. "Canada's Foray into Offensive Cyber: A Joint CAF-CSE Endeavour", JCSP 43, retrieved 22 May 2020: https://www.cfc.forces.gc.ca/259/290/402/305/corriveau.pdf.

Day, Malcolm. 2018. "Developing the CAF Cyber Capability: The Need to Integrate the Reserve", JCSP 43, retrieved 14 May 2020: https://www.cfc.forces.gc.ca/259/290/402/305/day.pdf.

Dvorkin, Corey Michael. Phone Interview, 23 May 2020. Mr. Dvorkin is Acting Policy Director, Cyber Security, Public Safety Canada.

Dias, R.F.J. 2016. 'The Institutional Cyber Gap Within the Canadian Armed Forces", JCSP 42, retrieved 12 May 2020: https://www.cfc.forces.gc.ca/259/290/318/192/dias.pdf.

FireEye: Cyber Threat Map. Accessed 24 May 2020: https://www.fireeye.com/cyber-map/threat-map.html.

Fouchard, Steven. 1 November 2019. "Cyber Operations an Enjoyable Puzzle, says First Female", *Esprit de corps*, Canadian Military Magazine. Retrieved 12 May 2020: http://espritdecorps.ca/army-articles/cyber-operations-an-enjoyable-puzzle-says-first-female.

Hess, Ken. 27 September 2011. "What is a Hacker?", *ZDNet*, retrieved 24 May 2020: https://www.zdnet.com/article/what-is-a-hacker/.

Hsu, Jeremy. 29 January 2018. "The Strava Heat Map and the End of Secrets", *Wired*, retrieved 24 May 2020: https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/.

Kaspersky Cyberthreat Real-Time Map. Accessed 24 May 2020: https://cybermap.kaspersky.com/.

Lanouette, J.M. 2016. "Naval Cyber Warfare Capability Requirement", JCSP 42, retrieved 12 May 2020: https://www.cfc.forces.gc.ca/259/290/318/192/lanouette.pdf.

Ling, Justin. 24 March 2016. "Man Who Sold F-35 Secrets to China Pleads Guilty", *Vice News*, retrieved 24 May 2020: https://www.vice.com/en_us/article/kz9xgn/man-who-sold-f-35-secrets-to-china-pleads-guilty.

Lyon, Barrett. 2003. *The Opte Project*. Lyon Labs. Retrieved 24 May 2020: https://web.archive.org/web/20040824013519/http://www.opte.org/.

Lyttle, R.J. 2016. "Due Online: Is Canadian Cyber Culture Secure?", JCSP 40, retrieved 12 May 2020: https://www.cfc.forces.gc.ca/259/290/301/305/lyttle.pdf.

Marshall, N.B. 2016. "Offensive Cyber in the Canadian Armed Forces: Opportunities from Bill C-51", JCSP 42, retrieved 12 May 2020: https://www.cfc.forces.gc.ca/259/290/318/192/marshalln.pdf.

Massicotte, Frederic, et al. December 2012. "Navigating and Visualizing the Malware Intelligence Space", *Institute of Electrical and Electronics Engineers* (IEEE), retrieved 16 May 2020: https://ieeexplore.ieee.org/document/6375889/authors#authors.

Mee, Paul, and Nico Brandenburg. 14 April 2020. "Digital Convenience Threatens Cybersecurity", *MIT Sloan Management Review,* retrieved 24 May 2020: https://sloanreview.mit.edu/article/digital-convenience-threatens-cybersecurity/.

National Collaborating Centre for Healthy Public Policy. June 2013, "Wicked Problems and Public Policy", retrieved 24 May 2020: http://www.ncchpp.ca/docs/WickedProblems_FactSheet_NCCHPP.pdf.

Norse: Real-time Visibility into Global Attacks. Not functioning when accessed 24 May 2020: http://norsenet.com/.

Organisation for Economic Cooperation and Development. 2019. Digital Security and Privacy. Retrieved 24 May 2020: https://www.oecd.org/going-digital/topics/digital-security-and-privacy/.

Orwell, George. 1968. "Politics and the English Language" in the collected essays, journalism, and letters of George Orwell, ed. Sonia Orwell and Ian Angos, vol 4(1), 127-40. New York: Harcourt, Brace, Javanovich. Retrieved 24 May 2020: https://faculty.washington.edu/rsoder/EDLPS579/HonorsOrwellPoliticsEnglishLanguage.pdf.

Palmer, Danny. 6 June 2019. "Don't let cybersecurity be driven by fear, warns NCSC chief", *ZDNet*, retrieved 23 May 2020: https://www.zdnet.com/article/dont-let-cyber-security-be-driven-by-fear-warns-ncsc-chief/.

Rittel, Horst W. and Melvin M. Webber. 1973. "Planning Problems are Wicked Problems" from "Dilemmas in a General Theory of Planning", *Policy Sciences*, 4, 155-69, retrieved 22 May 2020: https://cec.prodwebb.lu.se/sites/cec.prodwebb.lu.se/files/rittel_and_webber_1973_planning_problems_are_wicked_problems.pdf.

Rogin, Josh. 9 July 2012. "NSA Chief: Cybercrime constitutes the 'greatest transfer of wealth in history'", *Foreign Policy*, retrieved 24 May 2020: https://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/.

Singh, Abhijit. 27 August 2016. “India and the Scorpene Leak: Untangling the Knots”, *The Diplomat*, retrieved 24 May 2020: https://thediplomat.com/2016/08/india-and-the-scorpene-leak-untangling-the-knots/.

Skaburskis, Andrejs. June 2008. “The Origin of ‘Wicked Problems’”, Planning Theory and Practice, Vol 9(2), 227-280.

Smibert, Devon. 2019. “Building Cyber Operations in the Canadian Armed Forces: A Blueprint to Lay a Solid Foundation”, JCSP 42, retrieved 12 May 2020: https://www.cfc.forces.gc.ca/259/290/318/286/smibert.pdf.

Sterling, Bruce. 29 June 2011. “The Dropped Drive Hack”, *Wired*, retrieved 11 May 2020: https://www.wired.com/2011/06/the-dropped-drive-hack/.

Swanson, Ana, and Cecilia Kang. 20 January 2020. “Trumps China Deal Creates Collateral Damage for Tech Firms”, *The New York Times*, retrieved 24 May 2020: https://www.nytimes.com/2020/01/20/business/economy/trump-us-china-deal-micron-trade-war.html.

The Maple Leaf Defence Stories, “DND/CAF Welcomes First Cyber Operators”. 8 January 2018. Retrieved 16 May 2020: https://ml-fd.caf-fac.ca/en/2018/01/9092.

The Maple Leaf Defence Stories, “MGen Allen Speaks About Cyber at the Defence Women’s Advisory Organisation”. 29 January 2019. Retrieved 16 May 2020: https://ml-fd.caf-fac.ca/en/2019/01/24165.

Turner, J.T.D.S. 2016. “Buy Cyber-Secure: Improving Cybersecurity of Procured Combat Systems”, JCSP 42, retrieved 12 May 2020: https://www.cfc.forces.gc.ca/259/290/318/286/turner.pdf.

Unattributed. Email response from reliable source, ADM(IM) D Cyber Ops, 19 May 2020.

Walker, Lauren. 12 July 2015. “Real-time Cyber Attack Map Shows Scope of Global Cyber War”, *Newsweek*, retrieved 24 May 2020: https://www.newsweek.com/real-time-cyber-attack-map-shows-scope-global-cyber-war-352886.

Walkling, L.C. 2013. “Considerations: Canadian Forces’ Efforts in the Electromagnetic Spectrum and Cyber Operating Environment”, JCSP 39, retrieved 12 May 2020: https://www.cfc.forces.gc.ca/259/290/299/286/walkling.pdf.

Weston, Greg. 9 January 2013.”Fake Parts in Hercules Aircraft Called a Genuine Risk”, *CBC News*, retrieved 24 May 2020: https://www.cbc.ca/news/politics/fake-parts-in-hercules-aircraft-called-a-genuine-risk-1.1345862.

Yu, Howard. 2018. "Decentralized Cyber Forces: Cyber Functions at the Operational and Tactical Levels", JCSP 44, retrieved 16 May 2020: https://www.cfc.forces.gc.ca/259/290/405/305/yu.pdf.