National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

CYBER-ENABLED INFLUENCE WARFARE

Lieutenant-Commander Robin Moll

JCSP 46

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 46

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.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES

JCSP 46 – PCEMI 46

2019 – 2020

SOLO FLIGHT

CYBER-ENABLED INFLUENCE WARFARE

By Lieutenant-Commander Robin Moll

Word Count: 4,756

Nombre de mots : 4.756

CYBER-ENABLED INFLUENCE WARFARE

INTRODUCTION

The idea of operations in the "information domain" is not new or novel, but has received much attention in recent years in Canada, particularly with regard to the concept of influence warfare (IW) when enabled by the cyber domain. Contemporary examples that have brought these discussions to the forefront include the information campaign carried out by the Russian Federation (RF) in support of the annexation of Crimea,[1] as well as the radicalization campaign conducted by the Islamic State of Iraq and the Levant (ISIL) to recruit fighters and sympathisers.[2] IW, in this context is referred to as information or psychological operations (PSYOPS) within the Canadian Armed Forces (CAF). It is defined as "planned activities using methods of communication and other means directed at approved audiences in order to influence perceptions, attitudes and behaviour, affecting the achievement of political and military objectives."[3]

This paper argues that notwithstanding the recognition of the importance of cyber-enabled IW within Canada's Defence Policy,[4] Canada remains for the most part, vulnerable to it and is particularly weak in its application as compared to those who specialize in it. This paper is sub-divided into five sections. The first provides a brief

---

[1] Neil MacFarquhar, "A Powerful Russian Weapon: The Spread of False Stories," *The New York Times*, August 28, 2016, sec. World, https://www.nytimes.com/2016/08/29/world/europe/russia-sweden-disinformation.html.

[2] "Inside the Surreal World of the Islamic State's Propaganda Machine - The Washington Post," accessed April 13, 2020, https://www.washingtonpost.com/world/national-security/inside-the-islamic-states-propaganda-machine/2015/11/20/051e997a-8ce6-11e5-acff-673ae92ddd2b_story.html.

[3] "NATO Glossary of Terms and Definitions (English and French)," AAP 6, 6 (January 1, 2019): 129, https://nso.nato.int/nso/ZPUBLIC/_BRANCHINFO/TERMINOLOGY_PUBLIC/NON-CLASSIFIED NATO GLOSSARIES/AAP-6.PDF.

[4] Canada and Department of National Defence, *Strong, Secure, Engaged - Canada's Defence Policy.*, 2017, 41,53,66,68,69, http://epe.lac-bac.gc.ca/100/201/301/weekly_acquisitions_list-ef/2017/17-23/publications.gc.ca/collections/collection_2017/mdn-dnd/D2-386-2017-eng.pdf.

overview of the current state of affairs with respect to IW in the CAF context. The second section seeks to establish an understanding of some of the different elements of IW and raise awareness of issues related to the lack of a consistent taxonomy. The next section elaborates on the theoretical basis for IW and illustrates how it can be used to achieve objectives. The following section distinguishes the characteristics of modern cyber-enabled IW and discusses how traditional IW tactics are amplified as a result of these inherent characteristics. The final section discusses the resulting threats and opportunities for Canada's advancement with respect to cyber-enabled IW.

OVERVIEW – THE CAF AND IW

Updated in 2011, CAF influence activity techniques, tactics and procedures (TTPs) currently limit PSYSOPs to traditional activities such as the dissemination of physical media (such as leaflets, pamphlets, posters), face to face communications and loudspeaker operations.[5] While these operations continue to have value in conflict, and in particular peace support operations in countries with limited literacy and Internet connectivity, the TTPs do not reflect a keeping of pace with the art of IW. In particular, there has been no attempt to adapt, integrate and defend against the significant advances in IW that have been made possible by the opportunities afforded by the availability of the global Internet and the rise of social media as a platform. This absence of development exists for a variety of reasons, not the least of which is a lack of clear authorities and responsibilities denoting what the CAFs role is with respect to IW, what

[5] Department of National Defence Canada, *B-GL-353-002-FP-001, Psychological Operations Tactics, Techniques and Procedures*, Psychological Operations (Kingston, ON: Chief of Land Staff, 2011), chap. 3.

the role of the other agencies within the National Security apparatus should be, and where those roles might meet.

Canada's defence policy, titled Strong, Secure, Engaged (SSE), recognizes that state-sponsored influence activities conducted by adversaries can pose challenges because they are difficult to detect, can take place below the threshold of war, and their attribution is problematic.[6] While this speaks directly to Canada's need to learn to detect and attribute IW better, it also speaks to a potential opportunity for capability development in this warfare area. To this end and recognizing the gap, SSE directs the development of military-specific information operations capabilities able to target, exploit, influence and attack in support of military operations,[7] but how this will translate in terms of CAFs mandate remains to be understood.

Within our existing national security construct, CAF does not engage offensively (below the threshold of war or otherwise) unless in a declared conflict. What role should CAF then have in developing IW forces capable of achieving political and military objectives against non-military targets and non-combatants? Acknowledging this gap to a certain extent, SSE directs that the Defence Team must also "examine its capabilities to understand and operate in the information environment, in support of the conduct of information and influence operations."[8] While all this suggests an interest in further force development activities concerning IW within CAF, it also reveals how little is currently known about this space. While SSE is explicit on CAFs need to work cooperatively with

---

[6] Canada and Department of National Defence, *Strong, Secure, Engaged - Canada's Defence Policy.*, 53.

[7] Ibid., 41.

[8] Ibid., 66.

the Communications Security Establishment, Global Affairs Canada and Public Safety on the development and execution of cyber warfare,[9] it neglects to recognize IW in the same vein, which may be a further indication of the current lack of understanding of how to define the problem space.

TAXONOMY (OR LACK THEREOF)

One of the significant challenges related to advancing IW is defining the space adequately and coming to a common understanding of what it is and where it fits within Canada's national security framework. The purpose of this section is to raise awareness on some of the issues related to this challenge and establish a basic understanding of the different aspects of IW in order to inform the subsequent discussion.

One of the first issues relates to understanding the warfare domain in which IW occurs. One might intuit that IW happens in the Information Domain, but the class of JCSP 46 may be surprised to learn that the term "Information Domain," despite its relatively frequent use,[10] does not exist within our Information Operations doctrine.[11] Furthermore, there is also no North Atlantic Treaty Organization (NATO) agreed-upon definition for the Information Domain,[12] nor is there a definition for it within the United States Joint Doctrine on Information Operations.[13] The term *information environment* is found instead in various related references, but even among close allies, including NATO

---

[9] Ibid., 72.

[10] Chatham House Rules prevent explicit references; however the author can attest that the term has been used by several GOFOs during the academic year and at times in conflicting senses.

[11] Department of National Defence Canada, *Canadian Forces Joint Publication Information Operations*, 1st ed., vol. 3–10, Canadian Forces Joint Publication (Ottawa, ON: Canadian Joint Operations Command, 2015), http://armyapp.forces.gc.ca/SOH/SOH_Content/CFJP 3-10 (2015).pdf.

[12] "NATO Glossary of Terms and Definitions (English and French)."

[13] Joint Chiefs of Staff United States, *Joint Doctrine for Information Operations*, vol. 3–13 (Washington, DC: The Joint Cheifs of Staff, 2014), https://www.hsdl.org/?view&did=759867.

and ABCA (American, British Canadian, Australian) publications,[14] as well as US and Canadian doctrinal publications, the definitions are not entirely consistent. For example, the NATO Information Operations Reference book takes a somewhat technology-centric, cyberspace view. It defines the information environment as "the virtual and physical space in which information is received, processed and conveyed."[15] Conversely, the US Joint doctrine describes the information environment as instead consisting of three interrelated dimensions: physical, informational and cognitive.[16] To make matters more confusing, the Canadian doctrinal definition awkwardly combines elements of both definitions, but changes the US reference from three dimensions to three *domains* and labels them physical, virtual and cognitive instead.[17]

While concerns over these sorts of small differences may seem overly pedantic, I would argue the contrary. As a result of multiple existing definitions and nuances associated with terms in the information operations space (including overlap and confusion with cyber operations), it has become very unclear whose role it is to develop what capability within the CAF force structure and within the more general national security apparatus. Within this paper, when referring to IW, the intended usage is specific to warfare vis-à-vis the cognitive domain of the information environment, which equates

---

[14] ABCA Armies, *Influence Activities Handbook*, vol. 374, ABCA Publication, 2013, 1–4, https://bib.cfc.forces.gc.ca/CFCLearn/mod/resource/view.php?id=2078.

[15] North Atlantic Treaty Organization, *NATO Bi-SC Information Operations Reference Book* (NATO Bi-Strategic Command, 2010), 9, https://bib.cfc.forces.gc.ca/CFCLearn/pluginfile.php/6678/mod_folder/content/0/NATO Bi-SC Information Operations Reference Book.

[16] United States, *Joint Doctrine for Information Operations*, 3–13:19.

[17] Canada, *Canadian Forces Joint Publication Information Operations*, 3–10:1–1. To ensure a complete lack of conformity, the descriptions of domains and dimensions do not align. Elements of the "physical dimension" are found within the "virtual domain," and elements of the information dimension are found in the description of the cognitive domain.

to the existing CAF definition for PSYOPS presented earlier.[18] The focus of IW is on influencing human will, human understanding and a human's ability to make decisions.[19] In achieving these ends, there are three main categories of IW activities: propaganda, chaos-producing and leaks.[20]

Propaganda activities aim to propagate a narrative that will influence the opinions, attitudes and emotions of a target audience. These activities come in three forms: black, white and grey. Black propaganda is a narrative disseminated to look as though it is coming from a source other than the originator. In contrast, grey propaganda has no source disclosed (it could be anonymous or an unaccredited source). White propaganda is disseminated openly with clear attribution and acknowledgement by its originator.[21] For chaos-producing IW, rather than propagating one specific narrative, the aim is to disrupt and sow confusion and doubt through disinformation and information flooding. For example, an adversary may disseminate a mass of mutually inconsistent messages to provide alternative narratives to an event, ultimately concealing the truth, or diminishing the conviction in which a target audience believes the truthful narrative.[22] The last category of IW, "leaks," are differentiated from the other forms of IW because they involve the dissemination of information that is entirely or mostly true regarding a subject to which the population is not ordinarily privileged. This type of activity can

[18] Perhaps related to the current absence of unified taxonomy, the term PSYOPS has seemingly fallen out of favor due to a perceived negative ethical connotation, but remains unambiguously defined within Canadian and Allied publications and is most tightly aligned with the concept of influence warfare within the context discussed in this paper.

[19] Canada, *Canadian Forces Joint Publication Information Operations*, 3–10:1–5.

[20] Herbert Lin and Jaclyn Kerr, "On Cyber-Enabled Information Warfare and Information Operations," May 2019, 10, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3015680.

[21] Department of National Defence Canada, *B-GJ-005-313/FP-001 Joint Doctrine Manual*, Psychological Operations (Kingston: Chief of Defence Staff, 2004), 109.

[22] Lin and Kerr, "On Cyber-Enabled Information Warfare and Information Operations," 11–12.

serve to discredit or distract an adversary or influence the beliefs of populations impacted by the leaks in a manner that is favourable to the originator. The impact can be particularly useful if selected disinformation is credibly inserted into an otherwise accurate leak in order to achieve a specific effect.[23]

While none of this represents warfare in the Clausewitzian sense of "an act of violence to compel an opponent," it very much carries with it the theme of "politics by other means." As a result, and primarily due to the absence of direct violence, IW is generally considered to take place in the "grey zone" below the threshold of war. As such, there is little risk of an opponent responding to IW with military force.[24] This provides additional options for a nation or actor when it is desired to achieve an effect while remaining under the threshold of armed conflict. Seizing on this aspect, some nations such as the RF for example, embrace IW within their military doctrine, recognizing that "information confrontation" activities should take place in advance of *any* military conflict in order to achieve political goals without the use of force. [25] In the RF's case, the doctrine explicitly states that in the event military intervention is required, information confrontation activities should be conducted "in the interests of creating a favourable reaction of the world community to the use of military force."[26]

Currently, Canada's use of IW is limited to public relations at the strategic level and supporting conventional forces at the tactical level using traditional means such as

---

[23] Ibid., 12.
[24] Ibid., 5.
[25] Administration of the President of Russia, "Военная доктрина Российской Федерации [Military Doctrine of the Russian Federation]," trans. Google Inc., *Президент России*, February 5, 2010, para. 13, http://kremlin.ru/supplement/461.
[26] Ibid.

loudspeaker, leaflets and face-to-face communications. Notwithstanding, Moscow's successful employment of IW across the spectrum of operations and specifically in advance of (or in lieu of) the use of traditional forces suggests a potential opportunity for Canada to seize upon and develop further. Sun Tzu said: "The supreme art of war is to subdue the enemy without fighting." Given the RF's recognized proficiency in this domain, Canada would benefit from looking more closely at the RF doctrine when considering how to better conduct and integrate IW activities.

HUMAN VULNERABILITY – THE BASIS FOR IW

This section seeks to provide an overview of how IW works and why it is effective. Before moving further, it is also important to understand the terminology used to describe and evaluate the characteristics of potential targets. Within the information environment, targets are evaluated in terms of their *receptivity*, *susceptibility* and *vulnerability* to IW. Receptivity speaks to a target's psychological and technical ability to receive messages in any particular format (literacy, availability of electronic communication devices, use/penetration of social media). Susceptibility is related to a target's culture, attitude and values and speaks to their areas of interest and those issues that would attract their attention. Finally, vulnerability speaks to those issues, anxieties and fears that directly affect cognition and emotion of the targets and can be exploited by IW activities to create desired effects.[27]

IW targets perceptions with a view to increasing the likelihood that a target audience will make choices that are favourable to the originator. This is accomplished by

[27] Canada, *Canadian Forces Joint Publication Information Operations*, 3–10:4B – 2.

attacking knowledge, truth, and confidence and by degrading an adversary's decision-making ability "by injecting fear, anger, anxiety, uncertainty, and doubt."[28] It is also seen in a form of IW known as deception activities, where an adversary is caused to take actions (or inaction) that will either advantage the originator or disadvantage the adversary.[29] As an example, a successful IW campaign may cause an adversary to commit fewer assets to a battle, which can have the same effect as though those assets had been destroyed.[30] Success can be achieved by reinforcing adversary-preconceived beliefs, or by focusing the adversary's attention on otherwise unimportant activities to the benefit of the originator.

IW can also be particularly effective at altering perceptions because of a variety of factors related to social and behavioural psychology. In their paper "Firehose of Falsehood," social scientists Christopher Paul and Miriam Matthews from the RAND Corporation discuss these factors in the context of how propaganda can alter perception, proposing five key conclusions about society's general vulnerability to IW.[31] Firstly, humans often substitute heuristics when making judgements concerning the trustworthiness of information, particularly in an information-rich environment.[32] The use of these heuristics can lead to cognitive biases that can be exploited by an IW capable adversary.[33] The second key finding is that people generally have difficulty identifying false information, though they often overestimate their ability to recognize it. Studies also

---

[28] Lin and Kerr, "On Cyber-Enabled Information Warfare and Information Operations," 5.
[29] Ibid., 7.
[30] Ibid., 5.
[31] Christopher Paul and Miriam Matthews, *The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It* (RAND Corporation, 2016), 7, doi:10.7249/PE198.
[32] Ibid., 6.
[33] Lin and Kerr, "On Cyber-Enabled Information Warfare and Information Operations," 8.

show that information is often disassociated from its source when recalled, so even it is initially recognized as coming from a disreputable source, the information can be recalled at a later time as factual without any recollection of the disreputable source. Additionally, even when misinformation is retracted, it can leave a lasting impact and continue to influence people's perception despite their acceptance of the retraction.[34]

The third key finding speaks to the susceptibility of humans to confirmation bias and the fact that the likelihood of retransmission increases if it is expected to produce an emotional response in the recipient.[35] The fourth and fifth key findings are both strongly linked to the human tendency to use the representativeness heuristic when determining whether or not to accept information. The former is summarized as "statements are more likely to be accepted if backed by evidence, even if that evidence is false."[36] That is to say, people are accustomed to trusting evidence-based claims, without necessarily scrutinizing the evidence. Supporting this assertion, a University of Washington study demonstrated that the perceived credibility of a source could be increased simply by increasing the quantity and detail of evidence, without regard for its pertinence.[37] Similarly, the final takeaway from Paul and Matthews work is that the credibility of propaganda can be increased simply by peripheral cues that provide the appearance of authenticity or expertise. Once again, this can be attributed at least somewhat to the representativeness heuristic, whereby in the case of a live broadcast for example, if it

---

[34] Stephan Lewandowsky et al., "Misinformation and Its Correction: Continued Influence and Successful Debiasing," *Psychological Science in the Public Interest* 13, no. 3 (December 2012): 114, doi:10.1177/1529100612451018.

[35] Ibid., 108.

[36] Paul and Matthews, *The Russian "Firehose of Falsehood" Propaganda Model*, 7.

[37] Brad E Bell and Elizabeth F Loftus, "Trivial Persuasion in the Courtroom: The Power of (a Few) Minor Details," *Journal of Personality and Social Psychology* 56, no. 5 (1989): 4.

looks like a news broadcast in terms of format, lighting, content and presentation, it may be granted the credibility of a legitimate news broadcast without further thought from the viewer. Similarly, news sites on the internet are found to be consistently rated higher in terms of perceived credibility, as are sites with sophisticated designs and format.[38]

All these factors speak to a general human vulnerability to IW as a result of different forms of bias. When these different vulnerabilities are appropriately targeted and exploited, a competent IW actor is capable of altering the perceptions of its audience in a way that can be favourable to their objectives.

CYBER-ENABLED IW – IW ON STEROIDS

Given that propaganda and influence activities have existed since the first wars of man, the questions that should come to mind is why now? What has changed within the environment that makes IW an emerging priority? The purpose of this section is to discuss the emergence of *cyber-enabled* IW, what it is, and how it has changed the warfare landscape.

While providing expert testimony to the US Senate Committee on Armed Services, Rand Waltzman, Ph.D. and Senior Information Scientist with the RAND Corporation frames the problem well by stating: "Today, thanks to the Internet and social media, the manipulation of our perception of the world is taking place on a previously unimaginable scale of time, space and intentionality."[39] He maintains that for the most

---

[38] Andrew J. Flanagin and Miriam J. Metzger, "The Role of Site Features, User Attributes, and Information Verification Behaviors on the Perceived Credibility of Web-Based Information," *New Media & Society* 9, no. 2 (April 2007): 336, doi:10.1177/1461444807075015.

[39] U.S. Congress, Senate, Committee on Armed Services, *Cyber-Enabled Information Operations*, 115th Cong., 1st Sess., S. Hrg. 115-426, 2017, 14, https://www.govinfo.gov/content/pkg/CHRG-115shrg34175/pdf/CHRG-115shrg34175.pdf.

part, the techniques that have been used with print media, radio, movies and television have not changed significantly, but have been extended to the cyber domain through the advent and widespread adoption of the Internet and social media.[40] Essentially, it is the medium that has changed, not the messaging.

In the case of cyber-enabled IW, it is particularly important to distinguish between information operations intended to deliver effects *on* the cyber domain versus operations intended to deliver IW effects *through* the cyber domain. In the former, these types of operations represent what are known as cyber operations and are akin to operating in the virtual domain of the information environment. In the latter case, the cyber domain is the medium through which actions are taken in the cognitive domain within the information environment.

When employed advantageously, the characteristics of the cyber domain can significantly increase the magnitude and effectiveness of IW activities. In particular, adversaries can engage in IW on a scale not previously possible due to the low cost, high speed and global reach of the Internet. These characteristics enable a relentless high-speed tempo for the full spectrum IW operations, providing the sophisticated IW practitioner with a "first-mover advantage."[41] This is particularly relevant when, as discussed in the previous section, even information later proven to be false can continue to influence decisions.

Other beneficial characteristics of cyberspace with respect to the execution of IW include the disintermediation of information distribution, relative and absolute

---

[40] Ibid.

[41] Lin and Kerr, "On Cyber-Enabled Information Warfare and Information Operations," 14.

anonymity, and the insensitivity to distance and national borders.[42] Concerning disintermediation, in the past, information was primarily disseminated through traditional intermediaries (such as newspapers and national news outlets) who were responsible for distilling and interpreting large volumes of information and were held to account for its factual representation.[43] Because of the connectedness of cyberspace and the rise of social media however, information is now often shared without going through a trusted intermediary for distribution. As people access information through their social media feeds, they have also grown accustomed to receiving and accepting information from a variety of sources, many of whom are anonymous or at least unknown to the person accessing the information. All this to say that the disintermediation of information and the widespread acceptance of relatively anonymous sources of information fosters an environment that is ripe for use in the manipulation of perceptions. In addition, with few exceptions, the information in cyberspace is insensitive to travelling great distances and crossing national borders.[44] As such, cyber-enabled IW activities can be orchestrated from almost anywhere in the world and influence targets located almost anywhere else. What is more, due to the nature of cyberspace, regardless of where an IW actor is physically located, they can stage their attacks from within the relative safety of other jurisdictions, which may help to prevent prosecution, attribution or maintain anonymity.[45]

Another way in which the cyber domain enables the conduct of IW is the massive amounts of personal data available electronically that can be used by a would-be

---

[42] Ibid., 13.
[43] U.S. Congress, Senate, Committee on Armed Services, *Cyber-Enabled Information Operations*, 14.
[44] Lin and Kerr, "On Cyber-Enabled Information Warfare and Information Operations," 13.
[45] Ibid., 15.

adversary in the development of their influence campaign. Whether openly published or available for a fee, incredible amounts of catalogued electronic information is available that can provide meaningful insight into individuals, groups, corporations and governments' decision making. The availability and rapid pace at which information is maintained in cyberspace further provide for increasingly successful IW activities as this information can be used to measure the responses of individuals as well as groups to an actor's influence efforts.[46] In addition, while it is often taken for granted that information can be secured in cyberspace, the reality is that information insecurity in cyberspace results in a much greater potential for information leaking operations (discussed in the previous section) that would not otherwise be present.[47]

In the context of cyber-enabled IW, many of the fundamental characteristics and benefits of the cyber domain highlighted above (such as low cost, high speed, global reach, anonymity, and diversity), actually manifest as vulnerabilities to be exploited in the cognitive domain. While IW tactics and theory have not evolved significantly, the speed, reach, and low cost afforded by the cyber domain acts as a significant force multiplier, giving IW the potential to take a leading role in resolving (or preventing) conflict between states. As seen in the RF doctrine earlier, once cyber-enabled, where IW was once only a supporting function of conventional warfare, it can now be the preferred first strike.

---

[46] Rand Waltzman, "The Weaponization of Information: The Need for Cognitive Security," April 27, 2017, 2, https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT473/RAND_CT473.pdf.

[47] Lin and Kerr, "On Cyber-Enabled Information Warfare and Information Operations," 15.

THREATS AND OPPORTUNITIES

During Afghanistan operations, cyber-enabled IW was not a priority. When required, traditional IW was carried out utilizing direct communication with indigenous populations, with the multinational force delivering its message via newspapers and wind up radios.[48] From Canada's defence policy, it is clear that Canada is acutely aware that advances in IW present both threats to be defended against and opportunities for further development.[49]

As has been discussed earlier, one of the related challenges is understanding not only what capabilities cyber-enabled IW brings with it, but also understanding how the associated roles, authorities and responsibilities should be assigned within our national security construct. For example, one of the most significant IW threats to Canada stems from adversaries who wish to weaken democratic processes worldwide.[50] Canadian citizens are not immune to this threat, and in 2018, voters themselves represented more than 50% of the targets of the IW activities against democratic processes.[51] While there seems to be a consensus that Canadians should be defended against IW, a much more difficult question remains whose responsibility it should be, and what role the CAF might play (if any) in defence of the cognitive domain within Canada. In 2019, the Communication Securities Establishment (CSE), the Canadian Security Intelligence

---

[48] David Reynolds, "Cyber-Enabled Information Operations: The Battlefield Threat without a Face" (Jane's Defence Weekly, January 23, 2018), 6, https://www.janes.com/images/assets/438/77438/Cyber-enabled_information_operations_The_battlefield_threat_without_a_face.pdf.

[49] Canada and Department of National Defence, *Strong, Secure, Engaged - Canada's Defence Policy.*, 41,53,56.

[50] Communications Security Establishment Canada, *2019 Update on Cyber Threats to Canada's Democratic Process* (Ottawa, ON: Communications Security Establishment, 2019), 9, https://cyber.gc.ca/sites/default/files/publications/tdp-2019-report_e.pdf.

[51] Ibid., 17.

Service (CSIS), Global Affairs Canada (GAC) and the Royal Canadian Mounted Police (RCMP) jointly formed the Security and Intelligence Threats to Elections (SITE) task force. Somewhat surprising is that defending Canadians from IW is not an explicit task for any one of the partner agencies within Public Safety (namely CSE, CSIS, GAC and RCMP).[52] Part of the significant challenge related to defending Canadians from the threat of IW is that by current conventions, many of the affronts in the cognitive domain remain below the threshold of attack. As such, the existing agencies and institutions within Canada's national security framework are ill-equipped to respond in any capacity.

This failure to adapt to the realities of cyber-enabled IW is not unique to Canada. In 2017, former United States Under Secretary for Defence and Policy, Michael Lumpkin testified to the Senate Committee on Armed Services:

> While the means and methods of communications have transformed significantly over the past decade, much of the U.S. Government's thinking on shaping and responding in the information environment has remained unchanged, to include how we manage U.S. Government information dissemination and how we respond to the information of our adversaries.[53]

Similarly, Clint Watts, a distinguished research fellow with the Foreign Policy Institute, echoed this testimony, stating: "When it comes to Americans countering cyber-influence operations, when all is said and done, far more is said than [d]one. . . . When the U.S. has done something, it has not been effective. At worst, it has been counterproductive.[54]

---

[52] Democratic Institutions, "Security and Intelligence Threats to Elections (SITE) Task Force," *Aem*, February 7, 2019, https://www.canada.ca/en/democratic-institutions/services/protecting-democracy/security-task-force.html.

[53] U.S. Congress, Senate, Committee on Armed Services, *Cyber-Enabled Information Operations*, 9.

[54] Ibid., 20.

Watts goes on to blame the failure on the existing defence framework for managing IW and the failure of the associated bureaucracy.

Given that many elements within Canada's national security and force structures align closely with those of the United States, it is perhaps not surprising that similar institutional structures should lead to similar challenges with respect to adapting to advances in IW. While it is outside the scope of this paper to propose the specifics necessary to reform Canada's national security apparatus in support of IW, it is helpful to recognize key issues. In this case, it is useful to recognize that apart from the challenges associated with the evolving technology and doctrinal paradigms, the Canadian structure for the delivery of national security represents an impediment in and of itself. Given the considerable threat posed by cyber-enabled IW, Canada must adapt and learn how best to defend against it. CAF is the only entity within Canada's national security framework with the mandate and authority to conduct IW; however, this authority is limited to use within the context of military operations, and CAF experience in IW thus far is limited to traditional PSYOPS activities. Conversely, the other national security entities within Canada have neither a mandate to defend the cognitive domain, nor the authority to conduct IW.

Through SSE, Canada has recognized a need to operate more effectively in the cognitive domain; however, at present, neither the CAF nor the other national security entities have the appropriate mandates to be effective. While the advances in IW provide some potential military advantages at the tactical level, the most significant opportunities (and threats) that exist in the employment of cyber-enabled IW are at the political and

strategic levels. Recognizing this gap in policy, Canada needs to define better which (if any) national security entity should ultimately be responsible for conducting IW activities in support of non-military strategic objectives and defending Canadians against IW.

Worthy of further consideration, one nation that does not appear to be stymied with respect to IW by their national security structure is Russia. As discussed previously, RF doctrine recognizes the importance of employing "Information Confrontation" activities, in advance of or if possible in place of conventional forces. General Gerasimov, the Chief of Staff of the RF Armed Forces, reinforced this by stating that non-military to military operations should strive for a ratio of 4-1, putting an exceptional emphasis on non-kinetic operations which include IW.[55] Within the RF, the Federal Security Service (FSB) is the entity responsible for managing propaganda and disinformation campaigns.[56] They are the experts in cyber-enabled IW and lead both offensive and defensive influence activities across the spectrum of operations in support of achieving Moscow's strategic objectives. In this capacity, their role is to support RF stability and security by protecting against foreign efforts seeking to undermine it. To this end, many of the tactics that are used offensively to alter perceptions of adversaries are similar to those employed internally to reinforce notions of Russian patriotism and foster a strong narrative against western ideologies. Given the specialized skill set required to design IW campaigns, and the potential to reuse the same skill set for both offensive and defensive purposes, the concept of assigning a national security entity for being

[55] Valery Gerasimov, "The Value of Science Is in the Foresight," *Military Review* 96, no. 1 (2016): 28.
[56] Reynolds, "Cyber-Enabled Information Operations: The Battlefield Threat without a Face," 3.

responsible for both seems to represent a balanced compromise for managing limited resources.

Cyber-enabled IW has the potential to become a valuable capability for Canada. It can be used not only to weaken our adversaries but, more importantly, to prevent conflict and achieve strategic objectives while avoiding or reducing conventional military engagements and associated costs.[57] Conversely, cyber-enabled IW represents a significant threat. Canada must be ready to defend its citizens against those who would seek to manipulate them. In consideration of both the threat and the opportunity, Canada must quickly develop a comprehensive strategy for managing conflict in the cognitive domain. The current strategy of directing CAF to investigate and augment its existing reserve PSYOPS units in support of military operations,[58] and directing the non-military national security entities to simply watch and report on attacks on Canadian citizens[59] does not rise to the level of the occasion.

CONCLUSION

The purpose of this paper was to demonstrate that notwithstanding Canada's defence policy, Canada remains vulnerable to cyber-enabled IW and is weak in the application of it. The supporting themes throughout were that the cyber-enabled IW could be extremely beneficial (or dangerous) to Canada; however, the ambiguous terminology, the lack of experience and the lack of comprehensive national security strategy for IW

---

[57] Ibid., 11.

[58] Canada and Department of National Defence, *Strong, Secure, Engaged - Canada's Defence Policy.*, 66,69.

[59] Institutions, "Security and Intelligence Threats to Elections (SITE) Task Force."

continue to stymie Canada's ability to close the capability gap in IW (both offensively and defensively) with would-be adversaries.

In the first section, this was shown by highlighting that despite recognition for the importance of cyber-enabled IW within defence policy, current CAF doctrine is limited, and policymakers struggle to understand how IW has evolved and where it fits best within Canada's national security framework. In the second section, this was further demonstrated by exposing inconsistent terminology and contrasting doctrinal approaches between Canada and the RF. The following section detailed how humans are inherently vulnerable as a result of cognitive biases which can be targeted and exploited like any other vulnerability. In the penultimate section, the characteristics of the cyber domain were shown to act as a significant force multipliers for IW activities providing those who would embrace cyber-enabled IW a significant advantage. The final section revealed that agencies within the National security framework have neither the mandate nor the authority to conduct influence activities, leaving only the CAF with its limited experience in IW and lack of clear mandate to defend the cognitive domain of Canadians.

For all these reasons, Canada remains vulnerable to cyber-enabled IW and continues to be weak in its application. "The right bullet can stop a person; the right bomb can stop a regiment; the right message can stop a war."[60] While there can be little doubt that the CAF should be improving its own organic IW capabilities, the question remains one of scope. In order to be most effective, the CAF needs to better understand where they will fit within the greater national security framework. For any significant

[60] Phil Jones, *Communicating Strategy*, 1st ed. (New York: Gower Publishing, 2008), 20.

advances to be made, Canada will need to focus more effort on understanding the nature of the problem space, developing Canada's public policy towards operations in the cognitive domain (both at home and abroad) and designing the appropriate force employment structure.

BIBLIOGRAPHY

ABCA Armies. Influence Activities Handbook. Vol. 374. ABCA Publication, 2013. https://bib.cfc.forces.gc.ca/CFCLearn/mod/resource/view.php?id=2078.

Administration of the President of Russia. “Военная доктрина Российской Федерации [Military Doctrine of the Russian Federation].” Translated by Google Inc. Президент России, February 5, 2010. http://kremlin.ru/supplement/461.

Bell, Brad E, and Elizabeth F Loftus. “Trivial Persuasion in the Courtroom: The Power of (a Few) Minor Details.” Journal of Personality and Social Psychology 56, no. 5 (1989): 11.

Canada, Communications Security Establishment. 2019 Update on Cyber Threats to Canada’s Democratic Process. Ottawa, ON: Communications Security Establishment, 2019. https://cyber.gc.ca/sites/default/files/publications/tdp-2019-report_e.pdf.

———. Cyber Threats to Canada’s Democratic Process. Ottawa, ON: Communications Security Establishment, 2017. https://cyber.gc.ca/sites/default/files/publications/cse-cyber-threat-assessment-e.pdf.

Canada, Department of National Defence. B-GJ-005-313/FP-001 Joint Doctrine Manual. Psychological Operations. Kingston: Chief of Defence Staff, 2004.

———. B-GL-353-002-FP-001, Psychological Operations Tactics, Techniques and Procedures. Psychological Operations. Kingston, ON: Chief of Land Staff, 2011.

———. Canadian Forces Joint Publication Information Operations. 1st ed. Vol. 3–10. Canadian Forces Joint Publication. Ottawa, ON: Canadian Joint Operations Command, 2015. http://armyapp.forces.gc.ca/SOH/SOH_Content/CFJP 3-10 (2015).pdf.

———. Strong, Secure, Engaged - Canada’s Defence Policy., 2017. http://epe.lac-bac.gc.ca/100/201/301/weekly_acquisitions_list-ef/2017/17-23/publications.gc.ca/collections/collection_2017/mdn-dnd/D2-386-2017-eng.pdf.

Canada, and Public Safety Canada. Canada’s Cyber Security Strategy: For a Stronger and More Prosperous Canada. Ottawa, Ont.: Public Safety Canada, 2010. http://ra.ocls.ca/ra/login.aspx?inst=centennial&url=https://www.deslibris.ca/ID/225300.

Cary, Peter. “The Pentagon, Information Operations, and International Media Development.” Center for International Media Assistance, November 23, 201AD. https://www.cima.ned.org/wp-content/uploads/2015/02/CIMA-DoD-Report_FINAL.pdf.

Flanagin, Andrew J., and Miriam J. Metzger. “The Role of Site Features, User Attributes, and Information Verification Behaviors on the Perceived Credibility of Web-Based Information.” New Media & Society 9, no. 2 (April 2007): 319–42. doi:10.1177/1461444807075015.

Gerasimov, Valery. “The Value of Science Is in the Foresight.” Military Review 96, no. 1 (2016): 23.

“Inside the Surreal World of the Islamic State’s Propaganda Machine - The Washington Post.” Accessed April 13, 2020. https://www.washingtonpost.com/world/national-security/inside-the-islamic-states-propaganda-machine/2015/11/20/051e997a-8ce6-11e5-acff-673ae92ddd2b_story.html.

Institutions, Democratic. “Security and Intelligence Threats to Elections (SITE) Task Force.” Aem, February 7, 2019. https://www.canada.ca/en/democratic-institutions/services/protecting-democracy/security-task-force.html.

Jones, Phil. Communicating Strategy. 1st ed. New York: Gower Publishing, 2008.

Lewandowsky, Stephan, Ullrich K. H. Ecker, Colleen M. Seifert, Norbert Schwarz, and John Cook. “Misinformation and Its Correction: Continued Influence and Successful Debiasing.” Psychological Science in the Public Interest 13, no. 3 (December 2012): 106–31. doi:10.1177/1529100612451018.

Lin, Herbert, and Jaclyn Kerr. “On Cyber-Enabled Information Warfare and Information Operations,” May 2019, 29. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3015680.

MacFarquhar, Neil. “A Powerful Russian Weapon: The Spread of False Stories.” The New York Times, August 28, 2016, sec. World. https://www.nytimes.com/2016/08/29/world/europe/russia-sweden-disinformation.html.

“NATO Glossary of Terms and Definitions (English and French),” AAP 6, 6 (January 1, 2019). https://nso.nato.int/nso/ZPUBLIC/_BRANCHINFO/TERMINOLOGY_PUBLIC/NON-CLASSIFIED NATO GLOSSARIES/AAP-6.PDF.

North Atlantic Treaty Organization. NATO Bi-SC Information Operations Reference Book. NATO Bi-Strategic Command, 2010. https://bib.cfc.forces.gc.ca/CFCLearn/pluginfile.php/6678/mod_folder/content/0/NATO Bi-SC Information Operations Reference Book.

Paul, Christopher, and Miriam Matthews. The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It. RAND Corporation, 2016. doi:10.7249/PE198.

Perlman, David M. "Applied Computational Social Choice Theory as a Framework for New Cyber Threats." The Cyber Defense Review, 2019, 18.

Reynolds, David. "Cyber-Enabled Information Operations: The Battlefield Threat without a Face." Jane's Defence Weekly, January 23, 2018. https://www.janes.com/images/assets/438/77438/Cyber-enabled_information_operations_The_battlefield_threat_without_a_face.pdf.

Seaboyer, Anthony. "Influence Techniques Using Social Media." Defence Research and Development Canada, August 2018. https://cradpdf.drdc-rddc.gc.ca/PDFS/unc325/p807750_A1b.pdf.

United States, Joint Chiefs of Staff. Joint Doctrine for Information Operations. Vol. 3–13. Washington, DC: The Joint Cheifs of Staff, 2014. https://www.hsdl.org/?view&did=759867.

U.S. Congress, Senate, Committee on Armed Services. Cyber-Enabled Information Operations. 115th Cong., 1st Sess., S. Hrg. 115-426, 2017. https://www.govinfo.gov/content/pkg/CHRG-115shrg34175/pdf/CHRG-115shrg34175.pdf.

Waltzman, Rand. "The Weaponization of Information: The Need for Cognitive Security," April 27, 2017, 10. https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT473/RAND_CT473.pdf.

Wilson, Dennis G. "The Ethics of Automated Behavioral Microtargeting." AI Matters 3, no. 3 (October 10, 2017): 56–64. doi:10.1145/3137574.3139451.