

Canadian
Forces
College

Collège
des
Forces
Canadiennes



Canadian Joint Operations Command: Canadian Armed Forces Joint Information Operations Operational Authority

Maj Krzysztof Stachura

JCSP 44

SERVICE PAPER

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

ÉTUDE MILITAIRE

Avertissement

Les opinions 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.

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES
JCSP 44 – PCEMI 44
2017 – 2018
SERVICE PAPER - ÉTUDE MILITAIRE

**Canadian Joint Operations Command: Canadian Armed Forces
Joint Information Operations Operational Authority**

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: 2506

“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: 2506

CJOC: CAF Joint IO Operational Authority

AIM

1. The aim of this service paper is to propose who is best suited to manage Information Operations (IO) and its different Information Related Capabilities (IRCs) within the Canadian Armed Forces (CAF). This paper will propose a new framework for the CAF management and employment of Joint IO in the information environment.

INTRODUCTION

2. Canada's recent defence policy, Strong, Secure, Engaged (SSE) identifies an investment in joint capabilities to improve IO capacity and develop "military-specific information operations and offensive cyber operations capabilities able to target, exploit, influence, and attack in support of military operations."¹ IO is a military function that "plans and coordinates military activities to create desired effects focused primarily in the cognitive domain. IO is comprised of three core activity areas: influence activities, counter-command activities, and information-protection activities."² IO, manoeuvre, and firepower make up the "Act" operational function that integrates the three to achieve effects.

3. 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

¹Department of National Defence, *Strong, Secured, Engaged*, (Ottawa, ON: Department of National Defence, 201), 41.

²Department of National Defence, *B-GJ-005-300/FP-001 Canadian Forces Joint Publication 3.0 – Operations* (Ottawa, ON: Department of Defence, 2011), para 0142.

systems, and to shape the information environment.”³ 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.”⁴ At the operational and tactical level “IO targets and protects information, information transfer links, information gathering and processing nodes, and human decisional interaction with information systems.”⁵

4. In order to effectively execute CAF Joint IO, an organization framework must exist to manage IO and its different IRC’s.

DISCUSSION

5. IO is a broad term that encompasses both offensive and defensive actions that comprises three core activities intended to create desired effects on the cognitive domain: influence activities, counter-command activities, and information-protection. “When viewed as an integrating strategy, IO weaves together related disciplines and capabilities toward satisfying a stated objective.”⁶ IO activities are developed through the targeting mechanism through the Operational Planning Process (OPP). This ensures that IO is synchronized and de-conflicted with other effects based enablers.

6. Most literature, military and academic, on the topic of IO focuses on the use of IO to achieve a strategic goal against an enemy or adversary. This definition of IO must be challenged as information can, and has effectively been used, to achieve effects both domestically and on

³Ibid.

⁴Department of National Defence, *B-GG-005-004/AF-010, Canadian Forces Information Operations* (Ottawa, ON: Department of Defence, 1998), 1-1.

⁵Ibid., 1-3.

⁶Ibid., 1-1.

operations abroad. All information introduced into the system produces an effect. A commander exchanging a phone call with a host nation mayor can have positive, negative or neutral consequences in affecting the cognitive domain. Equally, something as small as a poster within unit lines for an upcoming BBQ is competing with other information.

7. The information environment is defined as “the aggregate of individuals, organizations, or systems that collect, process, or disseminate information; also included is the information itself.”⁷ IO seeks to manage various information enablers that operate in the information environment. Those elements that can be leveraged to achieve IO effects span a wide spectrum of CAF capabilities. These include but are not limited to Psychological Operations (PSYOPS); Civil Military Cooperation (CIMIC); electronic warfare (EW); Public Affairs (PA); operational security (OPSEC); Presence, Posture, Profile (PPP); cyber and others.

8. Physical actions also generate information effects. The deployment of the Disaster Assistance Response Team (DART), for example, makes Canadians feel good, shows that Canada is a global contributor to a rule based order, and provides a launching platform for a broad range of strategic messages. “During Operation Desert Storm, 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.”⁸ These distinctions are important because although it may be possible to group some IRCs under one umbrella, many enablers can be used to achieve effects in the cognitive domain.

⁷The Free Dictionary, “Information Environment,” Last accessed on 30 January 2018, <https://www.thefreedictionary.com/information+environment>.

⁸William 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>.

9. The broad spectrum of capabilities that can influence the cognitive domain far exceeds those IRC's that are more traditionally associated with IO. For this reason, it is assessed that managing IO and its respective IRC's under one umbrella is not possible or advisable.

10. One of the key challenges of IO is the poor understanding of the relationship between IO and kinetic enablers during military operations. Operations in the information environment don't simply complement or support kinetic military operations. "Collectively, they are properly understood as a specific purpose and emphasis within an overall plan of action that under some circumstances might be the main effort."⁹ This is important as it suggests that separating IO from other effects generators does not allow for effective use of IO through an effects based approach. It is primarily for this reason that standing up a new L1 organization responsible for Joint IO was discounted and is not recommended.

11. The need for developing a joint and integrated strategy for operating in a complex information environment is greater than ever. "The information components of counterinsurgency (COIN) strategies are the underlying foundation for all other COIN activities."¹⁰ It is no longer possible to simply relegate IO to a supporting domain. "Information operations cannot be prudently conceived as merely added value to an operation, but rather as essential activities that address specific needs associated with the nature of political

⁹William M Daley, "Clausewitz's Theory of War and Information Operations," Issue 40 (1st Quarter 2006): 73, <http://www.au.af.mil/au/awc/awcgate/jfq/4015.pdf>.

¹⁰Gina Cairns-McFeeters, 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>

conflict itself.”¹¹ This required synergy can only be achieved through the integration of Joint IO into the CAF operational lexicon.

12. Where does this leave IO in the Joint CAF context? Despite the fact that IO has been a component of Joint CAF doctrine since at least 1998¹², information as an effective tool to achieve effects has only recently gained substantial traction in the CAF. Under the direction of the CDS, Director General Public Affairs has been mandated to modernize and operationalize public affairs in the CAF. This project has now expanded and will focus on integrating most military capabilities operating in the information domain into one professional community; optimizing the coordinated delivery of cognitive effects; and enhancing the training of those individuals operating in the information environment while focusing on achieving effects and supporting targeting.¹³ This is a step in the right direction.

13. It’s important to note that IO is already integrated into the OPP and part of the keystone CAF publication about how joint, combined, and interagency forces conduct operations. A framework already exists for how IO is incorporated into planning for domestic, continental and international operations. This construct should remain but its scope needs to increase to cover the connectedness of the information environment.

14. In order to achieve effects through the use of information, a mechanism must exist to coordinate and synchronize information to achieve a common goal. Even in the domestic

¹¹William M Daley, “Clausewitz’s Theory of War and Information Operations,” Issue 40 (1st Quarter 2006): 79, <http://www.au.af.mil/au/awc/awcgate/jfq/4015.pdf>.

¹²Department of National Defence, *B-GG-005-004/AF-010, Canadian Forces Information Operations* (Ottawa, ON: Department of Defence, 1998), 1-1.

¹³Col Luc Gaudet, “A Word from the Branch Advisor,” Public Affairs Branch Notes (January 2018).

context, this has proven to be extremely difficult and despite attempts to create some synergy with respect to information dissemination, the CAF system is challenged to execute this effectively.

15. For many of the identified reasons, it is recommended that Canadian Joint Operations Command (CJOC) assume the full responsibility for the execution of the CAF IO domestic and international strategy. CJOC is well suited to assume this role for various reasons. As the primary headquarters that prepares for and conducts operations to defend Canada, assists in the defence of North America, and, as directed, promotes peace and security abroad, it possesses the organizational structure that can be leveraged for operating in the information environment.¹⁴ Another key factor is that CJOC already has an established command and control structure, through the Joint Task Force organizations, that give it geographic coverage domestically. Internationally, it is the CAF organization responsible for international operations.

16. For various reasons that will not be specifically discussed in this paper, the information environment cannot be compartmentalized the same way as conventional operations. Terms like Area of Operations (AOO), Area of Influence (AOI), or Area of Responsibility (AOR) are profoundly more difficult to frame in the context of IO and various IRCs. Certain information can move freely across borders and the same organization needs to have the tools and capacity to deal with offensive and defensive IO in a theater of operation and offensive and defensive IO domestically. This is true because “the information environment carries threats to Canada and

¹⁴Department 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>.

CAF operations at all levels from the tactical to the strategic.”¹⁵ 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,”¹⁶ the CAF needs a comprehensive strategy. Grouping this function under one operational command creates synergy, removes ambiguity and decreases information fratricide.

17. Currently, this is being done by many CAF organizations that have various information agendas, control various dissemination information mechanisms, other IRC’s and operate with very little operational oversight. For example, at this time it is not clear who would have the role for defensive IO in the face of a Russian disinformation campaign responding to a CAF deployment in Latvia. Many IRC’s may need to be effectively leveraged to provide this level of defensive IO and an operation style mandate is required to synchronize the counter narrative. Allowing respective L1s to develop and execute independent IO campaigns (through PA, social media, Key Leader Engagements (KLEs) and other mechanisms) increases the risk of information fratricide and decreases the effectiveness of the message.

18. As information is not limited by traditional borders, greater IO interoperability will also be required with the United States. The recent allegation of Russian involvement in the United States Presidential Election, if proven true, is an excellent example of why a strong and coordinated defensive IO capability needs to be in place in Canada. It also underscores why separating the information space is not possible.

¹⁵Col Luc Gaudet, “A Word from the Branch Advisor,” Public Affairs Branch Notes (January 2018).

¹⁶Col Luc Gaudet, “A Word from the Branch Advisor,” Public Affairs Branch Notes (January 2018).

19. In the new proposed model, other CAF organization would remain contributors to the process of IO. Strategic Joint Staff (SJS) would be responsible for the identification of desired effects and the development of a narrative. SJS would remain the strategic/political interface to ensure effects, domestic or international, are in line with the Government of Canada strategy. As targets are developed, CJOC would be responsible for the development of the corresponding IO strategy. For deployed operations, based on desired effects, IO enablers would deploy forward or execute from Canada. How this would be tactically executed would depend on the complexity of the information environment, resources available for the operation and desired effects. Concurrently, similar or different enablers would be supporting complementary effects in a domestic setting.

20. SJS would also be responsible for the prioritization of effects identified by L1s. In this structure, L1s would lose some latitude to structure independent activities in the information environment. This would allow for a more integrated CAF information strategy rather than one conducted in siloes. A small example is the lack of coordination between the plethora of social media accounts that currently exists within the CAF. Although this point is minute, it highlights the challenges of operationalizing information to generate effects. If the CAF is incapable of an effective social media strategy that transcends L1 requirements, how is it going to implement an effective IO strategy that seeks to incorporate many other information enablers?

21. Other organizations would continue to play a role in supporting Joint IO. While CJOC remains responsible for force employment, various other CAF and DND organizations would take a more proactive role in force generation. Key to success is the development of specialists

who understand how to use various enablers, kinetic and non-kinetic, to achieve cognitive effects. One possible location where this specialty could be generated is within Assistant Deputy Minister (Public Affairs). Such an option would be in line with the Chief of Defense Staff (CDS) mandated project currently underway by Director General Public Affairs. Various environments and L1s would also remain force generators for specific IO enablers that already reside in their respective areas of expertise. For example, the Canadian Army would remain the force generator for Influence Activities. This could be done through the Canadian Combat Support Brigade.

22. Under this proposal, any information based activity (domestic or international) conducted by the CAF that has the potential to generate an effect, would be synchronized and coordinated by CJOC. Supporting this endeavour would be JTFs. One of the key synergies gained by placing IO under CJOC is the opportunity to leverage non-traditional information enablers to achieve information effects.

23. One key impediment of implementing this strategy is the currently established IO doctrine. IO is a synchronization and de-confliction function. In this framework, IO would need to be executed more like conventional operations rather than just through coordination.

24. The CAF must also be cautious to not create another information effects enabling stove pipe. Key to effectively employing Joint IO is the need to properly coordinate and synchronize information enablers to achieve the commander's intent. In order for this to be done effectively, all information enablers need to be working to achieve the same effect. From a command engagement to the deployment of Electronic Warfare to a News Release needs to be

synchronized under one overarching umbrella. Otherwise, any efforts will simply add unnecessary noise to an already very crowded information space.

CONCLUSION

25. The need for the CAF to be actively involved in the information environment will continue to exist. As this space continues to grow in complexity the strategy required to operate in this environment will also need to mature. Technology that was once relegated to only the most powerful organizations has now been made available to almost every human on the planet. This access brings with it an opportunity for an adversary to spread hate and radical ideas that undermine the credibility of the CAF and erode the confidence of the Government of Canada.

26. CJOC is the best positioned command within the CAF to conduct Joint IO. Significant work and analysis still needs to be done to ensure that the current domestic IRC's that operate at the tactical level in support of L1s are integrated into an effective Joint IO strategy; however, the overall operational lead should nonetheless be CJOC.

27. A lot of expertise exists in the various IRC's that provide IO effects. What is missing is the capacity to effectively synchronize and coordinate those effects to achieve operational and strategic effects. The largest observed gap is lack of training and education; both in terms of specialists who are versed in operating in this environment and the Chain of Command in how to employ them.

RECOMENDATION

28. In closing, it is recommended that the CAF continue to expand its IO capacity particularly in understanding and training on how to use IO enablers to achieve effects in the cognitive domain. As the information environment grows in complexity, it is also recommended that the responsibility for the employment of IO, domestically and deployed, is grouped under CJOC. This proposal would require a fundamental restructure on how IO, strategic communication and public affairs are executed in Canada. Given the breadth of enablers that can be used to achieve informational effects, it is also recommended that individual organizations and LIs retain subject matter expertise in the various domains that make up IRC's.

Bibliography

- Allen, Patrick D. *Information Operations Planning*. Boston: Artech House, 2007.
- 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. "Canadian Joint Operations Command." Last accessed on 30 January 2018. <http://www.forces.gc.ca/en/about-org-structure/canadian-joint-operations-command.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>.
- Gaudet, Luc (Col). "A Word from the Branch Advisor." Public Affairs Branch Notes (January 2018).
- The Free Dictionary. "Information Environment." Last accessed on 30 January 2018. <https://www.thefreedictionary.com/information+environment>.