National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

THE TROUBLE WITH INFLUENCE: ASSESSING THE APPLICABILITY OF DOMESTIC INFORMATION OPERATIONS

Maj Krzysztof Stachura

JCSP 44

Exercise *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.

© Her Majesty the Queen in Right of Canada, as
represented by the Minister of National Defence, 2018.

PCEMI 44

Exercice *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.

© Sa Majesté la Reine du Chef du Canada, représentée par
le ministre de la Défense nationale, 2018.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES
JCSP 44 – PCEMI 44
2017 – 2018

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

THE TROUBLE WITH INFLUENCE: ASSESSING THE APPLICABILITY OF DOMESTIC INFORMATION OPERATIONS

Maj Krzysztof Stachura

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

Word Count: 4740

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

Compte de mots: 4740

THE TROUBLE WITH INFLUENCE: ASSESSING THE APPLICABILITY OF DOMESTIC INFORMATION OPERATIONS

INTRODUCTION

When turning on the news it is difficult not to notice some headline dealing with information. Be it the ongoing Facebook data breach or the suspected Russian meddling in the United States presidential election, information is a valuable commodity. Good information can lead to good decision making; a staple of any functioning government or military organization. Not surprisingly, the militaries from countries like Canada, the United States, the United Kingdom, as well as many others, are developing expert capacities in how to use and leverage information to generate effects. The application of these ideas in a military context is referred to by Canada, UK, US and NATO as Information Operations (IO).[1]

So common is the term, and the practice of using information, that even corporations like Facebook have developed security policies to deal with the challenges associated with it. "We define information operations… as actions taken by organized actors (governments or non-state actors) to distort domestic or foreign political sentiment, most frequently to achieve a strategic and/or geopolitical outcome."[2] But the concept of using information to generate effects is not a novel idea. After all, the Canadian Armed Forces has had IO doctrine since at least 1998, well before the emergence of what many would consider a modern information environment, where everyone is connected with a smart phone. Since that time a lot of work has been done by many

[1] The term IO may be used by many other military organizations globally, however, for the purpose of this paper, most of the analysis was conducted by examining the doctrine from Canada, US, UK and NATO.

[2] Jen Weedon, William Nuland, and Alex Stamos, "Informtion Operations and Facebook," April 27, 2017, last accessed April 25, 2018, https://www.mm.dk/wp-content/uploads/2017/05/facebook-and-information-operations-v1.pdf, 4.

countries and organizations to define IO and develop doctrine and procedures that would frame its use in a new information environment.

Although some similarities in the doctrine exist, there is no global consensus on what constitutes IO and when it should or should not be used. Despite the fact that IO has been extensively used by the CAF and other militaries during international operations, little has been written on the potential applicability of IO in a domestic context. Limiting the use of information related capabilities and techniques to only adversaries and potential adversaries could limit the full range of tolls and resources that militaries and governments have at their disposal. In a very complex information environment where the line between domestic and international, particularity in the context of information is blurred and hard to delineate, options that deal with information should be considered.

This paper contends that IO methodology should be used domestically to focus information efforts to generate effects, support domestic operations and protect vulnerable information systems by unifying information capabilities and information techniques under one strategic umbrella.[3] However, given the particular nature of the Canadian domestic context, authority, legality and perception must be carefully considered. This will be conducted by first exploratory what is IO from a Canadian, NATO, US and UK perspective. This section will examine some of the similarities between the respective doctrines and how, if at all, they tackle domestic applicability. Second, the paper will review various information related capabilities in a domestic context. This section will scrutinize terminology like information, influence, Strategic Communication (StratCom) and Public Affairs to frame further discussion. Third, the paper will examine various information related activities and techniques and their potential

[3] One strategic umbrella does not refer to a singular organization responsible for all things IO but rather an overarching strategic framework that synchronizes information related activities to generate effects.

domestic applicability. Lastly, the paper will examine the legal and perceptional challenges of applying IO domestically.

INFORMATION OPERATIONS PRIMER

The need to develop Information Operations (IO) capacity is clearly articulated in Canada's 2017 defence strategy. Strong, Secure, Engaged (SSE) recognizes the need for greater investment to enhance IO capabilities and develop "military-specific information operations and offensive cyber operations capabilities able to target, exploit, influence, and attack in support of military operations."[4] In this regard, IO is a military function that "coordinates actions to create desired effects on the will, understanding and capability of individuals and groups, in support of overall objectives by affecting their information, information-based processes and systems, while exploiting and protecting one's own."[5] Therefore, IO coordinates and synchronizes information capabilities and information techniques to influence the behaviour of a target audience by targeting their will, capability or understanding.

The purpose of IO "is to secure peacetime national security objectives, deter conflict, protect the Department of National Defense (DND) and CAF information and information systems, and to shape the information environment."[6] At the strategic level, the goal of "offensive IO is to affect a human decision-maker to the degree that an adversary will cease actions threatening to Canadian national security interests."[7] At the operational and tactical

[4] Department of National Defence, *Strong, Secured, Engaged*, (Ottawa, ON: Department of National Defence, 2017), 41.

[5] Department of National Defence, *B-GJ-005-300/FP-001 Canadian Forces Joint Publication 3.0 – Operations* (Ottawa, ON: Department of Defence, 2011), para 0142.

[6] Ibid.

[7] Department of National Defence, *B-GG-005-004/AF-010, Canadian Forces Information Operations* (Ottawa, ON: Department of Defence, 1998), 1-1.

level, "IO targets and protects information, information transfer links, information gathering and processing nodes, and human decisional interaction with information systems."[8] Consequently, IO is an offensive and defensive capability and it will be discussed in both ways throughout the paper.

To achieve effects, IO utilizes a combination of information related capabilities and information related techniques. According to CAF IO doctrine, information related capabilities include Psychological Operations (PSYOPS), Cyberspace Operations (CNO/CYBER), Electronic Warfare (EW), Public Affairs (PA), and Civil-Military Cooperation (CIMIC). Information related techniques include engagement, deception, Operations Security (OPSEC), physical destruction, and Presence, Posture and Profile (PPP).

NATO, the United States and Great Britain use similar definitions of IO. NATO defines IO as a military capability that uses information "to create desired effects on the will, understanding and capability of adversaries, potential adversaries and other NAC approved parties in support of Alliance mission objectives."[9] The United States defines IO as the "integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own."[10] The United Kingdom defines IO as a staff function that utilizes "information activities to create desired effects on the will, understanding and capability of adversaries, potential adversaries and other approved

[8] Department of National Defence, *B-GG-005-004/AF-010, Canadian Forces Information Operations* (Ottawa, ON: Department of Defence, 1998), 1-3.

[9] North Atlantic Treaty Organization, *AJP-3.10, Allied Joint Doctrine For Information Operations* (NATO, 2009), 1-3.

[10] United States Joint Chiefs of Staff, Joint Publication 3-13, Information Operations (US, 2014), I-1.

audiences in support of mission objectives."[11] Despite some nuanced differences, at the core of the definitions is the need to generate effects. Although slightly different, these effects are generated through the application of information capabilities and information techniques on adversaries or potential adversaries.

A key similarity between the various countries and organizations that have developed IO doctrine, and that which underscores the discussion for this paper, is the exclusive use of IO against adversaries or potential adversaries. Most military and academic literature on the topic of IO focuses heavily, if not exclusively, on the applicability of IO capabilities and techniques in an expeditionary/adversarial way. Even the limited references to domestic IO focus on the negative connotations assigned to it. "While much of the current reporting and public debate focuses on information operations at the international level, similar tactics are also frequently used in domestic contexts to undermine opponents, civil or social causes, or their champions."[12] Although it may appear bizarre to reference Facebook as a source in making this argument, given how prolific Facebook is in the information environment, it would be inappropriate to entirely dismiss it from being a knowledgeable source. Given this rather negative view of the capability, is there potential to use IO domestically in a more balanced and positive way?

A COMPLICATED SPACE

The discussion on IO is often muddled by a variety of information related terminology that is not always applied equally across the domain. This next section will aim to standardise

[11] Ministry of Defence, Joint Warfare Publication 3-80, Information Operations (Shrivenham, UK: The Joint Doctrine & Concepts Centre, 2002), 2-1.

[12] Jen Weedon, William Nuland, and Alex Stamos, "Informtion Operations and Facebook," April 27, 2017, last accessed April 25, 2018, https://www.mm.dk/wp-content/uploads/2017/05/facebook-and-information-operations-v1.pdf, 4.

this terminology so as to set a foundation for further examination. Key terms to be defined include: information, strategic communication (often referred to as StratCom), Public Affairs (PA), and influence. Each of these will be discussed in the context of IO.

Any discussion on IO, or the applicability of IO, must first begin by answering the question: what is information and why anyone should care? The Oxford dictionary defines information as "facts provided or learned about something or someone."[13] Such a broad definition requires further analysis to contextualize its importance to the government and the military. According to Canadian Armed Forces doctrine, information is one of the four key instruments of national power. "Information itself is a strategic resource vital to pursuing national interest."[14] If information is a national instrument of power, then tools, resources, programs, and activities that help to manage this important resource are equally vital. There is academic debate on how important information is in the equation of power, which this essay does not aim to capture, however, the use of information as an instrument of power remain valid. "[O]rganizations, national-states and even individuals can now influence policy at the systemic level by using information. This was not necessarily the case a decade ago, but the huge explosion in technology…has vastly changed the power paradigm."[15] If tools and mechanisms, like IO, are being developed to exploit this space externally, then perhaps there is some utility in leveraging them domestically.

Little is written in CAF and NATO doctrine on the definition of influence. US doctrine offers a useful definition. It defines influence as "the act or power to produce a desired outcome

[13] "Information | Definition of Information in English by Oxford Dictionaries," Oxford Dictionaries | English, last accessed April 23, 2018, https://en.oxforddictionaries.com/definition/information.

[14] Department of National Defence, *Canadian Forces Joint Publication 01 Canadian Military Doctrine*, (Ottawa: DND 2009): 2-1.

[15] Leigh Armistead, *Information Operations: Warfare and the Hard Reality of Soft Power* (Washington, D.C.: Brasseys, 2004), 13.

or end on a [target audience].”[16] By applying information related capabilities or information related techniques on a target audience one can begin to modify rules, norms and beliefs and achieve influence. This allows for a structured approach that aims to link means, ways and ends. A target audience can be defined broadly, i.e. the Canadian public, or specifically, i.e. a key decision maker. A force (means) uses capabilities and techniques (ways) to create influence to achieve effects (ends). Understanding influence is critical to further discussion on the utility/practicality of applying IO concepts domestically. A large component of IO is predicated on the idea of influencing human behaviour to achieve effects. Central to the discussion, and further examined later in this paper, will be the legal and perceptional issues which come with influencing Canadians.

According to the NATO StratCom Centre of Excellence, StratCom “is the coordinated and appropriate use of NATO communication activities and capabilities in support of Alliance policies, operations and activities, and in order to advance NATO’s aims.”[17] NATO further defines the activities and capabilities to include Public Diplomacy, Public Affairs, Military Public Affairs, Information Operations and Psychological Operations. However, Strategic Communication is more than just an umbrella term that encompasses various information domains and enablers to achieve desired outcomes. Rosa Brooks, Professor of Law at the Georgetown University Law Centre provided a unique and simplified definition during testimony before the House Armed Services Sub-Committee on Evolving Threats and Capabilities. “[F]or me, strategic communication is a process – the exceptionally hard to achieve

[16] United States Joint Chiefs of Staff, Joint Publication 3-13, *Information Operations* (US, 2014), 1-2.

[17] NATO, "About Strategic Communications," NATO STATCOM, last accessed April 18, 2018, https://www.stratcomcoe.org/about-strategic-communications.

process of communicating strategically."[18] Further clarifying, she adds that strategic communication is the "difficult but critical process of listening, engaging, understanding perceptions, and then trying, in an orchestrated way, to align a wide range of capabilities in order to affect people's perceptions in ways that advance our national interests."[19] IO can play a key role in executing government StratCom objectives.

DAOD 2008-0, the keystone document for public affairs in the Canadian Armed Forces, defines public affairs as "activities related to informing internal and external audiences. It includes research and analysis, communications advice and planning, and the delivery of information programs."[20] IO and PA are complementary but unique disciplines that utilize information, information channels, messaging, and narratives to achieve desired outcomes. Although they are both used extensively on international operations, PA has a much broader domestic application. For this reason, any use of IO domestically would require a very coordinated approach with PA.

When framing these definitions it is important to acknowledge that informing, by itself, would not constitute an effect. That is, informing, only for the purpose of someone having information, may not achieve the desired outcome. For example, if everyone is aware that they should not text and drive, yet they continue to do so, then the influence portion has not been effective. Although there are many factors that may contribute to this example, it is intend to be only illustrative. Giving, denying, manipulating, coercing or extorting information from an individual are steps towards achieving effects. Even PA, whose role is "to promote

[18] Rosa Brooks, "Evolution of Strategic Communication and Information Operations Since 9/11," Hearing Before the Subcomm. on Emerging Threats & Capabilities of the H. Comm. on Armed Services, 112th Cong., July 12, 2011 (Statement of Rosa Ehrenreich Brooks), 3.

[19] Ibid., 4.

[20] National Defence, "DAOD 2008-0, Public Affairs Policy," DND CAF, April 19, 2017, las accessed April 21, 2018, http://www.forces.gc.ca/en/about-policies-standards-defence-admin-orders-directives-2000/2008-0.page.

understanding and awareness among Canadians of the role, mandate and activities of the CAF and DND, and of the contributions that the CAF and DND make to Canadian society and the international community,"[21] does so for the purpose of generating public support. "Public support for the CAF and DND follows from public understanding of how the CAF and DND make a difference at home and abroad."[22] This is important as it suggests a much closer and effects based relationship between the principles of IO and PA. It also explains why such great efforts are taken to synchronize and coordinate the release of departmental and CAF information. It is not enough to simply give the public information about the CAF and allow them to formulate their own opinion. Information is presented in a way to generate public support, as such, its release is strategically timed and generally positively contextualized. The CAF does not withhold information from the pubic for the purpose of a positive image. However, how, who, and when information is released is strategically considered before a decision is made. Even very negative news can be used as an opportunity to highlight positive policy information. Posturing that such doings are simply an information activity would be misleading.

Further complicating the CAF information environment is a vary compartmentalized information strategy. A quick review of the CAF external information presence yields in the discovery of hundreds of social media accounts, websites, and internal publications. What is more troubling is the lack of an apparent overarching CAF brand, message or narrative that aims to link them together. This paper does not aim to address the cause of this issue, however, it does conclude that operationalizing information through IO could help to better align the space. The effects based approach of IO, from a coordinating and synchronizing perspective, would provide a much needed structure to fuse this space under one coherent strategy.

[21] National Defence, "DAOD 2008-0, Public Affairs Policy," DND CAF, April 19, 2017, las accessed April 21, 2018, http://www.forces.gc.ca/en/about-policies-standards-defence-admin-orders-directives-2000/2008-0.page.

[22] Ibid.

A GOOD TYPE OF EFFECT?

As discussed in the previous section, one of the key tenants of IO is the use of information to generate effects. Generating effects is a key differentiating factor between IO and other information related domain activities. Are there effects that are more palatable then others in the context of IO that could be used domestically? What if there is a domestic requirement to influence people to certain behaviour or a certain pattern of behaviour? The domestic applicability of IO hinges on the discussion of effects. Canadian, NATO, UK and, to some extent, US doctrine refer to the concept of creating desired effects. The natural question becomes, what kind of effects are appropriate for a domestic target audience and is there a difference between a 'virtuous' effect and one that would be considered vile? And if so, who gets to decide?

In a theater of operation (outside of Canada), combinations of various information related enablers and techniques can be used to achieve desired effects. "During Operation Desert Strom, one of the most powerful IO instruments against Iraqi forces consisted of pre-announced B-52 strikes that followed leaflet drops detailing procedures for surrender; the key IO element being the B-52 itself."[23] In this particular example, the desired effect is the surrender of Iraqi forces. The same principle can be applied domestically, albeit in a different way and to generate very different effects.

Consider the applicability of IO in a Canadian Armed Forces response to a major domestic natural disaster. Given CAF involvement in recent Canadian natural disasters, such as floods and forest fires, it's reasonable to assume that the CAF would play some role. Also

[23] William M Daley, "Clausewitz's Theory of War and Information Operations," Issue 40 (1st Quarter 2006): 74, http://www.au.af.mil/au/awc/awcgate/jfq/4015.pdf.

important to this discussion is the acknowledgement that the Canadian Public is not one homogeneous entity that receives, processes or synthesizes information the same way. As such, IO can be either be applied generally, to a large component of the population, or more specifically towards a key decision maker.

The focal point of Canadian IO doctrine is the ability to create desired effects on "the will, understanding and capability of individuals and groups."[24] In the domestic natural disaster example, many of the information related capabilities could be used. For example, PSYOPS, which aims to influence target audience behaviour could be used to move people to particular safe areas or locations. This could be done through a leaflet drop or a text message burst.

Public Affairs (PA) can be used to communicate strategic messages about what the government is doing locally, to the rest of Canada, and internationally. This in turn can be used to encourage individual or international donations or the mobilization of local support efforts. Civil-Military Cooperation (CIMIC) could be used to provide a link between the CAF and various civilian organizations to better synchronize and coordinate effects. Other information related capabilities can be used to facilitate decision making or the protection of information systems and chains. It would be difficult to argue that using IO in this way would constitute a problem as the desired effects are in line with Canadian norms and practices.

Another area where IO could easily be applied domestically is defensive IO. Just as much as IO seeks to create desired effects on a particular group, it also seeks to protect one's own information capacity. As it becomes increasingly difficult to use traditional terminology to frame military problems, the utility of defensive IO becomes more pronounced. The recent

[24] Department of National Defence, *B-GJ-005-300/FP-001 Canadian Forces Joint Publication 3.0 – Operations* (Ottawa, ON: Department of Defence, 2011), para 0146.

example of Russian involvement in the United States Presidential Election underscores this modern requirement.

In the face of growing information threats from state and non-state actors, some domestic defensive IO capacity is paramount. "The internal infrastructure of a functioning society and/or state have now become objects of policy that considers these structures to be integral elements of a state's security."[25] Defensive IO seeks to protect those structures that "have become the object of governments' discourse about security and, particularly with regard to IO, a potential target for adversaries."[26] This is underscored by the fact that states like Russia see the deployment of IO as part of a modern weapon system[27]. As such, defensive IO cannot be relegated to named domestic operations but be constantly active in the background.

Defensive IO ensures that information is protected and that decision makers have access to relevant information. "Defensive IO also ensures friendly decision makers are protected from any adversary Offensive IO efforts. Defensive IO strives to ensure the friendly decision making process is protected from all adverse effects, deliberate, inadvertent or accidental."[28] This definition can be expanded to include those who then have the ability to influence the greater Canadian public. The Public Affairs Office at Canadian Joint Operations Command has embarked on an education campaign with Canadian media to ensure they are not being falsely swayed by an adversaries IO strategy. Although this is not specifically designed as a defensive IO strategy, it does demonstrate the practical applicability of IO in a domestic context. Such actions are necessary because "the information environment carries threats to Canada and CAF

[25] Stephen Blank, "Russian Information Warfare as Domestic Counterinsurgency," *American Foreign Policy Interests* 35, no. 1 (2013): 31.

[26] Ibid., 31.

[27] Stephen Blank, "Russian Information Warfare as Domestic Counterinsurgency," American Foreign Policy Interests 35, no. 1 (2013): 31.

[28] Department of National Defence, *B-GG-005-004/AF-010, Canadian Forces Information Operations* (Ottawa, ON: Department of Defence, 1998), 1-7.

operations at all levels from the tactical to the strategic."[29] In order to deal with actors that "seek to erode our values, culture, and our people's confidence in government and institutions by means of insidious disinformation campaigns,"[30] the CAF can leverage the concepts contained in IO doctrine and apply them domestically in a very similar fashion to the way they would be applied in any theater of operation. Similar to the natural disaster example, as the effects are generally positive, the benefits of using IO for this purpose appear to be obvious.

SO WHAT IS THE PROBLEM?

The previous sections laid the foundation for discussion and provided some examples of how IO can be used domestically. The following section aims to consider some of the challenges inherent in employing IO domestically and consider some risk mitigation strategies.

One of the significant challenges of applying the principles of IO domestically deals with intelligence. "Intelligence is the bedrock of IO. It is both foundational and essential to all military operations and its importance to influence campaigns is crucial."[31] This is true because by "providing population-centric social-cultural intelligence and physical network lay downs…intelligence can greatly assist IRC planners and IO integrators in determining the proper effect to elicit the specific response required."[32] Domestically, limitations exist on what type of general and specific information can be collected on the Canadian public. Without fully understanding the network and how decisions are made in this network it is impossible to apply the right capability to achieve that that effect.

[29] Col Luc Gaudet, "A Word from the Branch Advisor," Public Affairs Branch Notes (January 2018).

[30] Ibid.

[31] Leigh Armistead, *Information Operations: Warfare and the Hard Reality of Soft Power* (Washington, D.C.: Brasseys, 2004), 49.

[32] United States Joint Chiefs of Staff, Joint Publication 3-13, *Information Operations* (US, 2014), II-10.

Consider, if you will, a family trying to decide where to go on their next vacation. Both the parents have different views on how to proceed. Each will try to influence the other by presenting certain information with the aim of convincing the other. That approach only works by understating what information is important and how the individual makes decisions. If parent A trusts the advice of a friend, then parent B can try to influence the decision by first influencing the friend. Contrast this example against parent A who attempts to influence parent B by threatening to expose a secret. Although these are extreme examples on the opposites sides of the spectrum they underline the necessity of intelligence. Parent A needs to know who the friend is and that their opinion matters and parent B needs to know the secret.

The CAF defines this body of knowledge as part of the Intelligence Preparation of the Battlespace and concludes that the "conduct of sophisticated IO requires unique and detailed intelligence never before asked of intelligence collection agencies and activities."[33] Developing a list of information sources is normally only limited by ones imagination. It can include anything from covert operations to social media and open source news. However, collecting this type of information can be legally problematic. When considering broad target audiences, such as regional or national populations, a variety of open source documentation can be used to extrapolate what type of information may generate influence. Specific target audiences can be significantly more problematic. Designing a visit program for a parliamentarian with the aim of influencing their decision on a CAF acquisition project requires key knowledge of the individual that may fall outside the parameters of open source documentation. Setting aside the issues of influencing a politician, which will be discussed in a separate section, the execution of such a

[33] Department of National Defence, *B-GG-005-004/AF-010, Canadian Forces Information Operations* (Ottawa, ON: Department of Defence, 1998), 1-7.

strategy would rely heavily on intelligence. Canadian law limits the collection of this type of information.

Canada is not the only country that has legal or policy limitation that governs the information space from an IO perspective. In the US, the Smith-Mundt Act is the keystone documentation that limits the use of information operations by the US government, specifically psychological operations, on the US population. Signed into law by President Harry Truman in 1948, the Information and Educational Exchange Act, commonly referred to as the Smith-Mundt Act, was originally intended to give the US government the legal framework to deal with communist propaganda.[34] While the Act allowed for the distribution of US content abroad, it also limited what type of information the US government could release domestically. Although the act is not applicable in Canada, it does highlight the broader sensitivities and complexities associated with applying IO concepts domestically.

A second key challenge with the use of IO domestically deals with the problem of perception. Terms like PSYOPS, IO and influence have a negative connotation associated with them. What would be the reaction of the Canadian public if they knew that they were being influenced by CAF PSYOPS teams? Perhaps moving into the future, the CAF could examine the extant applicability of military terminology to define these capabilities. Certainly, marketing and advertising is a far more palatable term then PSYOPS and many similarities between the capabilities exist.

The concept of terminology change has been used by others in the past to good effect. In the US, "NORTHCOM took a liberal view regarding using information operations…following

[34] Weston R. Sager, *Apple Pie Propaganda? The Smith–Mundt Act Before and After the Repeal of the Domestic Dissemination Ban*, 109 Nw. U. L. Rev. 511 (2015). https://scholarlycommons.law.northwestern.edu/nulr/vol109/iss2/7, 518.

Hurricane Katrina. By replacing 'PSYOP' and 'information operations' with 'public information' and 'public information teams', they appear to have 'gotten around' legal restrictions."[35] Any future CAF doctrine work in this regard should carefully examine what terminology is used to define what capability. Although terminology may not address other concerns related to the use of IO domestically, it may help with the perception issues.

While the Russian example provided earlier serves to strengthen the need for defensive IO, it simultaneously causes pause for concern from an offensive domestic IO perspective. While Russia is using information warfare (IW) and IO externally it "has frequently waged its own from of IW and IO against its own people in order to secure or sustain the existing political regime." The potential fear is that, without the right control mechanisms, IO could be used domestically to generate questionable effects. Intelligence, authority, legality and perception are just some of the challenges that emerge when discussing the applicability of IO domestically. Combining these challenges with the issue of generating questionable effects further complicates the discussion.

MITIGATING THE RISK

Maj Peter Elstad, who conducted a detailed analysis questioning whether or not the US Army can execute information tasks domestically, concluded that "[t]he majority opinion…points to an 'implied' permission for using information tasks in domestic operations. Therefore it must be concluded that Army Information Tasks may be legally and doctrinally

[35] Peter L. Elstad, "Overcoming Information Operations Legal Limitations in Support of Domestic Operations" (U.S. Army Command and General Staff College, 2008), 49.

applied in domestic operations."[36] He is however careful to contextualize this legal and doctoral authority by stating that "there is some differing opinions regarding whether 'all', 'some' or 'none' of these Army information task capabilities may be utilized in domestic operations."[37] If that is the case, then some control mechanisms would be required to limit the use of IO domestically.

Perhaps one mechanism that could be used to limit IO use domestically is through a carefully constructed set of Rules of Engagement (ROE). Currently, ROE are defined as "directives issued by competent military authority which specify the circumstances and limitations under which forces will initiate and/or continue combat engagement with other forces encountered."[38] Furthermore, "ROE must coordinate the use of force appropriate to the mission assigned, ensure compatibility amongst potentially dissimilar partners, and ensure that military operations meet political objectives."[39] Although the current definition is focused on a more traditional application of military force it could be expanded to include IO in a domestic context.

If IO concepts were used domestically, within a structured named domestic operation or more broadly to coordinate all information, mechanisms will need to be put in place to limit its use. The ROE process provides an established mechanism for identifying authority and limitations under which force can be used. By broadening the definition of force to include the systematic use of information to generate effects, the established ROE mechanism could be used. These ROEs could be specific to individuals, target groups, messages, approaches or even effects. Given the growing use of information as a means to achieve effects, it is likely that

[36] Peter L. Elstad, "Overcoming Information Operations Legal Limitations in Support of Domestic Operations" (U.S. Army Command and General Staff College, 2008), 65.

[37] Ibid., 65.

[38] Department of National Defence, *B-GJ-005-000/FP-001 Canadian Forces Joint Publication 1.0 – Canadian Military Doctrine (*Ottawa, ON: Department of Defence, 2009), 2-16.

[39] Ibid., 2-16.

authority to use IO domestically in this fashion would require very senior military or political approvals.

CONCLUSION

This paper set out to examine the applicability of IO in a domestic context, contending that IO should be used domestically to focus information efforts to generate effects, support domestic operations and protect vulnerable information systems. Despite the fact that IO has doctrinally been developed as a means to deal with adversaries, some of the concepts have domestic applicability. CIMIC, PA and even PSYOPS could be used domestically in the right situation. Using IO is not without its challenges and risks. Legal limitations on the collection of intelligence and perception challenges remain. Although influencing may be considered negative in a domestic context, in the right framework it may be appropriate. By developing the right control mechanisms, through things like ROEs, it may be possible to effectively use IO domestically. Despite the fact that CAF IO doctrine is dated, the conceptual framework remains valid. Tools used for information will continue to evolve but the need to effectively coordinate and synchronize information will remain. The current CAF information environment is extremely complex and IO provides a mechanism for managing the space.

Significantly more research and analysis into this topic is warranted. How information is used will continue to change and evolve and the CAF needs the right tools to deal with it. IO provides a unique framework that aims to harmonize and synchronize information related capabilities and techniques to generate focused effects. If nothing else, the growing risk of cyber underscores the necessity of a robust defensive IO capability to protect ones vulnerable information systems. This can be achieved by operationalizing those activities through a nuanced and measured application of IO domestically. While there is risk in taking this approach, through careful management of the capability, open and transparent discussion with the Canadian public, it could become the singular mechanism to guide all CAF information efforts.

BIBLIOGRAPHY

Allen, Patrick D. Information Operations Planning. Boston: Artech House, 2007.

Armistead, Leigh. *Information Operations: Warfare and the Hard Reality of Soft Power*. Washington, D.C.: Brasseys, 2004.

Belgium. North Atlantic Treaty Organization. AJP-3.10, *Allied Joint Doctrine For Information Operations*. Brussels, Belgium: NATO 2009).

Blank, Stephen. "Russian Information Warfare as Domestic Counterinsurgency." *American Foreign Policy Interests* 35, no. 1 (2013): 31-44.

Brooks, Rosa. "Evolution of Strategic Communication and Information Operations Since 9/11." Hearing Before the Subcomm. on Emerging Threats & Capabilities of the H. Comm. on Armed Services, 112th Cong., July 12, 2011 (Statement of Rosa Ehrenreich Brooks)

Cairns-McFeeters Gina, John Shapiro, Steve Nettleton, Sonya Finley and Daryk Zirkle. "Winning the Ground Battles but Losing the Information War." Small Wars Journal (2010). http://smallwarsjournal.com/blog/journal/docs-temp/352-mnfiio.pdf.

Canada. Department of National Defence. B-GG-005-004/AF-010, *Canadian Forces Information Operations*. Ottawa, ON: Department of Defence, 1998.

Canada. Department of National Defence. *Strong, Secured, Engaged*. Ottawa, ON: Department of National Defence, 2017.

Canada. Department of National Defence. *B-GJ-005-300/FP-001 Canadian Forces Joint Publication 3.0 – Operations.* Ottawa, ON: Department of Defence, 2011.

Canada. Department of National Defence. *B-GJ-005-000/FP-001 Canadian Forces Joint Publication 1.0 – Canadian Military Doctrine.* Ottawa, ON: Department of Defence, 2009.

Canada. Department of National Defence. "Canadian Joint Operations Command." Last accessed on 30 January 2018. http://www.forces.gc.ca/en/about-org-structure/canadian-joint-operations-command.page.

Canada. Department of National Defence. "DAOD 2008-0, Public Affairs Policy." DND CAF. April 19, 2017. Accessed April 21, 2018. http://www.forces.gc.ca/en/about-policies-standards-defence-admin-orders-directives-2000/2008-0.page.

Daley, William M. "Clausewitz's Theory of War and Information Operations." Issue 40 (1st Quarter 2006): 73-78. http://www.au.af.mil/au/awc/awcgate/jfq/4015.pdf.

Elstad, Peter L. "Overcoming Information Operations Legal Limitations in Support of Domestic Operations." U.S. Army Command and General Staff College, 2008.

Gaudet, Luc (Col). “A Word from the Branch Advisor.” Public Affairs Branch Notes (January 2018).

NATO. "About Strategic Communications." NATO STATCOM. Accessed April 18, 2018. https://www.stratcomcoe.org/about-strategic-communications.

Oxford Dictionary. "Information | Definition of Information in English by Oxford Dictionaries." Oxford Dictionaries | English. Accessed April 23, 2018. https://en.oxforddictionaries.com/definition/information.

Sager, Weston R.. *Apple Pie Propaganda? The Smith–Mundt Act Before and After the Repeal of the Domestic Dissemination Ban*, 109 Nw. U. L. Rev. 511 (2015). https://scholarlycommons.law.northwestern.edu/nulr/vol109/iss2/7

The Free Dictionary. “Information Environment.” Last accessed on 30 January 2018. https://www.thefreedictionary.com/information+environment.

US. Joint Chiefs of Staff. Joint Publication 3-13, *Information Operations*. US: Joint Chiefs of Staff, 2014.

UK. Ministry of Defence. Joint Warfare Publication 3-80, *Information Operations*. Shrivenham, UK: The Joint Doctrine & Concepts Centre, 2002

Weedon, Jen, William Nuland, and Alex Stamos. "Informtion Operations and Facebook." April 27, 2017. Accessed April 25, 2018. https://www.mm.dk/wp-content/uploads/2017/05/facebook-and-information-operations-v1.pdf.