National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

BLACK HOODIES: CANADIAN RANGER MODEL FOR CYBER OPERATORS

Lieutenant-Colonel Christopher Stobbs

JCSP 50

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 n° 50

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 50 - PCEMI n° 50
2023 - 2024

Service Paper – Étude militaire

BLACK HOODIES: CANADIAN RANGER MODEL FOR CYBER OPERATORS

Lieutenant-Colonel Christopher Stobbs

BLACK HOODIES: CANADIAN RANGER MODEL FOR CYBER OPERATORS

AIM

1. The aim of this service paper is to look at the current force development model and employment model for cyber operators employed in the Canadian Armed Forces (CAF). I propose that a model similar to the one used to force generate and force employ Canadian Rangers will provide greater results in creating a military cyber capability that can accomplish military cyber tasks both domestically and abroad. The creation of a military cyber organization in metaphorical black hoodies symbolic of the red hoodies that Canadian Rangers don as part of their military uniforms. Cyber operators with the proper cyber training and expertise needed to support joint operations in the pan-domain battlefield.

INTRODUCTION

2. Cyberspace is defined as: "a domain framed by the use of electronics and the electromagnetic spectrum to capture or create, store, modify, exchange, and exploit information via interdependent and interconnected networks to produce kinetic and information effects."[1] Cyberspace is seen as being in its infancy, when described as a military domain in comparison to air, land and sea. The United States Department of Defence first began to recognize cyberspace as its own war domain in 2006.[2] Additionally, in 2016 at the Warsaw Summit, the North Atlantic Treaty Organization (NATO) identified cyberspace as a domain for operations.[3] Conversely, cyber threats within the cyber domain and its use within warfare began well before it was named as a cyber domain. It has provided the opportunity for nations to gain an advantage on the battlefield through a domain that can be persecuted from a distance with minimal resources and no resulting casualties. More specifically, Russia, China and others use the cyber domain to conduct malicious cyber activities just below the level of armed conflict to gain a strategic advantage.[4] Thus developed the need for militaries to have both offensive and defensive cyber capabilities to defend against and gain an advantage on the battlefield.

3. With the recognition of cyberspace as a domain and the threat that countries like Russia and China pose in the cyber domain came the need to create a military force structure with the applicable personnel capable of operating in cyberspace. The need for military operators with a specialization in the domain of cyberspace. Both the US and UK were recruiting and building military organizations tasked with managing cyberspace in

---

[1] Damien V Puyvelde, and A.F. Brantly. U*S National Cybersecurity: International Politics, Concepts and Organizations* (New York: Routledge, 2017).
[2] Ale Tesa, Fabian Baxa, and Dalibor Prochzka. "M.A.D. AGAIN? Shift of the Term M.A.D. to the Cyber Domain." *Obrana a Strategie 22*, no. 2 (2022): 42.
[3] Tesa, *M.A.D. Again*, 43.
[4] Richard A. Clarke, Robert K. Knake. *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats*. (New York: Penguin Press, 2019), 169.

2009 and 2013.[5] Cyber units have also been established by North Korea, Israel, China, India and Russia.[6] As with most new capabilities, the initial stand-up comes with the challenge of starting from scratch with limited training plans available. Additionally, recruiting members from other technical components of the CAF creates the domino effect of reducing the already limited pool of technical personnel needed to fill current established positions. Conversely, looking at drawing from new recruits when they first join creates the issue of limited initial capability until the recruits can be trained and have gained the experience necessary to operate within cyberspace.

4. Within Strong Secure Engaged, Canada's Defence Policy, the Canadian government outlined new initiatives to improve cyber capabilities within the CAF.[7] The new initiatives include the development of active cyber capabilities to use against adversaries in support of missions.[8] The creation of a cyber operator occupation and significantly increase the military personnel assigned to the cyber domain.[9] Lastly to use reservists with the required skill-set to augment to cyber force.[10] All great initiatives but centered around the premise that recruitment and retention within the cyber force will be steady, and that cyber specialists outside of the CAF will be receptive to the idea of joining as a reservist. More recently the Pan-Domain Force Employment Concept describes the threat our adversaries pose in the cyber domain, that the cyber domain is a less understood domain, but important to our success in a pan-domain battlefield.[11] More specifically it outlines the importance of using a whole of nation approach to the challenge of cyber by leveraging the expertise of academia, industry and innovators.[12]

DISCUSSION

5. The pathway to become a cyber operator involves numerous steps. First step upon enrolment is completion of basic military training. Next students are enrolled in a 15-month cyber course at the Willis College in Ottawa. Upon course completion they need to complete a 4-month course that builds upon the cyber training received at the Willis College and adds the additional job requirement of military cyber operator skillsets. Lastly, they are posted to the Canadian Forces Network Operations Centre where they are employed as cyber operators and further develop their cyber skills. The process produces cyber operators that have the basic knowledge and skills to perform, but lacks the ability to provide the operators tangible experience in the field that can only be gained overtime. Experience that is gained through the application of skills both in

---

[5] Lech J Janczweski and W. Caelli, *Cyber Conflicts and Small States* (Surrey: Ashgate Publishing Limited, 2016), 47.
[6] *Ibid*,, 47.
[7] Canada. Department of National Defence. *Strong Secure Engaged: Canada's Defence Policy*. (Ottawa, 2017), 73.
[8] Canada, *Strong Secure Engaged*, 73.
[9] *Ibid.,* 73.
[10] *Ibid.,* 73.
[11] Canada. Department of National Defence. *Pan-Domain Force Employment Concept: Prevailing in an Uncertain World* (Ottawa: CJOC, 2023), 19.
[12] Ibid., 21.

domestic and deployment opportunities. Additionally, the training gained by members makes them highly valuable outside of the CAF in jobs that provide greater financial incentives. Willis College advertises that its cyber training translates to job opportunities paying upwards of 45$ per hour.[13]

6. In order to tap into the expertise of cyber operators that currently work in the field I propose looking at the Canadian Rangers force development and force employment concept. Due to the extreme cold climate, low population density and the high operating costs needed to cover the massive size of the Canadian Arctic, northern Canada is seen as a difficult region to maintain and train a conventional military force.[14] The Canadian Rangers were created as a unique way to deal with Canada's difficult task of maintaining a military presence in Northern Canada. A grassroots military organization that ensures the CAF has boots on the ground in the north and is able to demonstrate sovereignty in the region.[15] Individuals from northern communities that already have the baseline skills and knowledge needed to operate in the north. Lieutenant Colonel Bob Keane expertly described the Canadian Rangers as a small slightly organized group with an interest to protect Canada through the use of their knowledge and expertise.[16]

7. The mandate of the Canadian Rangers as described in 1947 is to operate in locations where it isn't practical to employ Reserve Force units. A military entity with roles both in war and peace, but without all of the military training of regular of reserve force members. They only need to complete specific Ranger training required to help accomplish the tasks they are assigned as Canadian Rangers. They are not required to complete basic training or annual training. Due to their experience of living in the arctic, they have the skillset needed to manage the Canadian Ranger task of assisting military operations in the Arctic.

8. The force development model of the Canadian Rangers can be used to develop cyber force operators. Instead of developing individuals from the ground up with little to no experience, the CAF could look at members within the cyber operator community that have the skillsets needed but lack military experience. The force development model for these members would focus on the military training delta needed to accomplish the cyber operator tasks they would be required to accomplish. Instead of waiting 15 months to develop the basic knowledge necessary to function as a cyber operator then numerous years working at CFNOC to further develop those skills, these operators can begin their careers after completing only a finite amount of delta training, and still have the capability to accomplish meaningful tasks within the cyber domain. Cyber operators would remain employed in the cyber operator public sector and would surge in as

---

[13] Willis College. "CyberSecurity Operator." https://williscollege.com/programs/split-testing/cybersecurity-operator-program/

[14] P. Whitney Lackenbauer, *The Canadian Rangers @ 75: Key Documents, 1947*-2022 (Calgary: Centre for Military, Security and Strategic Studies, 2022), iii.

[15] Whitney, *The Canadian Rangers @75*, iii.

[16] P. Whitney Lackenbauer, *The Canadian Rangers: A Living History* (Vancouver: UBC Press, 2013), 57.

required to complete tasks within the cyber domain. Tasks would depend on the knowledge and expertise of the operator and their availability.

9. The key to developing a meaningful cyber capable doesn't lie in the purchase of the latest and greatest equipment.[17] The key to developing a meaningful cyber capability lies in recruitment, training and retention.[18] So how do you recruit individuals already working in cyberspace and making a descent wage? The recruitment centres around a few key things. First is flexibility in the employment model. The current model of recruitment into the reserve and regular force simply doesn't provide the flexibility needed to recruit skilled personnel already working in the public sector. Both the reserve force and regular force require a rigid commitment of time that doesn't always align with the professionals that would make ideal candidates as cyber operators. The Canadian Rangers model would provide flexibility by allowing candidates to remain employed while working as a cyber operator when convenient. The second recruitment benefit is the specialized opportunities that working in the military cyber force will provide in comparison to the public sector. By working with the military cyber organization personnel could be given the opportunity to take part in offensive cyber actions that aren't authorized in private industry. These unique opportunities that are only authorized in few instances are what sets working with the military apart from working for a private company.[19]

10. The current cyber operator model doesn't include the officer component. Officers normally fill cyber officer positions from the Army and Air Force communications community. Due to the additional responsibilities and authorities that are afforded to officers their path needs to be more deliberate and structured in comparison to cyber operators. They will need to have both the requisite technical and military expertise necessary to provide Commanders advice on the use of cyber to shape the battlefield. This type of responsibility simply can't be given to someone with years of technical training but no proper understanding of how the military works and the ramifications of cyber activities. As such the Canadian Ranger model would be limited to the force generation of cyber operators and not cyber officers.

11. The Canadian Ranger model as a force development and employment model does have its flaws. It lacks uniformity and its members lack the military experience that members within the regular force and reserve force have through the traditional military development stream. In order for the Canadian Ranger model to be successful, there needs to be diverse skillset by also including regular and reserve force members. When planning and executing tasks within the cyber domain, the inclusion of reserve and regular force members will ensure that not only the technical implications are considered but also the military implications. Secondly, an organization centered around personnel

---

[17] Max Smeets. 'The Challenges of Military Adaptation to the Cyber Domain: A Case Study of the Netherlands'. *Small Wars & Insurgencies* 34, no. 7 (3 October 2023): 1343–62. https://doi.org/10.1080/09592318.2023.2233159.

[18] Smeets, *The Challenges of Military Adaptation to the Cyber Domain*.

[19] *Ibid.*

with limited military experience might have difficulties integrating into military structures in war or peacetime. This type of integration is possible and is similar to the integration concerns when other domains are integrated into a pan domain effort. As long as planning and coordination is included in the battle rhythm then integration won't be an issue.

12. The Canadian Ranger model will also support future needs and requirements in the cyber domain. One of the keys to future success in the cyber domain revolves around collaboration. Sharing lessons learned in private industry and academia with the military helps in understanding current threats and vulnerabilities while prepare for future threats in the cyber domain. By recruiting professionals that are currently working in private industry, you gain additional knowledge and perspective that might not be seen simply working with regular force or reserve force members. This whole of nation approach is described in the Pan-Domain Force Employment concept as key to managing the constant threat that our adversaries pose.[20] Lastly, the Canadian Ranger model allows its members to continue to work in private industry and as a result they are able to continue to gain knowledge and expertise not otherwise gained within a military context. Continued growth and experience in the cyber domain through diverse experiences in the workplace.

CONCLUSION

7. The current force development model and employment model for cyber operators employed in the CAF is not ideal. The threats that our adversaries currently pose in the cyber domain and the future threats require cyber operators with the technical competence and skills gained not only though education but also through experience working in the cyber field. Unfortunately, in a domain like cyber that is in its infancy, it is difficult to gain work experience in a short period of time. A force development and employment model similar to the one used to force generate and force employ Canadian Rangers will provide greater results in creating a military cyber capability that can accomplish military cyber tasks both domestically and abroad. A military cyber organization in metaphorical black hoodies symbolic of the red hoodies that Canadian Rangers don as part of their military uniforms. Cyber operators with the proper cyber training and expertise needed to support joint operations in the pan-domain battlefield.

RECOMMENDATION

8. I recommend that the CAF looks at creating of military cyber organization in similar to the Canadian Rangers. Cyber operators with the proper cyber training and expertise needed to support joint operations in the pan-domain battlefield. Each operator would remain apart of the private sector in the cyber community, but would surge in to support cyber tasks both domestically and aboard as required. The organization would reside under the Command of a conventional force officer so that proper oversight and

---

[20] Canada. Department of National Defence. *Pan-Domain Force Employment Concept: Prevailing in an Uncertain World* (Ottawa: CJOC, 2023), 21.

direction can be provided to members within the organization. The cyber operators would have the flexibility to support based on availability and would only be required to complete delta military training vice traditional military training, including annual training. The cyber organization would also be augmented by reserve and regular force members that would follow the traditional recruitment stream currently being used to force employ and develop cyber operators. This will ensure there is diverse perspective and knowledge within the organization.

BIBLIOGRAPHY

Canada. Department of National Defence. *Pan-Domain Force Employment Concept: Prevailing in an Uncertain World*. Ottawa: CJOC, 2023.

———. *Strong Secure Engaged: Canada's Defence Policy*. Ottawa, 2017.

Clarke, Richard A., Robert K. Knake. *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats*. New York: Penguin Press, 2019.

Janczewski, Lech J and W. Caelli, *Cyber Conflicts and Small States*. Surrey: Ashgate Publishing Limited, 2016.

Lackenbauer, P. Whitney. *The Canadian Rangers @ 75: Key Documents, 1947*-2022. Calgary: Centre for Military, Security and Strategic Studies, 2022.

———. *The Canadian Rangers: A Living History.* Vancouver: UBC Press, 2013.

Puyvelde, Damien V, and A.F. Brantly. US National Cybersecurity: International Politics, Concepts and Organizations. New //York: Routledge, 2017.

Smeets, Max. 'The Challenges of Military Adaptation to the Cyber Domain: A Case Study of the Netherlands'. *Small Wars & Insurgencies* 34, no. 7 (3 October 2023): 1343–62. https://doi.org/10.1080/09592318.2023.2233159.

Tesa, Ale, Fabian Baxa, and Dalibor Prochzka. "M.A.D. AGAIN? Shift of the Term M.A.D. to the Cyber Domain." Obrana a Strategie 22, no. 2 (2022): 36-50.

Willis College. "CyberSecurity Operator." https://williscollege.com/programs/split-testing/cybersecurity-operator-program/