National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

A 500-POUND BOMB DOWN A 100-MICRON FIBER: THE POTENTIAL TO USE OFFENSIVE CYBER OPERATIONS TO REPLACE COMBAT TROOPS

Maj N.B. Marshall

JCSP 42

Exercise *Solo Flight*

Disclaimer

PCEMI 42

Exercice *Solo Flight*

Avertissement

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES
JCSP 42 – PCEMI 42
2015 – 2016

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

A 500-POUND BOMB DOWN A 100-MICRON FIBER: THE POTENTIAL TO USE OFFENSIVE CYBER OPERATIONS TO REPLACE COMBAT TROOPS

Maj N.B. Marshall

Word Count: 4638

Compte de mots: 4638

INTRODUCTION

Militaries have been looking to leverage the cyber realm to gain military advantage ever since the Internet grew out of a United States military research project. Although killer robots out of *Terminator*[1] are still some years away, the ubiquitous connectivity used by friend and foe alike have given rise to many types of cyber operations. Shrouded in secrecy, militaries attempt to protect their own networks from adversaries and to better share information with friendly forces all while attempting to infiltrate adversary networks for intelligence gathering or attack. Slowly, the use of cyber for military offensive operations has developed and, although direct confirmation of specific capabilities and targets remains highly classified, evidence of the use of cyber attacks to support military operations has trickled down into more widely available media. The challenge has been to determine how this offensive cyber capability might be integrated with other kinetic and non-kinetic operations to act as a force multiplier or as a force in and of itself.

Canada's new Liberal Government signaled a sea-change of defence policy in 2015 with the proclamation that they would reverse the former government's aerial bombardment mission against the Islamic State and would focus more on peacekeeping.[2] Further, the Minister of Foreign Affairs suggested that future Canadian peace support operations would deploy only a few senior personnel and would not focus on large numbers of the rank and file, as seen in previous similar missions.[3] This suggests that although the current government wishes to support allied military operations, there is a

---

[1] Jonathan Mostow, *Terminator 3: Rise of the Machines*, 2003.
[2] *Canada's CF-18s Bomb ISIS Targets* (Toronto: Canadian Broadcasting Corporation, 2015).
[3] Mike Blanchfield, "Liberals Grapple with how to Return to a New Era of UN Peacekeeping," *The Canadian Press*, 2016.

desire to keep the numbers of deployed soldiers small and to reduce or eliminate combat operations. With the government's desire to reduce the number of troops deployed, would it be possible to leverage offensive cyber operations in the Canadian Armed Forces (CAF) as a way to contribute military force, while keeping its combat roles and deployment numbers to a minimum?

This paper posits that since cyber operations are inherently secretive, replacing combat elements with cyber elements does not meet the Canadian Government's strategic aims, regardless of operational or tactical effects.

In the first section, existing theories of cyber activities will be discussed, particularly as they apply to military operations. Next, the paper will explore the potential of cyber capabilities as an alternative to the deployment of combat forces, with a focus on why the Canadian Government would deploy combat forces and how the use of cyber forces may be preferred. Third is an examination of how cyber operations might generally fit into the overall design and planning of operations and specifically how offensive cyber dovetails with the targeting process. It shows that offensive cyber operations are best integrated into the joint targeting process to maximize their effects. The fourth section discusses how cyber operations might be applied to attack the Islamic State as a brief case study. These two sections show that the use of offensive cyber, both kinetic and non-kinetic, in Canada's participation in operations as a coalition partner, could reduce or replace its deployed combat elements. Finally, the efficacy for cyber operations as a replacement for combat forces is examined within the unique Canadian strategic context, particularly against the Islamic State. Here, the idea of secrecy of cyber operations is explored as a counter-weight to the attractiveness of using cyber operations as a combat force replacement from a policy perspective.

CYBER OPERATIONS

The role of cyber operations within a military context continues to be debated. Even the definitions of cyber are hard to find agreement on. The United States Department of Defense probably has the most robust and agreed-upon definition. Cyberspace operations, or "cyber" refers to "the employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid."[4] The definition specifically excludes capabilities like electronic warfare and psychological operations that "may cause effects in cyberspace [but] do not employ cyber capabilities."[5] Interestingly, then, cyber includes not only defence of, but also operation within computer networks.

Authors like Busbridge argue that cyber has its own domain within the military[6] and the North Atlantic Treaty Organization created its own cyber component on major exercises[7], however at a purely theoretical level, McGuffin clearly demonstrates that, since one physically operates through, instead of inside, cyberspace, cyber is not its own domain.[8] Although much hype has been generated about the possibilities of reality existing in a cyber virtual realm, this have been shown to be unrealistic now and for the future; people living in *The Matrix* remains in the domain of science fiction for military

---

[4] M Kunkel, "New Cyber Definition Excludes EW," *Journal of Electronic Defense*, sec. 31, 2008.
[5] Ibid.
[6] Richard J. Busbridge, *The 5th Dimension of Operations: A Case for Acknowledgement of a Separate Cyber Domain* (Toronto, ON: Canadian Forces College, 2015).
[7] Gordon Danylchuck, "Joint Command and Staff Program 42," 2016.
[8] W. C. McGuffin, *Soldiers of FORTRAN: Militarization of the 5th Dimension* (Toronto, ON: Canadian Forces College, 2013).

purposes.[9] Further Betz and Stevens expand on the practical limitations of cyber. Cyber operations are not a decisive mechanism in warfare.[10] Although they can contribute to military operations and may perhaps tip the scale in terms of victory or defeat, independent cyber operations cannot win battles. This inherent limitation can be compared to air power; where air power may be a critical element of a campaign, it has not been shown to be decisive without being part of the joint fight.[11] In fact, air power can be a useful metaphor for cyber operations, particularly since air power has a century of military thought behind it and cyber is relatively new. What air power does in the skies, cyber does in the virtuality of cyberspace. Air power can defend a nation's borders from incursion, can provide excellent intelligence on the adversary, and can attack both kinetically and non-kinetically. Cyber does all of this as well. Cyber operations, then, can been seen as a supporting element of a larger joint operation.

Cyber operations consist of three sub-types: defensive, intelligence gathering, and offensive. Defensive operations, termed computer network defence, ensure that the network is maintained against all threats, including deliberate attack by an adversary.[12] It also includes guarding essential elements of friendly information from disclosure to the enemy.[13] These operations, although linked to threats and risks, are ongoing constantly

---

[9] David LaGesse, *Taking a Walk in 'the Cloud'; More and More People are Moving their Lives Onto the Web. it's Not the Matrix, but Close*, Vol. 146 (Washington: U.S. News and World Report, L.P, 2009), 71.
[10] David Betz, Tim Stevens and International Institute for Strategic Studies, *Cyberspace and the State: Toward a Strategy for Cyber-Power*, Vol. no. 424 (New York: Routledge, for the International Institute for Strategic Studies, 2011), 128.
[11] Ibid, 131.
[12] Gajanan Dattatray Kurundkar, Quadri M N and Santosh D Khamitkar, "Attacks on Computer Network and Corresponding Security Measures," *International Journal of Advanced Research in Computer Science* 1, no. 4 (2010).
[13] Canada. Department of National Defence, Chief Defence Intelligence, *B-GJ-005-200/FP-001, CFJP 2.0 - Intelligence*, Canadian Forces Warfare Centre, 2011), 2A-1.

and are not linked to specific campaigns. Therefore, these pervasive defensive operations are not within the scope of this paper.

The second type of operation is computer network exploitation (CNE), which consists of using computer networks to gather intelligence.[14] In Canadian military doctrine, this is technically Communication Intelligence, or COMINT, a sub-category of Signals Intelligence or SIGINT.[15] This intelligence gathering can range from real-time targeting through cellular networks, to corporate-type espionage, to open-source analysis. For example, a significant amount of intelligence can be gleaned from the Islamic State's twitter followers who forgot to turn their geo-location feature off.[16] It is fair to assume that, based on leaks like Snowden's, classified intelligence gathering techniques would yield significantly better results.[17] Rid uses the term "espionage" to highlight this type of cyber operation in his succinct discussion on the types of cyber attacks saying, "espionage is an attempt to penetrate an adversarial system for purposes of extracting sensitive or protected information."[18]

The last type of cyber operation is the use of computer network attacks (CNA), which are operations to disrupt adversary networks.[19] These attacks can be simple denial of service (DOS) attacks that use multiple computers to simultaneously make requests of a network, overwhelming its capability to respond and making the system unavailable to

---

[14] F. J. Allen, "CN(EH?): A Recommendation for the CF to Adopt Computer Network Exploitation and Attack Capabilities," Canadian Forces College, 2002.
[15] Canada. Department of National Defence, Chief Defence Intelligence, *B-GJ-005-200/FP-001, CFJP 2.0 - Intelligence*.
[16] JM Berger and Jonathon Morgan, *The ISIS Twitter Census - Defining and Describing the Population of ISIS Supporters on Twitter,* The Brookings Institute, 2015.
[17] Susan Landau, "Highlights from Making Sense of Snowden, Part II: What's Significant in the NSA Revelations," *IEEE Security & Privacy* 12, no. 1 (2014), 62-64.
[18] Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (2012), 20.
[19] Jason Andress and Steve Winterfeld, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners* (Amsterdam: Elsevier, 2014), 181.

legitimate users. They can also be far more sophisticated like STUXNET, resulting in physical damage to Iranian nuclear enrichment facilities through the introduction of subtle errors in their machine control software.[20] Again, Rid classifies CNA as having two separate applications: sabotage and subversion. He defines sabotage as "a deliberate attempt to weaken or destroy an economic or military system,"[21] which could be used as a stand-alone operation or synchronized with other military operations. They are the most technically sophisticated type of cyber operations and typically "things are the prime targets, not humans."[22] Nevertheless, humans can be killed in such operations as a consequence of an attack on the material world. Subversion is the other type of CNA, defined as "the deliberate attempt to undermine the authority, the integrity, and the constitution of an established authority or order."[23] It seeks to "erod[e] *social* bonds, beliefs, and trust in the state and other collective entities."[24] Here, different from sabotage, which targets objects, subversion targets the human mind.[25] This type of cyber operation is the least technically sophisticated, although to be effective, gaining the required understanding of the target's psyche may be challenging.

In summary, doctrine frames cyber operations as computer network defence, exploitation and attack, but Rid's framework of subversion, espionage, and sabotage are more relevant for discussion on the efficacy of cyber operations. It provides a paradigm for cyber operations that can be easily linked to the type of military activities that have been a part of operations for centuries. Cyberspace merely provides another *way* to help

---

[20] Paulo Shakarian et al., *Introduction to Cyber-Warfare: A Multidisciplinary Approach* (US: Syngress Media Incorporated, 2013).
[21] Rid, *Cyber War Will Not Take Place*, 16.
[22] Ibid.
[23] Ibid, 22.
[24] Ibid.
[25] Ibid.

reach the desired *end*. Yet cyber forces are a distinct *mean*, and therefore can be compared to other, military elements, specifically combat forces. This helps to better understand the strategic and operational factors that inform the decision to contribute cyber or combat forces to a coalition mission.

CYBER FORCES VERSUS COMBAT FORCES

In order to better understand why a nation may employ cyber forces instead of combat forces, particularly in the Canadian context, it is important to better understand why Canada might contribute combat forces and consequently why cyber forces might look like a more attractive option.

Essentially, since Canada's decision to declare war on Nazi Germany in 1939, Canada has gone to war by choice. Although there may have been pressure exerted on it by its allies, Canada has entered into all expeditionary operations, not due to existential threats, but in pursuit of broader geopolitical aims.[26] Since the end of the Second World War, Canada's military policy has continued to be a blend of protecting national sovereignty, continental defence, and improving global peace and security through allies and partners.[27] Because Canadian sovereignty is guaranteed by the United States as part of their interest in continental defence and Canada's security is greatly enhanced by its geographic isolation from Africa and Eurasia, as Durand said in 1924, Canadians continue to "live in a fire-proof house far from inflammable materials."[28] Although terrorism and other security issues may have the potential to create changes in the

---

[26] Jean Daudelin et al., *Canada among Nations 2008: 100 Years of Canadian Foreign Policy* (Montréal: McGill-Queen's University Press, 2009), 19.
[27] Ibid 20.
[28] Robert Bothwell, "The Canadian Isolationist Tradition," *International Journal* 54, no. 1 (1999), 76.

Canadian way of life, these threats do not pose a risk to the elimination of it. Therefore, when Canada chooses to contribute combat forces to an operation, it does so for other reasons.

When Canada commits combat forces for expeditionary operations, it does so to demonstrate commitment.[29] This could be commitment to an alliance, country of interest, or external organization, such as NATO, the United States, or the United Nations; to an adversary such as Somali pirates, or Al-Qaeda or; to an internal audience, such as the large Ukrainian-Canadian population in key electoral districts.[30] In all of these cases, Canada sends forces overseas to demonstrate some sort of commitment to some group. Commitment is demonstrated practically by "waving the flag," to be seen to be a part of the operation of choice.[31] The Harper Conservative government opted to contribute six CF-18 fighter-bombers to bomb the Islamic State in 2015. This decision had a very minor effect on the ground tactically as the Canadian bombing sorties only made up a tiny fraction of the overall missions flown as part of the coalition.[32] However, what it did do, was demonstrate, to allies, foes, and to the Canadian population itself, Canada's resolve to defeat the Islamic.[33] Further, putting combat forces into an operational theatre demonstrates this commitment by putting the personnel of those forces at risk. The

---

[29] J. H. Vance, *Canada's Departure from the Classic Doctrine of Operational Art* (Toronto, Ont.: Canadian Forces College, 2004).

[30] Mark MacKinnon, "How Private Canadians are Aiding Kiev's War Effort; A Powerful Force in Ukraine's Battle with Russian-Backed Separatists, Canada's Ukrainian Diaspora Presses Ottawa to Give Aid to the Homeland while Privately Raising Funds and Providing Supplies to Troops. A Few have Even Taken Up Arms and Headed to the Front Lines. Mark MacKinnon Reports from Kiev," *Globe & Mail (*Toronto, Canada: 2015).

[31] Vance, *Canada's Departure from the Classic Doctrine of Operational Art*, 30.

[32] David Pugliese, "DND Gears for Shift in Mission; Iraq and Syria Canada Likely to Stop Bombing, Expand Training," *Edmonton Journal*, 2015.

[33] Scott Taylor, *Canada Gains Nothing from Bombing Iraq Or Training Kurds* (Ottawa, Ont: Hill Times Publishing, 2016), 7.

potential for spilling Canadian blood for the cause shows that the government is serious about doing something about the issue.

The use of cyber forces may be an attractive one to various nations, particularly Canada. If one suspends judgment about the efficacy of cyber forces to generate operational effects and assumes that cyber operations are equally effective to conventional kinetic operations, then it is possible to examine why Canada or anyone else may choose cyber over conventional forces. Generally, the commitment of cyber forces provides a military option that is less attributional, less risky, and at a lower cost, both human and financial.

Putting conventional forces in a theatre of operations, whether ground, naval, or air forces, makes it very clear that the contributing nation is involved in the conflict; to be effective, the forces have to be in the theatre of operations in order to conduct operations. However, cyber forces are not similarly limited. The internet is ubiquitous around the world and most unclassified military networks can be accessed directly through it.[34] Classified military networks tend to use civilian internet infrastructure but with encryption to help protect the information travelling on them.[35] Even the infamous Stuxnet virus was able to infiltrate a stand-alone network at a distance by using a mix of social engineering and technology. Therefore, cyber forces can create effects in an active theatre of operation with a minimal or no physical footprint in that theatre. This, in turn, provides a potential advantage. Since operators do not have to be physically present to create effects, it is possible to attack an adversary in a clandestine, or covert manner.[36] As a minimum, cyber operations generally provide the aggressive nation a shield of plausible

---

[34] Paul T. Mitchell, *Network Centric Warfare,* Routledge, 2013, 29.
[35] Ibid, 30.
[36] William J. Lynn III, *Defending a New Domain,* 2010.

deniability.[37] This, coupled with the fact that most cyber operations, even if the results were violent, would not be legally considered acts of war and cause for a conventional retaliation make the use of cyber forces an attractive option.[38]

Additionally, the risk to personnel is less when cyber forces engage an adversary. Since most, if not all, of those forces remain at home, they are almost invulnerable to conventional physical attack, with very sophisticated terrorism on home soil or cyber retaliation being the main threat. This also reduces the strategic and political risk, as a downed pilot engaged in air strikes, for example, could have massive strategic consequences. This risk is avoided by using cyber forces instead. Finally, the cost of employing cyber forces is less than conventional combat forces. The creation of defensive cyber capabilities can be expensive, but far less than other infrastructure or military projects.[39] Offensive cyber capabilities are quite inexpensive and once in place, the cost of employing cyber forces are far less than the costs of fuel, maintenance, ammunition, additional pay and benefits, and deployment and redeployment costs.[40] Overall, then, provided that cyber forces can provide similarly effective results to combat forces within a coalition, then they would be an attractive alternative to a country like Canada that will seek to contribute to allied or coalition operations.

CYBER OPERATIONS AND TARGETING

Should Canada opt to use cyber forces as part of its contribution to coalition operations, how cyber operations mesh with other operations becomes a critical issue.

---

[37] Peter Margulies, "Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility," *Melbourne Journal of International Law* 14, no. 2 (2013), 496-519.
[38] William J. Lynn III, *Defending a New Domain*.
[39] Christian Czosseck and Kenneth Geers, *The Virtual Battlefield: Perspectives on Cyber Warfare*, Vol. 3. (Amsterdam: Ios Press, 2009), 125.
[40] Ibid, 126.

The integration of cyber operations into the overall planning and conduct of military activities is still in its nascent stages. Although some theoretical work has been done on how this ought to take place, little practical advice currently exists. However, by looking at offensive cyber as a type of fires to be applied to the targeting process and applying Rid's classifications of types of cyber attacks, a more practical approach to integration can be developed.

Western militaries use a process that takes strategic direction, conceptualizes a vision of the problem and solution space, develops a plan based on an analysis of the various factors and then executes that plan. For Canada, this process is the Joint Operational Planning Process (OPP), enshrined in doctrine – *CFJP 5.0, The Canadian Forces Operational Planning Process*. The OPP seeks to answer four questions:

(1) Which conditions must be attained in order to achieve the strategic and operational objectives?
(2) What sequence of actions is most likely to produce these conditions?
(3) How should military resources be applied to produce these conditions?
(4) Are the associated risks acceptable?[41]

Although cyber is not mentioned in *CFP 5.0*, it would be fair to assume that cyber operations would be a means to produce the conditions discussed as part of the process. Canadian doctrine sees the integration of cyber with operations is as part of the targeting process. *CFJP 3-9, Targeting* sees targeting as a "part of a broader planning and evaluation process that enables commanders to continuously update and assess the

[41] Canada, Dept. of National Defence, *CFJP 5-0 the Canadian Forces Operational Planning Process (OPP)* (Ottawa: Issued on Authority of the Chief of the Defence Staff, 2008), 2-5.

progress of operations,"[42] nesting targeting firmly within the OPP. Targeting's "purpose is to plan, integrate and synchronize military means of action, into CAF joint operations to achieve the … desired end state."[43] This implies that cyber operations, as a means of action, would fit into the overall targeting process. The doctrine even discusses cyber targeting, but only provides a foundation of how the law of armed conflict might apply to cyber operations.[44] Overall, Canadian doctrine suggests that offensive cyber operations should be considered targeting, but stops short of providing any useful practical advice on how this might be achieved.

Western cyber doctrine is most advanced in the United States. Their Joint Operations doctrine, *JP 3-0*, suggests that cyberspace dominance should be sought, similar to air superiority, but does not provide any insight as to how this may be accomplished.[45] *JP 3-60, Joint Targeting* indicates that offensive cyber operations "should be coordinated and deconflicted with the joint targeting process."[46] So clearly, offensive cyber needs to be a part of targeting. More detail is contained in *JP 3-12, Cyberspace Operations* which suggests that offensive cyberspace operations are considered "cyberspace fires" that should "be included in the joint planning and execution processes from inception in order to facilitate synchronization and unity of effort."[47] These fires can either deny (by degrading, disrupting, or destroying the use of a target) or

---

[42] Canada, Dept. of National Defence, *CFJP 3-9 Targeting* (Ottawa: Issued on Authority of the Chief of the Defence Staff, 2014), 1-1.
[43] Ibid.
[44] Ibid, 2-11.
[45] United States, Joint Chiefs of Staff, *Joint Operations* (Washington, D.C: Joint Chiefs of Staff, 2010), V-47.
[46] United States, Joint Chiefs of Staff, *Joint Targeting* (Washington, DC: Joint Chiefs of Staff, 2007), III-2.
[47] United States, Joint Chiefs of Staff, *Cyberspace Operations* (Washington, D.C: Joint Chiefs of Staff, 2013), II-9.

manipulate the adversary's data or network.[48] Although *Cyberspace Operations,* more than any other doctrinal publication, attempts to come to grips with the practicalities of integrating cyber operations within targeting and the overall planning process, it instead takes a technical approach to defining the technical *means* that cyber operations can be used within targeting instead of the *ways*.

As discussed above, Rid's framework of subversion, espionage, and sabotage provides a needed bridge between theory and practice. By classifying offensive cyber operations as either providing a subversive or sabotaging *effect,* cyber fires becomes just another *means* of delivering two specific *ways*. Sabotage intends to damage things, either temporarily or permanently. Therefore, its effects are kinetic in nature, not unlike other, munitions-based fires. Conversely, subversion intends to influence the human mind in a way that supports the overall plan. Therefore, its effects are non-kinetic in nature, similar to other non-munitions-based fires like psychological or information operations.[49] In short, offensive cyber provides both a kinetic and non-kinetic capability that can create either physical destruction of things, or influence of peoples respectively and these capabilities should be fully nested into the larger targeting process. Thus, cyber operations are simply another *means* to "service" either high-value or high-payoff targets that are defined during the planning process and refined during the targeting process. In this way, as suggested in *JP 3-12*, offensive cyber becomes just another type of fires available to targeteers leading to its full integration.[50] Thus cyber operations can integrate with overall coalition operations with relative clarity and ease.

---

[48] Ibid, II-5.
[49] Canada, Dept. of National Defence, *CF Information Operations* (Ottawa: Issued on authority of the Chief of the Land Staff, Dept. of National Defence, 1998).
[50] United States, Joint Chiefs of Staff, *Cyberspace Operations*, viii.

CYBER OPERATIONS AGAINST THE ISLAMIC STATE

Today, Western militaries are focused on the goal of defeating the Islamic State militarily. In Iraq, they are using a combination of special forces working with Kurdish, Iraqi, and other groups and air strikes to slowly grind down the Islamic State. Similarly, in Syria, Russian and, to a lesser extent, Western militaries are doing the same.[51] Should a country like Canada wish to contribute offensive cyber, would it be effective against the Islamic State in the "war du jour?" Likely, these cyber operations would be a superb tool for bringing about the defeat of the Islamic State.

If the power of the Islamic State is looked at through a lens of the DIME model and its elements of diplomatic, information, military, and economic power are examined, it is clear that their power rests chiefly within the information domain.[52] Their narrative of social and religious extremism provides a great deal of information power and the messaging is expertly disseminated using social media, unlike any terrorist organization has done before, synchronizing their messaging and their means of transmission. Nevertheless, it is the hardline stance of the Islamic State that detracts from the other elements of power. Its inability to compromise forces it to shun any accepted diplomatic processes, limiting diplomatic power. Its need to hold ground and fight conventionally without air power or logistics has led to recent military reversals, and its need to govern populations requires far more money than the reliance on pillage and black-market oil sales has produced.[53] Overall, their power resides in their narrative – that the Islamic State is uncompromising and incorruptible and that despite the challenges from the West, they

---

[51] "Who are the Russians Bombing in Syria and Why?" *Telegraph.Co.Uk*, 2015.
[52] Neil Marshall, "Just Give ISIS some Rope: The Coming Self-Destruction of the Islamic State," Canadian Forces College, 2015, 9.
[53] Ibid, 14.

are winning.[54] To defeat the Islamic State, therefore, is to defeat *the idea of the Islamic State*.[55] Cyber operations can be uniquely suited for doing exactly that.

To defeat the idea of the Islamic State, offensive cyber can be applied to both subvert the idea itself and to sabotage the means of transmission of their ideas. VICE News released a video based on footage of Islamic State fighters battling the Kurdish Peshmerga.[56] This short video, purportedly shot from a headcam of an Islamic State fighter in early 2016 outside of Mosul shows his detachment to be disorganized and comically inept. They are burnt by hot casings and injured by the back blast of their own weapons before their vehicle is disabled and the driver killed by the Peshmerga. Finally, after a chaotic dismount, the cameraman is shot and later dies. As VICE News states, "unlike Islamic State propaganda, which often presents sweeping battlefield victories, the footage shows the fighters in disarray."[57] This video and others like it can be extremely useful in discrediting and subverting the narrative of purity and victory of the Islamic State. Further, although there is no evidence to the contrary, this video may not be authentic. Therefore, instead of waiting for unflattering videos to appear, why not produce them? Once filmed in secret, cyber operations could then seed them into the Islamic State's or supporters' video feeds, ensuring that they are captured by media prior to them being discovered and deleted by the account administrators. Videos could focus on "members" of the Islamic State losing, bumbling, dying and acting un-devout. This would cast doubt on the existing narrative and would force the Islamic State to defend

---

[54] Ibid, 18.
[55] Graeme Wood, *What ISIS really Wants*, Vol. 315 (Boston: Atlantic Media, Inc, 2015), 78.
[56] *What its really Like to Fight for the Islamic State*, directed by VICE News, 2016.
[57] Ibid.

which videos were legitimate and which were not, again reducing their prestige and power.

Sporadic cyber sabotage operations have already been conducted to remove some Twitter accounts supporting the Islamic State,[58] but a broader, more concerted effort is needed. The goal would be to gain the initiative and to force the Islamic State and the Cyber Caliphate, its electronic support arm, onto the defensive. Through account hacking, social engineering, and denial of service attacks, offensive cyber operations could require the Islamic State to have to fight in cyberspace to get their message out.[59] This will help disconnect the message from its intended audience and push it further away from the mainstream media. In this way, the combination of subversion and sabotage could replace and confuse the Islamic States' narrative, their chief source of power, and force them to defend their networks and information, which would support the defeat of the Islamic State. This could be a military force contribution for Canada.

CYBER OPERATIONS AS AN ECONOMY OF FORCE

Clearly the use of cyber forces could be an attractive alternative to combat forces for Canada as it tries to limit its deployed forces and its combat roles. However, generally, and specifically in Iraq and Syria, this would not meet Canada's strategic aims.

In Iraq, Canada withdrew its fighter-bombers from the coalition mission to defeat the Islamic State as part of its shift towards peacekeeping. It remains, however,

---

[58] Berger and Morgan, *The ISIS Twitter Census - Defining and Describing the Population of ISIS Supporters on Twitter*.

[59] Aaron Brown, "ISIS Fights Back Against Anonymous, Tells Followers to use Self-Destructing Message App," *Express (Online)*, 2015.

committed to the defeat of the Islamic State.[60] Therefore, employing cyber forces could be a low risk contribution to the fight. As discussed above, cyber forces could play a significant role in defeating the Islamic State and few, if any, military personnel would have to deploy into theatre. In fact, Lynn uses cyber power as an analogue of air power, so swapping Canadian bombers for Canadian cyber forces makes intuitive sense: both can attack to disrupt, deny, or destroy; both can provide non-kinetic effects; and both cannot take and hold ground.[61] Air power is still required within the coalition, but Canada could contribute combat power through cyber, in support of the other elements of the overall mission. Therefore, extrapolating to allied or coalition warfare in general, Canada could provide cyber forces, mostly in Canada, as an economy of force operation while still contributing to the alliance or coalition. But should it?

Should Canada decide to use cyber forces in lieu of combat forces as part of its contribution to a coalition, it would be constrained by the characteristics of cyber targeting. First, developing specific targeting capabilities takes time and is often built around specific characteristics of the target.[62] Because of this, cyber targeting is often not tactically flexible. Unlike bombing the Islamic State, which often involves attacking targets of opportunity, cyber attacks need to be planned and coordinated far in advance.[63] Second, cyber targeting can only be effective if the adversary relies on the use of information networks for critical activities. Arguably, this is the case with the Islamic State because of its reliance on social media to leverage its information power, but this may not always be the case with other adversaries. Finally, secrecy is critical to protecting

---

[60] *Canada's CF-18s Bomb ISIS Targets*.
[61] William J. Lynn III, *Defending a New Domain*.
[62] Andress and Winterfeld, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, 184.
[63] Ibid, 191.

capabilities, attribution, and technical methods of attack.[64] The best cyber attack is one where the adversary does not even realize that it is being attacked. This limitation, however, is the main weakness in the use of cyber forces to replace combat forces.

Because of Canada's unique geo-political position, it can choose its expeditionary operations. As discussed earlier, the key reason for Canada to send combat forces overseas is to demonstrate commitment both internally and externally. Putting forces in theatre and risking Canadian personnel shows Canada is deeply concerned and supportive to the mission. However, since cyber forces need to operate in secret and do not have a significant deployed footprint, Canada would not be in a position to use the allocation of cyber forces to demonstrate commitment. Therefore, despite the potential operational effect that cyber forces may generate for the coalition, the Government of Canada would not meet its strategic aims because their contribution would not be seen or understood internally or externally. Using cyber forces in lieu of combat forces is not a good strategy for Canada.

CONCLUSION

How to best leverage cyber operations remains an elusive problem. The use of cyber to support military operations has been much contemplated and has been the topic of many articles and books. Yet there still remains little practical guidance on how to integrate cyber into military planning and execution. Computer Network Defence is needed to ensure the availability and reliability of friendly networks. Computer Network Exploitation is a critical intelligence tool. Computer Network Attack forms the basis of cyber fires that need to be integrated into the overall targeting process. Perhaps the best

[64] Ibid, 176.

way to classify and align offensive cyber operations is to separate them into the kinetic, sabotage capability and the non-kinetic, subversive capability.

Offensive cyber operations, like air power, cannot defeat an adversary alone. However, it can be used in conjunction with other joint forces as a force multiplier. Because of the small deployed footprint of cyber forces and the low physical and strategic risks involved with cyber operations, employing cyber forces in lieu of combat forces may be an attractive alternative. However, for a contributing country like Canada that relies on its deployment of forces to demonstrate commitment and resolve, the secrecy required of cyber operations does not make this a good strategic choice.

Regardless of the advantages of employing cyber forces, it is the sharing of risks within the coalition that garners respect both at home and abroad. In the end, nothing shows that you care like boots on the ground.

BIBLIOGRAPHY

Aaron Brown. "ISIS Fights BACK Against Anonymous, Tells Followers to use Self-Destructing Message App." *Express (Online)*,2015.

Allen, F. J., Canadian Forces College, and Collège des Forces canadiennes. "CN(EH?): A Recommendation for the CF to Adopt Computer Network Exploitation and Attack Capabilities."Canadian Forces College, 2002.

Andress, Jason and Steve Winterfeld. *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. Amsterdam: Elsevier, 2014.

Berger, JM and Jonathon Morgan. *The ISIS Twitter Census - Defining and Describing the Population of ISIS Supporters on Twitter*: The Brookings Institute, 2015.

Betz, David, Tim Stevens, and International Institute for Strategic Studies. *Cyberspace and the State: Toward a Strategy for Cyber-Power*. Vol. no.424. New York: Routledge, for the International Institute for Strategic Studies, 2011.

Blanchfield, Mike. "Liberals Grapple with how to Return to a New Era of UN Peacekeeping." *The Canadian Press,* 2016.

Bothwell, Robert. "The Canadian Isolationist Tradition." *International Journal* 54, no. 1 (1999): 76.

Busbridge, Richard J. and Canadian Forces College. *The 5th Dimension of Operations: A Case for Acknowledgement of a Separate Cyber Domain*. Toronto, Ont: Canadian Forces College, 2015.

Canada. Department of National Defence, Chief Defence Intelligence. *B-GJ-005-200/FP-001, CFJP 2.0 - Intelligence* Canadian Forces Warfare Cenre, 2011.

Canada. Dept. of National Defence. *CF Information Operations*. Ottawa: Issued on authority of the Chief of the Land Staff, Dept. of National Defence, 1998.

———. . *CFJP 3-9 Targeting*. Ottawa: Issued on Authority of the Chief of the Defence Staff, 2014.

———. . *CFJP 5-0 the Canadian Forces Operational Planning Process (OPP)*. Ottawa: Issued on Authority of the Chief of the Defence Staff, 2008.

Canada's CF-18s Bomb ISIS Targets. Toronto: Canadian Broadcasting Corporation, 2015a.

Czosseck, Christian and Kenneth Geers. *The Virtual Battlefield: Perspectives on Cyber Warfare*. Vol. 3. Amsterdam: Ios Press, 2009.

Danylchuck, Gordon. "Joint Command and Staff Program 42." 2016.

Daudelin, Jean, Robert Bothwell, Centre for International Governance Innovation, and Norman Paterson School of International Affairs. *Canada among Nations 2008: 100 Years of Canadian Foreign Policy*. Montréal: McGill-Queen's University Press, 2009.

Kunkel, M. "NEW CYBER DEFINITION EXCLUDES EW." *Journal of Electronic Defense*, 2008, sec. 31.

Kurundkar, Gajanan Dattatray, M N Quadri, and Santosh D Khamitkar. "Attacks on Computer Network and Corresponding Security Measures." *International Journal of Advanced Research in Computer Science* 1, no. 4 (2010).

LaGesse, David. *Taking a Walk in 'the Cloud'; More and More People are Moving their Lives Onto the Web. it's Not the Matrix, but Close*. Vol. 146. Washington: U.S. News and World Report, L.P, 2009.

Landau, Susan. "Highlights from Making Sense of Snowden, Part II: What's Significant in the NSA Revelations." *IEEE Security & Privacy* 12, no. 1 (2014): 62-64.

Lynn, William J. III. *Defending a New Domain.* 2010.

MacKinnon, Mark. "How Private Canadians are Aiding Kiev's War Effort; A Powerful Force in Ukraine's Battle with Russian-Backed Separatists, Canada's Ukrainian Diaspora Presses Ottawa to Give Aid to the Homeland while Privately Raising Funds and Providing Supplies to Troops. A Few have Even Taken Up Arms and Headed to the Front Lines. Mark MacKinnon Reports from Kiev." *Globe & Mail (Toronto, Canada)*,2015.

Margulies, Peter. "Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility." *Melbourne Journal of International Law* 14, no. 2 (2013): 496-519.

Marshall, Neil. "Just Give ISIS some Rope: The Coming Self-Destruction of the Islamic State." Canadian Forces College, 2015.

McGuffin, W. C. "Soldiers of FORTRAN: Militarization of the 5th Dimension." Canadian Forces College, 2013.

Mitchell, Paul T. *Network Centric Warfare.* Routledge, 2013.

Mostow, Jonathan. *Terminator 3: Rise of the Machines*, 2003.

Pugliese, David. "DND Gears for Shift in Mission; Iraq and Syria Canada Likely to Stop Bombing, Expand Training." *Edmonton Journal*,2015.

Rid, Thomas. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35, no. 1 (2012): 5-32.

Shakarian, Paulo, Jana Shakarian, and Andrew Ruef. *Introduction to Cyber-Warfare: A Multidisciplinary Approach*. US: Syngress Media Incorporated, 2013.

Taylor, Scott. *Canada Gains Nothing from Bombing Iraq Or Training Kurds*. Ottawa, Ont: Hill Times Publishing, 2016.

United States. Joint Chiefs of Staff. *Cyberspace Operations*. Washington, D.C: Joint Chiefs of Staff, 2013.

———. . *Joint Operations*. Washington, D.C: Joint Chiefs of Staff, 2010.

———. . *Joint Targeting*. Washington, DC: Joint Chiefs of Staff, 2007.

Vance, J. H. *Canada's Departure from the Classic Doctrine of Operational Art*. Toronto, Ont.: Canadian Forces College, 2004.

What its really Like to Fight for the Islamic State. Directed by VICE News. 2016.

"Who are the Russians Bombing in Syria and Why?" *Telegraph.Co.Uk,* 2015.

Wood, Graeme. *What ISIS really Wants*. Vol. 315. Boston: Atlantic Media, Inc, 2015.