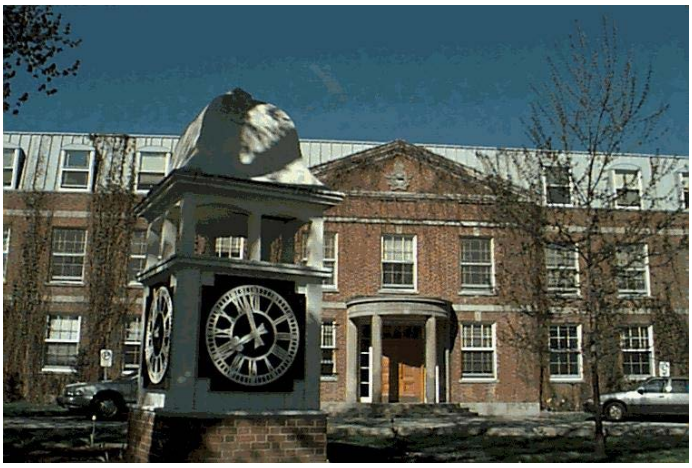
National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes



IMPROVING NATO DETERRENCE: CYBERSPACE IN NATO'S ENHANCED FORWARD PRESENCE

Lieutenant-Colonel Matthias-Michael Carl

JCSP 45

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 45

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

CFC COVER PAGE

CANADIAN FORCES COLLEGE/COLLÈGE DES FORCES CANADIENNES

JCSP 45/PCEMI 45

14 October 2018

DS 545/ Component Capabilities

"IMPROVING NATO DETERRENCE: CYBERSPACE IN NATO'S ENHANCED FORWARD PRESENCE"

By Lieutenant-Colonel Matthias-Michael Carl

Par le Lieutenant-Colonel Matthias-Michael Carl

Word Count: 2467

Nombre de mots: 2467

IMPROVING NATO DETERRENCE: CYBERSPACE IN NATO'S ENHANCED FORWARD PRESENCE

AIM

1. The aim for this service paper is to explore how cyberspace is included in North Atlantic Treaty Organization´s (NATO) deterrence posture and assurance measures by examining the Canadian Armed Forces (CAF) participation in NATO`s enhanced Forward Presence (eFP) through Op REASSURANCE (OpR). Using OpR as an example the document will inform on deterrence measures through conventional forces and NATO`s challenging task of achieving deterrence in the cyber realm. The discussion will present conventional and cyberspace deterrence, followed by a short summary of CAF OpR operational domains and conclude with presenting the challenges of cyberspace and the cyberspace policies of NATO and the CAF. Based on the CAF participation in eFP it will then outline recommendations on where the CAF should concentrate efforts to include and improve cyber operations in future operations.

INTRODUCTION

2. NATO collective defence. NATO`s collective security strategy is based on the principles of collective defence, crises management and cooperative security.[1] Nuclear deterrence is the backbone of NATO´s policy, but will not be considered as the focus will solely be on the deterrence through conventional forces and cyber. The illegal occupation and annexation of Crimea and the military intervention and aggressive actions in Ukraine in March 2014 by the Russian Federation took NATO by surprise. NATO`s focus on crises management and expeditionary operations had led to a neglected understanding of the collective security strategic concepts in general and concepts like deterrence and assurance. NATO needed to address the shortfalls in its military capabilities to deter an existential threat. This led to the creation of the enhanced NATO Response Force, with a Very High Readiness Joint Task Force spearheading any deployment, followed by the Initial Follow on Forces Group and later forces of the Response Force Pool of NATO would reinforce the force dispositive with the required command and control, combat and support units.[2] Concerns, that Russia might use hybrid warfare in one of the Eastern European NATO countries, were addressed by NATO through the development of the Readiness Action Plan (RAP) which foresaw an eFP in those countries. The military presence was aimed at assuring the eastern European NATO members of NATO´s full commitment to collective defence. Canada participates in NATO´s eFP with OPR in order to reinforce NATO´s collective defence and to demonstrate the strength of allied solidarity with up to 835 CAF members.[3]

---

[1] cf. North Atlantic Treaty Organization, Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation, Lisbon, 19 December 2010, last accessed 06 Oct 2018, https://www.nato.int/strategic-concept/

[2] cf. NATO, Supreme Headquarters Allied Powers Europe, NATO Response Force/ Very High Readiness Joint Task Force", updated April 2018, https://shape.nato.int/nato-response-force--very-high-readiness-joint-task-force

[3] cf. Government of Canada, National Defence and the Canadian Armed Forces, "Operation REASSURANCE", date modified: 26 Sept 2018, http://www.forces.gc.ca/en/operations-abroad/nato-ee.page

3. Cyber security. Based on Canada's Cyber Security Strategy of 2010 and 2018, "cyberspace is the electronic world created by interconnected networks of information technology and the information on those networks."[4] The importance of military command and control functions in combination with the development of information and communication technology, as well as the evolution of social media and its possible use by state and non-state actors made it clear that cyberspace would become a battlespace.[5] The threat of hostile cyber operations by state and non-state actors is not new, but the intensity and quality has increased significantly. Hostile operations aim to disrupt, to exploit or destroy existing cyber infrastructure. Russia`s cyber operations during the Ukraine crises underlined the significant challenges for the targeted country to counter and neutralize the attacks. Russia was able to infiltrate Ukraine`s critical infrastructure, impacting both energy distribution and defence networks.[6] NATO was also targeted during the crises and the analysis of the attacks highlighted a further gap in NATO`s crises management and defence mechanisms. Cyber security became a focal point of allied efforts. NATO worked on increasing the threat awareness and early warning mechanisms, improving its resilience to resist cyber attacks, and on developing capacities to respond in order to allow for a rapid decision-making process.[7]

DISCUSSION

4. Conventional deterrence. Deterrence can be defined as a "military strategy under which one power uses the threat of reprisal effectively to preclude an attack from an adversary power."[8] NATO now uses the term modern deterrence. The understanding is that a presence of multinational forces, on a rotational basis and supported by a programme of exercises, including infrastructure, pre-positioning of equipment to facilitate rapid reinforcements will deter Russia.[9] The approach chosen is to inform Russia of NATO`s intentions through the NATO- Russia Council, but also using the media to explain the intentions of the RAP. Publicly communicating allied solidarity by presenting the force posture being deployed in the eFP raises the awareness in Russia of the risks in interfering in allied member countries. NATO Article 5 is very clear that a military attack on one member will be considered as an attack against all members. In order to support NATO and to achieve the desired deterrence effect the Canadian government provided forces to NATO with OpR. The use of conventional forces also serves as a trip wire function for NATO in regard to a conventional aggressor.

---

[4] Government of Canada, Public Safety Canada, "Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada.", 2010, 2. and Government of Canada, Public Safety Canada, "National Cyber Security Strategy", 2018, p. 34, last accessed: 10 Oct 2018 at 1230h, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx

[5] cf. Mihai-Ștefan Dinu, "The 5th operational domain and the evolution of NATO`s cyber defence concept.", Annals: Series on Military Sciences. 2017; 9(2), p. 71

[6] cf. Sorin Dumitru, "The cyber dimension of modern hybrid warfare and its relevance for NATO", Europolity, vol. 10, no. 1, 2016, p. 17

[7] Ibid, p. 19

[8] Encyclopaedia Britannica, „Deterrence Political and military strategy", last accessed 09 October 2018 at 1100h, https://www.britannica.com/topic/deterrence-political-and-military-strategy

[9] cf. Robin Allers, "Modern deterrence? NATO´s Enhanced Forward presence on the eastern flank", "NATO and Collective Defence in the 21st Century: An Assessment of the Warsaw Summit", Routledge, 2017, p. 23, https://ebookcentral.proquest.com/lib/cfvlibrary-books/reader.action?docID=4809731&query=

5. Deterrence in cyberspace. In military operations the cyber domain transcends from the strategic to the tactical level and across all operational functions. Cyberspace is used by weapon system platforms, as well as command and control systems, civilian industries and critical infrastructure. These are all vulnerable to cyber operations and different entities are in charge of protecting them. The challenge to deter an opponent requires a holistic and partnered approach of civilian industry, national government organizations and NATO.[10] NATO Secretary General Stoltenberg stated that the Alliance had come to the agreement that a cyber attack on a NATO country could be regarded as an attack on all allies. The level or intensity of a cyber attack which would lead to a declaration of NATO Article 5 was intentionally left undefined.[11] The assumption is, that defining a required level might invite aggressors to stay below the publicly known threshold and thus prevent NATO from acting. Through the development of capabilities that will allow in-depth analysis of hostile actions, in order to clearly identify the point of origin and to safeguard the own capabilities, the resilience against any attack will be increased. NATO`s goal is to raise the risk for an adversary to a level at which they might become identified and so politically exposed to pressure by the world community, sot the risk of possible reprisals might prevent them from executing their attack.

6. Domains of operations. NATO`s deterrence posture makes use of the four agreed domains for military operations: sea, land, air and cyberspace.[12] Canada`s contribution to eFP through OpR uses conventional capabilities to support deterrence towards Russia and assurance to NATO allies.

a. Land component. The land component, in the form of a battlegroup pre-positioned in Latvia, provides the capability to train host nation forces and allied partners in order to increase mutual understanding and capabilities, to participate in joint and combined exercises and to present a multinational fighting capability in Latvia. The CAF contributions include headquarters staff, an infantry company with light armoured vehicles, military police, and logistical and communications support.[13]

b. Sea component. The sea component has consisted of seven different ships since the beginning of OpR. A frigate is currently deployed within the Standing NATO Maritime Group 2 providing training opportunities and cooperation with NATO partners and allies and non-NATO countries. The frigate prepared for operations in the Mediterranean Sea through integration and staff planning.[14]

---

[10] c.f. Melanie Bernier and Joanne Treurniet, „Understanding Cyber Operations in a Canadian Strategic context: More than C4ISR, more than CNO,", Conference on Cyber Conflict Proceedings, 2010, p. 231

[11] cf. Jens Stoltenberg, NATO Secretary General, Speech at the Cyber Defence Pledge Conference, last updated 15 May 2018, https://www.nato.int/cps/en/natohq/opinions_154462.htm

[12] cf. Klara, Jordan, „NATO Cyber Center: Implementing Recognition of Cyberspace as a domain of Operations, Atlantic Council, 14 Nov 2017, last accessed 10 Oct 2018at 1241h, http://www.atlanticcouncil.org/blogs/new-atlanticist/nato-cyber-center-implementing-recognition-of-cyberspace-as-a-domain-of-operations

[13] cf. Government of Canada, National Defence and the Canadian Armed Forces, "Operation REASSURANCE", date modified: 26 Sept 2018, http://www.forces.gc.ca/en/operations-abroad/nato-ee.page

[14] Ibid

c. Air component. The air component in the form of an air task force, conducts peacetime collective defence missions to safeguard the integrity of NATO airspace as part of the NATO enhanced Air Policing mission in Romania, Iceland and Lithuania.[15]

d. Cyberspace operations. Within the Canadian contribution to eFP, information on the cyber operation aspect could not be found in any of the available sources. This does not exclude that the capability is used or deployed, as information security is part of any military operation and details on any cyber capability might be classified.

7. Challenges of cyberspace. Several NATO member countries, like Estonia and other NATO partner countries, like Ukraine, have become victims of cyber attacks, which came allegedly from Russia or Russian proxies. The rapidly evolving technological advances within the cyber domain makes it challenging for organizations to adapt and develop concepts and doctrines. The challenges in cyber warfare are manifold, but to find the point of origin of a cyber attack and to identify which systems have been affected and how is critical for political decision making. On the other hand, contrary to conventional force on force engagements, the defence can be organized at any place which allows access to the affected networks. Recruitment, training and retention of personnel who have the required capabilities and expertise to deal with cyber operations is difficult, as militaries are in direct competition with civilian industry.

8. NATO cyber policy. Cyber was recognized as an operational domain during the NATO Warsaw Summit in 2016. NATO intensified its cooperation with partners like the European Union and industry to improve its cyber capabilities. The development of a NATO Computer Incident Response Capability (NCIRC) was a primary task aimed to protect NATO´s networks. NATO used the NATO Defence Planning Process in order to support allies in developing cyber capabilities. Estonia hosts the NATO Cooperative Cyber Defence Centre of Excellence that focusses on cyber defence research, education, consultation and development.[16] NATO will adhere to its guiding policy for collective defence, which is purely defensive and will not allow for offensive cyber operations.[17] All above mentioned efforts are supported by media work and press releases in order to inform the allied public. This ensures that possible adversaries will be aware of the capability, but ideally should stay in doubt on the details or the capacity.

9. Canadian cyber policy. Public Safety Canada is the lead body for cyber security in Canada. The Royal Canadian Mounted Police, the Canadian Security Intelligence Service and the CAF and the Communications Security Establishment agency under the Department of National Defence are part of the cyber security effort.[18] After the publication of the first National Cyber Defence Policy in 2010 the CAF established an ad-hoc Task Force Cyber, followed by an establishment of a Director General Cyberspace. The 2018 National Cyber Defence Policy advocates a Whole-of-Government approach and underlines the need for

[15] Ibid

[16] cf. NATO, Factsheet cyber defence July 2016, last accessed 10 Oct 18 at 1348h, https://www.nato.int/nato...07/20160627_1607-factsheet-cyber-defence-eng.pdf

[17] cf. Mihai-Ștefan Dinu, "The 5th Operational Domain and the Evolution of NATO´s Cyber Defence Concept", p. 76

[18] cf. N.B. Marshall, "Offensive cyber in the Canadian Armed Forces: Opportunities from Bill C-51", Joint Command and Staff Studies Course Paper, Canadian Forces College, 2016, p. 4

collaboration between Canadian governmental organizations, civilian industry and international partners.[19] The heavily debated Anti-Terrorism-Act with Bill C-51 might provide the Canadian government with opportunities to use defensive and offensive cyber operations inside Canada and possibly abroad, if Canada were threatened.[20] The requirement for a military cyber policy seems to be acknowledged by the leadership of the CAF, however clear division of tasks between the governmental organizations have yet to be defined.

CONCLUSION

10. Cyberspace has become a part of everyday military operations through networks from the tactical to the strategic level and in-between weapons system platforms. NATO`s forces rely heavily on command and control capabilities that are networked and multifaceted, and these networks are vulnerable to attack. The complex task of deterring potential opponents from executing their plans becomes even more complex in an Alliance framework. Cyberspace adds an additional layer of complexity. OpR provides conventional deterrence in support of NATO´s eFP, but misses the cyber security aspect. The challenge to including cyber is mainly due to a not yet matured cyberspace policy and capability within the CAF. Clear delineations of cyberspace operations between governmental organizations needs to be defined and implemented in policies and doctrines, as well as techniques, tactics and procedures at the operator level. Only aligned efforts at a national and multinational level will provide a robust capability over all domains and may serve as a deterrent for possible adversaries.

RECOMMENDATION

11. In order to deliver deterrence across the conventional and cyberspace, measures must be taken to integrate cyber more effectively in Canadas approach to NATO´s eFP. The following recommendations are aimed at improving the inclusion of cyber in Canada´s eFP operations, but will positively affect all CAF operations, not solely in a NATO context:

a. Cyber defence concept. The CAF should develop a military cyber defence concept in close cooperation with other government agencies in order to support a Whole-of-Government approach.

b. Adapting the force structure. The CAF should consider the development of a military cyber capability command, including the Canadian Forces Network Operations Centre (CFNOC), focussing on CAF networks and operational requirements in operations. This should be developed within the remit of the National Defence Act and in support and in close cooperation with the Communications Security Establishment and Public Safety Canada.

c. Multinational approach. Canada is a sponsoring nation in NATO`s Multinational Cyber Defense Capability Program. On this basis the CAF should investigate the possibility to of becoming a cyber NATO Framework Nation or join other NATO countries that would take the lead in the cyber domain.

[19] cf. Government of Canada, Public Safety Canada, National Cyber Security Strategy, (2018), p. 4-5
[20] Ibid., p. 5

d. Mobile Network Operation Centre. The development of a mobile military network operation centre would benefit the CAF. It should be deployable capability in order to protect CAF networks and to provide support to CAF operations, allied forces and civilian entities with cyber response teams.

BIBLIOGRAPHY

Bernier, Melanie and Treurniet, Joanne, "*Understanding Cyber Operations in a Canadian Strategic context: More than C4ISR, more than CNO*.", Conference on Cyber Conflict Proceedings, CCD COE Publications, 2010, Tallinn, Estonia, https://ccdcoe.org/publications/2010proceedings/Benier%20-%20Understanding%20Cyber%20Operations%20in%20a%20Canadian%20Strategic%20Context%20More%20than%20C4ISR,%20More%20than%20CNO.pdf

Dinu, Mihai-Ştefan,*"The 5th Operational Domain and the Evolution of NATO´s Cyber Defence Concept",* Annals: Series on Military Sciences. 2017; 9(2), p. 69-77

Dumitru, Sorin, "*The cyber dimension of modern hybrid warfare and its relevance for NATO*", Europolity, vol. 10, no. 1, 2016

Encyclopaedia Britannica, „*Deterrence Political and military strategy*", last accessed 09 October 2018 at 1100h, https://www.britannica.com/topic/deterrence-political-and-military-strategy

Friis, Karsten, "*NATO and Collective Defence in the 21st Century : An Assessment of the Warsaw Summit*", Routledge, 2017, https://ebookcentral.proquest.com/lib/cfvlibrary-ebooks/reader.action?docID=4809731&query=

Government of Canada, National Defence and the Canadian Armed Forces, "*Operation REASSURANCE*", date modified: 26 Sept 2018, http://www.forces.gc.ca/en/operations-abroad/nato-ee.page

Government of Canada. "*Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada.*", Ottawa, 2010

Government of Canada, Public Safety Canada, "*National Cyber Security Strategy*", (2018), last accessed, 10 Oct 2018 at 1230h, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx

Jackson, Nicole J., "*Canada, NATO and Global Russia*", International Journal, 2018, Vol 73(2), p. 317-325

Jordan, Klara, „*NATO Cyber Center: Implementing Recognition of Cyberspace as a domain of Operations*", Atlantic Council, 14 Nov 2017, last accessed 10 Oct 2018 at 1241h, http://www.atlanticcouncil.org/blogs/new-atlanticist/nato-cyber-center-implementing-recognition-of-cyberspace-as-a-domain-of-operations

Marshall, N.B., "*Offensive cyber in the Canadian Armed Forces: Opportunities from Bill C-51*", Joint Command and Staff Studies Service Paper, Canadian Forces College, 2016

Mearsheimer, John J., "*Deterrence*", Cornell Studies in Security Affairs, Harvard University, 1983

North Atlantic Treaty Organization, "*Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation*", Lisbon, 19 December 2010, last accessed 06 Oct 2018, https://www.nato.int/strategic-concept/

North Atlantic Treaty Organization, Supreme Headquarters Allied Powers Europe, "*NATO Response Force/ Very High Readiness Joint Task Force*", updated April 2018, https://shape.nato.int/nato-response-force--very-high-readiness-joint-task-force

Allers, Robin, "*Modern deterrence? NATO´s Enhanced Forward presence on the eastern flank*", "NATO and Collective Defence in the 21st Century : An Assessment of the Warsaw Summit", Routledge, 2017, p. 23 - 32, https://ebookcentral.proquest.com/lib/cfvlibrary-ebooks/reader.action?docID=4809731&query=