National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

INTERSECTION OF THE INFORMATION AND CYBER DOMAINS

Major Lauren Banks

JCSP 46

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.

PCEMI 46

Étude militaire

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

SERVICE PAPER - ÉTUDE MILITAIRE

INTERSECTION OF THE INFORMATION AND CYBER DOMAINS

Major Lauren Banks

Word Count: 2,426

Nombre de mots : 2,426

INTERSECTION OF THE INFORMATION AND CYBER DOMAINS

AIM

1. The vast majority of the world is now interconnected in unprecedented ways. Technology has permeated all aspects of modern life across the globe and has enabled societies to access large amounts of information, providing reach and scale that transcend time and space. This era of instantaneous access to information has enabled broad advances in the technology used to modernize the way the Canadian Armed Forces (CAF) engages in conflict, but it has also opened up significant vulnerabilities. The aim of this paper is to demonstrate the need for the CAF to formally recognize the Information/Cyber space as a war fighting domain by enabling coordination between Cyber Operations, Information Operations, and Public Affairs at the strategic, operational, and tactical levels. It will also justify the need to foster an "Information Warrior" culture in order to fully leverage this domain, and provide recommendations on areas for further study.

INTRODUCTION

2. Several incidents in the recent past have demonstrated that nation states are actively engaged in information and cyber operations against Canada and its allies, to include online persona operations, social media influence operations, and active cyber operations.[1] Strong, Secure, Engaged (SSE) acknowledges that:

> social media and smart technology have transformed every aspect of daily life, conferring great benefits on the people it connects, worldwide. But much greater

[1] O'Flaherty, *Cyber Warfare: The Threat from Nation States.* https://www.forbes.com/sites/kateoflahertyuk/2018/05/03/cyber-warfare-the-threat-from-nation-states/#741fed751c78. (accessed October 25, 2019).

> access to communications technology has simultaneously fostered new vulnerabilities, which we are called to address.[2]

Conversely, this also provides a variety of new opportunities to further military objectives, both in the manipulation of the technology or the deliberate use of the information residing on it. This has resulted in a new kind of conflict that is asymmetric, constantly evolving, and extremely effective for those who know how to properly leverage it.

3. This will only continue as adversaries across the world, from nation states with political or economic agendas to terrorist groups attempting to expand their reach, continue to leverage the Information/Cyber Domain to achieve objectives contrary to Canada and Canadian interests. Given that nation state adversaries have been investing in ways to leverage information to gain political and national advantage, it is reasonable to assume that future conflicts will include the deliberate use of this space. The CAF must be prepared to both defend against it and leverage it to our advantage.

4. This paper will first define the Information/Cyber Domain and describe the requirement for centralized coordination between Information Operations, Public Affairs, and Cyber Operations. It will then identify the importance of close coordination between defensive and offensive operations within this space and, subsequently, will discuss the importance of developing deliberate Information/Cyber campaign plans in order to provide the necessary training and guidance to members of the CAF as active contributors to the overall Information/Cyber environment.

---

[2] Department of National Defence, *Strong, Secure, Engaged.* (Ottawa, ON: Department of National Defence, 2017), 49

DISCUSSION

5. In "How We Fight", LGen Rouleau states that the "CAF is operating today, every day, in the Grey Zone. We are in conflict with nation states below the threshold, largely in the informational space which is fast becoming the CENTRAL theatre for strategic competition."[3] To adequately respond to this challenge, it is necessary for the CAF to not only develop an expertise in all aspects of this information space, but to maximize coordination of these efforts.

6. **Defining the Information/Cyber Domain.** In order to fully understand the intersection between the information space and "cyber", it is necessary to clarify the difference between Cyber Operations and other activities within the cyber domain. Cyber Operations is defined as "attacking, defending, or collecting information from other computers, where computers is used broadly to mean electronic systems that collect, process, store, and communicate information."[4] For the purpose of analysis within this paper, this does not include those in cybersecurity such as Information Systems Security Officers (ISSOs) or Network Security Engineers, nor does it include those in Information Technology (IT) service provision, such as the J6 community.

7. The intersection between the information environment and cyberspace can be described as follows:

> Cyberspace represents flows of information to machines and humans… these flows of information have a physical manifestation and can create physical effects by altering the logic of computing systems. Information also has a

[3] Rouleau, MGen M, *How We Fight: Commander CJOC's Thoughts* (Canadian Joint Operational Command, 2019), 6

[4] Conti, Gregory, and David Raymond, *On Cyber: Towards an Operational Art for Cyber Conflict.* (Kopidion Press, 2017), 4

> cognitive component, and the right flow of information at the right time will alter the decision making of humans, whether they be governments, militaries, insurgent groups, businesses, or individuals. We can expect militaries to operate in cyberspace not just to cause physical effects on the battlefield or to gather intelligence, but also to carefully target the decision making capabilities of allies, adversaries, neutral parties, and populations.[5]

As described above, the CAF must be postured to operate in the Information/Cyber Domain to achieve both physical and cognitive effects. However, the communities that operate within both the physical and cognitive subsets of this domain are largely disjointed, and there does not exist a centralized element at any level that brings them together.

8. Within the cognitive subset of the Information/Cyber Domain exists the Public Affairs and Information Operations functions. The role of Information Operations is to "influence decision makers by affecting other's information while exploiting (fully utilizing) and protecting one's own information,"[6] while the role of Public Affairs is to provide information to Canadians related to the Government's decision to deploy the CAF and any information related to the structure, people, and activities of deployed forces.[7] Although the intended audiences and underlying objectives are quite different, this all occurs within the same cognitive space of the Information/Cyber Domain.

9. Within the physical subset of the Information/Cyber Domain is the Cyber Operations community, including Defensive Cyber Operations (DCO) and Offensive Cyber Operations (OCO) planners, staff, and Cyber Operators within the Joint Force

---

[5] Conti, Gregory, and David Raymond, *On Cyber: Towards an Operational Art for Cyber Conflict*., 55

[6] Department of National Defence. *B-GG-005-004/AF-010, CFJP 03.10 – Information Operations.* (Ottawa, ON: Chief of the Defence Staff, 1998), 1-2

[7] Department of National Defence. *DAOD 2008-4, Public Affairs, Military Doctrine and Canadian Forces Operations*. (Ottawa, ON: Department of Defence, 1998)

Cyber Component Command (JFCCC), as well as various cyber operations planners located throughout the other L1s. The Communications Security Establishment (CSE) is also prominently involved in this space, notably with the authorities to conduct Active Cyber Operations (ACO) under Bill C-59 and with the establishment of the Canadian Centre for Cyber Security (CCCS) to defend government systems, among other tasks.[8]

10. The concept of leveraging both the cognitive and physical subsets of the Information/Cyber Domain within the CAF is not new. The Canadian Forces Joint Publication on Information Operations published in 1998 dictates that offensive and defensive Information Operations should be coordinated between the disciplines involved, including Cyber Network Attack[9] and Public Affairs.[10] More recently, task 65 in SSE states that the CAF will improve several information and cyber operations capabilities, including "the development of military-specific information operations and cyber operations capabilities able to target, exploit, influence, and attack in support of military operations."[11] Despite the direction in doctrine, the CAF is not organized to ensure full collaboration between the IO, PA, and Cyber communities.

11. In order to foster the culture and establish the necessary policies, training, and doctrine to effectively engage in this domain, the CAF must establish an entity at the strategic level consisting of personnel with expertise in each of the above areas. This will

---

[8] Canadian Centre for Cyber Security Website. https://www.cse-cst.gc.ca/en/backgrounder-fiche-information (Accessed October 26, 2019)

[9] The term "Cyber Network Attack" is no longer used; it has evolved to include Defensive Cyber Operations - Response Action (DCO-RA) and OCO

[10] Department of National Defence. *B-GG-005-004/AF-010, CFJP 03.10 – Information Operations*, 1-5

[11] Department of National Defence, *Strong, Secure, Engaged*. (Ottawa, ON: Department of National Defence, 2019), 41

provide the necessary guidance and support to operational planners across all domains in order to properly incorporate Information/Cyber Domain considerations into their planning. Subsequently, this should permeate down to the tactical level both domestically and abroad with planners employed at each level.

12. **Importance of coordination between offensive and defensive planning.** In addition to ensuring coordination between Information/Cyber Domain stakeholders, it is necessary to ensure that both defensive and offensive efforts are closely coordinated. Given that the vast majority of information is delivered through networks and other digital media, most information-related activities are contingent on maintaining freedom of maneuver in the cyber domain. Therefore, both defensive and offensive plans must be synchronized between those coordinating the deliberate delivery of information (ie. Information Operations/Public Affairs), and those safeguarding the freedom of maneuver (ie. Cyber Operations), in order to ensure de-confliction of activities.

13. Considerations of the defensive plan on a given mission should include an analysis of both the cognitive and physical components of the Information/Cyber Domain and how CAF forces communicate, access, and utilize information. This will require a thorough understanding from the J6 staff on all networks and systems that will be used throughout the mission, including C2 systems, Mission Planning systems, Morale and Welfare networks, etc. It is important to note that this is not limited to “Blue Space”, or portions of cyberspace that are managed or controlled by the CAF, but could also include commercial cell phone towers, local Internet Service Providers (ISPs), or online services that are located outside the Area of Operations. The next aspect to take into consideration is the information itself, and whether the integrity, availability, or confidentiality is the

higher priority. This will enable DCO planners to effectively plan where to place sensors and monitor the network for indicators of compromise (IOC).

14. The next layer of the defensive plan should include an understanding of the cognitive space, which highlights the need for expertise in Public Affairs. For example, if an adversary intends to uses social media to slander Canadian forces in the public eye, Public Affairs planners would be required to properly advise on how to effectively counteract those attempts while minimizing damage to mission objectives. From a coordination perspective, DCO planners could then aim to monitor areas of the network deemed to contain photos or information that, if ex-filtrated by adversaries, could be used to further the slander campaign. Close coordination between the Information/Cyber Domain planners would increase the Situational Awareness of both the cognitive and physical elements of the defensive plan, increasing its overall effectiveness.

15. Similarly, an effective offensive plan should centre around a thorough understanding of the adversary's use of information, and the elements of the plan would seek to deny, degrade, disrupt, destroy, or manipulate this information. This could include a variety of effects that range from strictly IO, to strictly cyber, or a combination of both. One example would be the denial of their C2 with an OCO effect against their primary means of communication. Another would be the disruption of the message they send to their supporters through a targeted information operations campaign. It could be a combination of the two, in which an IO message is delivered through text messages. In all of these cases, it is necessary to understand the adversary's use of the Information/Cyber Domain, including the physical and cognitive elements.

16. In order to develop an effective offensive and defensive strategy at the tactical level, it will be necessary to include both "physical effects" (ie. manipulation of code on adversary systems with a cyber effect) and "cognitive effects" (ie. IO message delivery). Without proper coordination between the two, there is a risk that a cyber effect could take out the delivery platform intended for IO message delivery, or an IO message could not reach the intended target due to a misunderstanding of the target's use of cyberspace. This is all contingent on accurate intelligence, but it highlights the need for all elements conducting operations in the information space to be closely coordinated.

17. **Fostering a culture of "Information Warriors" to fully leverage the Information/Cyber Domain.** The CAF contains an unprecedented number of people who grew up in the digital age and are well versed in the power of the internet. This can be an immense asset if leveraged properly, as each soldier could become a tactical asset within the ongoing information war. However, if left unchecked or not properly managed, this creates further vulnerabilities as errors in the information space at the tactical level can have grave strategic impacts. This not only requires an increase in standard training across the CAF for all members, but also amplifies the need for a deliberate, well-understood Campaign Plan for each mission to provide proper guidance to each deployed member on how to navigate the Information/Cyber Domain. The plan should be coordinated with the overall mission Campaign Plan, though aspects of it such as Area of Influence, Area of Operations, and Area of Interest[12] and should reflect the cognitive and physical aspects of the Information/Cyber Domain the mission will operate within.

[12] Department of National Defence. *B-GJ-005-300/FP-001 Canadian Forces Joint Publication 3.0 - Operations*. (Ottawa, ON: Department of Defence, 2011), 5-4

18. In the same way that soldiers, sailors, and aviators are engrained with a thorough understanding of how to properly handle a weapon, so too should they be engrained with an understanding of how to properly handle information as a critical resource, and a keen awareness of their presence in the cyber domain as a contributor to the fight. The CAF must foster an "Information Warrior" culture in which all members are trained to understand the part they play in the broader picture.

19. In the past, most Social Media policies for deployed operations placed an emphasis on Operational Security (OPSEC), operating under the assumption that an adversary might leverage information posted online to cause harm to friendly forces. As a result, Social Media policies were developed with restriction in mind, to inform troops what they should not do, and put little emphasis on informing them of what they should do. In addition to the leadership challenge this presents when personnel inevitably post on social media in an unsuitable manner, this also fails to acknowledge the advantage that could be gained with the online presence of our soldiers deployed overseas.

20. An integrated Information/Cyber Campaign Plan will be necessary to provide guidance to the soldiers on the ground in any deployed setting. This will not only reduce the potential negative outcomes of misuse of social media, but it will also leverage each soldier as a potential asset to contribute to the informational objectives. Whether this is the contribution to the Public Affairs message in order to gain support from the Canadian Public, acting as a sensor to gain intelligence on the adversary's use of cyberspace, or a keen delivery of messaging in line with the Information Operations strategy, enabling the troops on the ground will enable the greatest impact in the cyber domain.

CONCLUSION

21. The time it takes for information to traverse the internet from one side of the globe to the other is almost instantaneous, and the ways in which information is weaponized are evolving as quickly as the human imagination. In order to properly prepare for the ongoing and future conflict within the information space, it is necessary for the CAF to not only invest in the expertise of uniformed information and cyber professionals, but also to enable them to coordinate closely in developing deliberate, intelligence-driven strategies.

RECOMMENDATION

22. Building off of the tasks set out in SSE, it is recommended that the CAF establishes an entity at the strategic level comprised of expertise in Information Operations, Public Affairs, and Cyber Operations to establish the policy, doctrine, and training required to foster a culture of disciplined Information Warriors at all levels. At the operational level, staff from these three disciplines must collaborate to integrate Information/Cyber Domain considerations into Operations Plans for every mission, both domestic and deployed. At the tactical level, it is necessary to have cyber, IO, and PA staff employed to develop coordinated Information/Cyber Domain operations, both offensive and defensive.

23. Further analysis is recommended to address whether the CAF currently has the ability to recruit, train, and retain personnel with the right skill sets to effectively address this issue, specifically in the Information Operations space. Further analysis is also recommended regarding the organizations or sections under which the strategic, operational, and tactical elements should be placed.

BIBLIOGRAPHY

Canada. Department of National Defence. B-GG-005-004/AF-010, CFJP 03.10 – Information Operations. Ottawa, ON: Chief of the Defence Staff, 1998-04.

Canada. Department of National Defence. *Strong, Secure, 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. *DAOD 2008-4, Public Affairs, Military Doctrine and Canadian Forces Operations*. Ottawa, ON: Department of Defence, 1998.

Canadian Centre for Cyber Security Website. https://www.cse-cst.gc.ca/en/backgrounder-fiche-information (Accessed October 26, 2019)

Conti, Gregory, and David Raymond. *On Cyber: Towards an Operational Art for Cyber Conflict.* Kopidion Press *(2017).*

O'Flaherty, Kate. "Cyber Warfare: The Threat from Nation States." *Forbes.com*. https://www.forbes.com/sites/kateoflahertyuk/2018/05/03/cyber-warfare-the-threat-from-nation-states/#741fed751c78. (accessed October 25, 2019).

Rouleau, Lieutenant-General M. *How We Fight: Commander CJOC's Thoughts*. Ottawa: Canadian Joint Operations Command, 10 February 2019.

The Initiatives Group. *Information Environment Assessment Handbook, Version 5*. Washington, DC: Officer of the Under Secretary of Defense for Intelligence, 2013.