National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

# THE CASE FOR AN ARMY CYBER INTELLIGENCE CAPABILITY

Maj A.T. Legge

## JCSP 42

## 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 42

## 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 42 – PCEMI 42
2015 – 2016

JCSP SERVICE PAPER – PCEMI ÉTUDE MILITAIRE

# THE CASE FOR AN ARMY CYBER INTELLIGENCE CAPABILITY

Maj A.T. Legge

*"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: 2267

*"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: 2267

# THE CASE FOR AN ARMY CYBER INTELLIGENCE CAPABILITY

## AIM

1. This service paper recommends that the Commander of the Canadian Army (CCA) create a Land cyber Intelligence capability to address the current operational deficit faced by the Canadian Army.[1] Its findings are the result of analysis done by Army Int regarding future threats and capability gaps our force will face.

## INTRODUCTION

2. This paper addresses a critical operational requirement facing the Canadian Army (CA), then examines the future cyber force structure; and second, informs any future PRICIE+G analysis of how to structure the Intelligence component for Land forces.[2] Currently there are no person years (PY) dedicated to cyber Intelligence in the Army and despite the joint nature of cyber, virtually all infrastructure is found on land.[3] Across the CAF, there is a very limited staff element of nine PYs dedicated to directly supporting cyber activity. Six of these are with the Canadian Armed Forces Intelligence Command (CFINTCOM), and one is a senior non-commissioned member (NCM) with the Joint Cyber Operations Team at Canadian Joint Operations Command (CJOC); the remaining three are in Chief of Force Development (CFD) charged with developing cyber Int force structure.[4] Unlike other Intelligence analysts, these specialists focus on "cyberspace," which CAF and the United States (US) Department of Defence (DOD) define as: "a global domain consisting of interdependent networks of information technology, including the internet, telecommunications, computer systems,

[1] The terms "Army," "Land" and "Land forces" are used interchangeable in this service paper to refer to the land environment and Canadian Army because the nuance between these terms will not affect the recommendations, or the gap/needs analysis.

[2] PRICIE+G stands for: Personnel, Research and Development, Infrastructure and Organization, Concepts, Doctrine and Collective Training, Information Management, Equipment; and Generation of Forces.

[3] There are rare instances, such as the Google "barge" that use floating platforms, as well as satellites.

[4] The total cyber establishment is 40 PYs; however, not all of these positions have been filled.

embedded processors and controllers."[5] Additionally, CAF defines the cyber domain as "the subset of the global cyber environment where CAF users process, disseminate, and store information, (as well as the) communications information systems (CIS) for command and control (C2), Intelligence operations and business functions of the CAF."[6] Thus, although a small amount of Intelligence capability is devoted to cyber, it does not remotely resemble the level of capability found in the All Source Intelligence Center (ASIC), or in a Joint Intelligence Center (JIC).[7] Furthermore, it does not address the longer term institutional issues of cyber Intelligence doctrine, training and policy.

3. The central argument to this paper is that the Canadian Army requires a cyber Intelligence center to address the threat from its adversaries as well as maintain a robust defence against the current persistent, sustained cyber threats. Such a capability would also put the CA on equal footing with its allies, who already have cyber Intelligence staffs. The Army's analysis notes that: "the projection of power is possible with the use of information rather than only through the movement of forces. Small, highly networked and collaborative entities will be capable of defeating larger and more powerful organizations."[8] Further, the Chief of Force Development's (CFD) Future Security Environment (FSE) document notes that "shortages in cyber experts, highly trained and motivated attackers constitute a growing threat to security."[9] Despite identifying these concerns, the Army has not committed resources to address this gap. This paper therefore, establishes the case for a Land cyber Intelligence capability that will

[5] United States, Department of Defence, "Cyber Intelligence Preparation of the Environment (CIPE)," Joint Publication 1-02, (CAF uses the exact same definition, CAF Cyber Effects V1.3, 10 Aug 15, 5A-1/3 refers).

[6] CAF Cyber Effects V1.3, 10 Aug 15, 5A-1/3.

[7] CAF defines the ASIC as "a task-tailored Intelligence unit that conducts Intelligence operations, analysis and administration," whereas a JIC is a staff responsive to the J2, and is not responsible for its own administration, nor can it conduct operations. Defence Terminology Bank Record #30440; and CFJP 2-0 refer).

[8] Directorate of Land Concepts and Designs, "Designing Canada's Army of Tomorrow: Land Operations 2021," (Kingston, Ontario, 2011), 23.

[9] Chief of Force Development, "Future Security Environment 2013-2040,"(17 Wing Publication Office, 2013), 72.

permanently address the Commander's Priority Intelligence Requirements (PIRs) to understand the cyber domain. To demonstrate the need that this new capability will address, this paper will use a task-based analysis, outlining the sources of Intelligence applicable to the cyber fight, as well as the effects Intelligence can achieve in the cyber domain. Lastly, it is important to note that because this is pre-doctrine, there are no established concepts or techniques, tactics and procedures (TTPs) to introduce.

## DISCUSSION

4. The Canadian Army currently does not have any means of planning, sharing or conducting cyber Intelligence activities. Intelligence plays a vital role in several of the key aspects of both offensive and defensive cyber action using an iterative four step process: Direction; Collection; Processing; and Dissemination. Furthermore, it contributes to the continued situational awareness (SA) and planning that drive all aspects of operations, be they offensive or defensive. According to technology giant Cisco, "global Internet traffic in 2019 will be equivalent to 64 times the volume of the entire global Internet in 2005," which means that CAF networks will face a massive increase in the amount of traffic they face, both legitimate and hostile.[10] Therefore, the need for an enduring CAF capability to understand and respond will only grow; especially if hostile actors are able to successfully compromise a DND network.

5. Based on a task-tailored model, this Cyber Joint Intelligence Center, (CJIC), would use the established concept of an organization that is specifically built to conduct: cyber Intelligence Preparation of the Environment (CIPE); cyber attack including penetration testing and targeting; defence; long-term all-source analysis of adversaries and their weapons; and Intelligence collection and tasking management. Table 1.1 outlines the source types leveraged and effects

[10] Cisco "Visual Networking Forecast Methodology Whitepaper, 2014-2019," http://www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white_paper_c11-481360.html. Accessed 11 Nov 15.

achieved by a cyber JIC.[11] It is important to note that the CJIC concept does not presuppose its size or recommend an effective manning strength to prevent influence over the subsequent – and critical – PRICIE+G analysis. Lastly, this paper describes the kinds of tasks in detail to aid follow-on analysis, by providing the clearest understanding of the problem.

## THE ROLES AND EFFECTS OF CYBER INTELLIGENCE

6. Cyber Intelligence Preparation of the Environment (CIPE). Like all environments, before CAF can operate in the cyber domain it must first understand the operating environment, and the features that exist on the physical, social and logical layers, which can transect land, air and maritime domains. Using all available sources of Intelligence such as: SIGINT; OSINT; HCI; IMINT; GEOINT; MET; HTT; and All-Source Analysis, the CIPE process follows the same four steps of traditional IPE, which are: Define the Cyber Environment; Describe the Cyber Environment's Effects; Evaluate the Cyber Adversary; and Determine the Cyber Adversary's Courses of Action. Beginning from an Open Source Intelligence base, CIPE builds the picture for the Cyber Operations Commander as part of the Initiation stage of the Operational Planning Process (OPP). The critical benefit to the Commander at this stage is the ability of Intelligence to determine who the cyber adversary is; what their capabilities and intentions are; and what infrastructure and tactics they use.[12] The Commander of US Fleet Cyber Command states, "Cyberspace is a unique domain with a totally different set of challenges. To operate

[11] The source types referred to herein include: Signals Intelligence refers to intercepted communications or emissions. Open Source Intelligence (OSINT) includes the Internet, social media, academics and commercial / public sources; HCI refers to Human Intelligence, Counter-Intelligence and Interrogation, which are all derived from human sources; IMINT is Imagery Intelligence and is acquired by photographic, radar, electro-optical, infrared, thermal, or multi-spectral sensors. GEOINT is the exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the earth. Accessed from: http://codes.lp.findlaw.com/uscode/10/A/I/22/IV/467, 11 Nov 15. Meteorological Intelligence includes all aspects of earth and space weather, and includes oceanography. Human Terrain Teams, (HTT) are employed to understand the population living in the operating environment, and the effects that operations have on them. All-Source analysis involves multiple independent types of reporting combined with structured analytical techniques to overcome the weaknesses and biases inherent in all source types. CFJP 2-0 refers.

[12] Although attribution of cyber acts is extremely difficult, Intelligence analysis provides assessments based on structured analysis, a wide range of sources and an evaluation of what will occur next.

successfully… we must first think differently about cyberspace operations."[13] This is significant because the complexities of the cyber environment are greater than any single domain as evidenced by the inextricable linkages between public, private and government infrastructures; as well as national, allied, neutral and adversarial spaces. Thus, to conduct operations or planning effectively, the Commander and staff must have a clear picture of where they can operate as well as the risks of doing so. The Canadian Army would have tremendous difficulty doing this today, and would require significant reorganization to achieve a limited effect because the greater capability is lacking.

7. Cyber Defence. Once the cyber environment is understood and defined, the Cyber Commander can properly develop a meaningful and comprehensive defensive plan. Dedicated All-Source analysts are required to fully understand all the threats, capabilities and end-states of the myriad of adversaries who operate against, on, and in CAF networks. With the full range of classified and open reporting available as well as advanced software tools, Intelligence analysts gain the understanding and detail on developing attack plans, their indicators, and range of weapons. These analysts also identify new trends and provide warning of changes in the cyber environment. The importance of this is providing attribution especially in low-intensity conflicts where opposition forces use false information on social media and internet sites to influence public opinion; inspire action among supportive elements; or simply undermine our credibility. Two common techniques used by adversaries are: *sock puppeting*; and *astro-turfing*. The former is a fictitious online propaganda tool that disseminates false opinions to create the sense of wider support or non-support; whereas astro-turfing is a more sophisticated and wide-spread effort using "bots" to prompt mass action.[14]

[13] CIPE, 1-5.

[14] Patrick M. Duggan, Colonel, "Special Warfare in Cyberspace," Joint Forces Quarterly 79, (4th Quarter, 2015), 51.

8. Cyber Attack. When ordered to do so, Intelligence would play a significant role in cyber attack through the targeting process as well as identifying the TTPs, tools and vulnerabilities of the adversary. Although cyber operations can affect the physical domain, most often they are against virtual and logical layers where high-value targets (HVTs), named areas of interest (NAIs), and targeted areas of interest (TAIs) are rapidly-changing networks, nodes and attack tools. Thus, whether the aim would be to physically destroy a piece of infrastructure used in the adversary's cyber network, or to degrade their capabilities, these target packages require specifically trained Intelligence professionals to vet and validate them to ensures the Commander is acting according to the Law of Armed Conflict (LOAC). One example of where Intelligence would play an even greater role is through penetration testing. The seven steps are: Pre-engagement Interactions; Intelligence Gathering; Threat Modeling; Vulnerability Analysis; Exploitation; Post-Exploitation; and Reporting.[15] In the first step, Intelligence Gathering, this is driven almost entirely by the Intelligence function and one where the CIC would play a vital role. Using the aforementioned sources, each would contribute to defining the characteristics, vulnerabilities and opportunities for attack. In the second step, which closely mirrors steps two and three of CIPE, where the environment's effects and the adversary's are taken into account. It is also key example of where cyber operators and Intelligence professionals would need to work closely to conduct reconnaissance of adversary networks, conduct port scanning and map the network. The "Threat Modelling" stage resembles CIPE steps three and four, which describe the adversary and his capabilities and options. Although much of Vulnerability Analysis is done by cyber operators, certain aspect such as passive data analysis, further research on the target; and validation of the data gained are tasks aided, or best performed by cyber-trained Intelligence

[15] "The Penetration Testing Execution Standard," http://www.pentest-standard.org/index.php/Main_Page, Accessed 14 Nov 15.

analysts. The role of Intelligence in steps five and six albeit reduced, does benefit greatly from the data collected, and does contribute to the final assessment of the penetration test in step seven. This final step, like the targeting cycle, ends with a ‘battle damage assessment’ that shows what the effects were on the adversary, as well as to identify any second and third order outcomes. The CA cannot currently conduct these activities because it lacks this capability.

9. Analysis. Like the trained, professional analysis required for CIPE; or Attack and Defence; *routine* cyber activity demands the same. The workload the comes from monitoring a global environment, as well as the details gained from the plethora of networks, nodes and even adversaries involved suggests that this cannot be staffed with only a handful of analysts. Furthermore, to anticipate and analyze trends, as well as the social / adversarial networks is also product cyber Int analysts would fulfil. The CAF’s current lack of dedicated, in-depth analysis of global cyber environment is analogous to the arrival of improvised explosive device (IED) exploitation teams in Afghanistan. Prior to the arrival of these teams, targeting and intelligence collection were done in a less focused manner, and even ad hoc. Once exploitation became commonplace; however, operations could then focus on the individuals and locations responsible for using and making these weapons. Lastly, the knowledge gained by these cyber analysis increases the benefits to the CA and its allies by building our collective experience, knowledge and TTPs. It also provides the entry point for allied cyber staffs to coordinate, plan and share related Intelligence with CA cyber Int staffs.

10. ISR Management. Another aspect lacking in the Army’s current cyber posture, is the ability to formally collect, track and disseminate cyber Intelligence. Although the Land Force Intelligence Center (LFIC) does provide the Commander of the Canadian Army (CA) with routine *ground* Intelligence, it does not have the training, mandate or resources to support him, or

forces he might generate for cyber operations. Thus, a cyber IC would manage the Requests for Information (RFI) relating to all cyber Intelligence issues, as well as provide an accountability mechanism through which CAF and allied assets could leverage the JIC's capabilities. Perhaps most crucially, it would conduct the Army's cyber ISR operations, to collect, understand and learn about areas the Commander deems to be of cyber importance.

## CONCLUSION

11. Canada, like all Western countries are currently under cyber attack. Army Intelligence is at the Preferred Manning Level (PML), and therefore any internal restructuring or reorganization to create a cyber JIC would not be possible without cutting one of its current lines of operation (LOO), or accepting an equal level of risk by not conducting another equally-important task. Second, once trained, resourced and committed to the cyber task, these PYs could not be re-rolled without further significant loss of institutional capability due to the required training and reconstitution. Lastly, because CAF, like its NATO allies are already under cyber threat, there would be significant risk if cyber Int resources were not permanently dedicated to this task. By creating this capability, CCA not only provides a valuable response to an urgent need, but also sends a strong signal to its allies and adversaries that Army networks are protected. Further, it would add or enhance the Army's ability to anticipate attacks, bolster its defence, enable targeting, learn about adversary TTPs, enable the adaptation and advancement of Army TTPs; and add accuracy to our actions. It would also give the Army the ability to coordinate and conduct operations with Allied Cyber Commands as well as other cyber formations within CAF – a capability that the Army does not currently have. Lastly, the spectrum of risk from cyber is growing, which will increase the requirement for the CCA to have a flexible response as it will be much more difficult due to attribution and political will to conduct decisive operations.

## RECOMMENDATION

12. This paper recommends that the Canadian Army create a cyber Intelligence capability because there is a critical operational requirement; based on a persistent and growing cyber threat.

# BIBLIOGRAPHY

Cisco “Visual Networking Forecast Methodology Whitepaper, 2014-2019,” http://www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white_paper_c11-481360.html. Accessed 11 Nov 15.

Department of National Defence. CAF Cyber Effects V1.3, Ottawa: DND Canada, 10 Aug 15.

B-GJ-005-000/FP-001, CFJP 2-0, Intelligence. Canadian Forces Experimentation Center, Apr 2009. http://publications.gc.ca/collections/collection_2010/forces/D2-252-2009-eng.pdf. Accessed 12 Nov 15.

Chief of Force Development, “Future Security Environment 2013-2040,” 17 Wing Publication Office, 2013.

Directorate of Land Concepts and Designs, “Designing Canada’s Army of Tomorrow: Land Operations 2021,” Kingston, Ontario, 2011.

Patrick M. Duggan, Colonel, “Special Warfare in Cyberspace,” Joint Forces Quarterly 79, (4th Quarter, 2015).

“The Penetration Testing Execution Standard,” http://www.pentest-standard.org/index.php/Main_Page, Accessed 14 Nov 15.

United States, Department of Defence, “Cyber Intelligence Preparation of the Environment (CIPE),” Joint Publication 1-02.