National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

CYBERFIGHTERS: NOT AFRAID OF NO GHOST

MAJOR TRAVIS HANES

JCSP 46

Service Paper

Disclaimer

PCEMI 46

Étude militaire

Avertissement

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES

JCSP 46 – PCEMI 46
2019 – 2020

SERVICE PAPER - ÉTUDE MILITAIRE

CYBERFIGHTERS: NOT AFRAID OF NO GHOST

Major Travis Hanes

Word Count: 2,635

Nombre de mots : 2.635

CYBERFIGHTERS: NOT AFRAID OF NO GHOST

... a glimpse of war's future: organized but crowdsourced, directed but distributed.
- *LikeWar.* Peter Singer and Max Brooking

If there's something weird and it don't look good, Who you gonna call?
- Original *Ghostbusters* Lyrics, Ray Parker Jr

AIM

1. Recommend a cyberfighter program be initiated in the CA. Analogous to the gunfighter program developed in the mid-2000s to meet close quarter combat deltas for the fight in Afghanistan, the initiative would be a *Mission Command initiative that jump starts and resources the tactical level.*

INTRODUCTION

2. Who We Are Facing. The Communist Manifesto begins with the sentence "A spectre is haunting Europe – the spectre of communism."[1] Though communism is dead as practiced in the first half of the 19th century, and exorcised with the fall of the Berlin Wall and U.S./China détente, its ghost roams cyberspace. Personified by our current neer-peer adversaries, it haunts western democratic society. The progenitors of a communist system responsible for the largest mass societal pogroms of the 20th century, both Russia and China have invested heavily in developing cyber capabilities capable of taking possession and control of our most sacrosanct institutions: free and fair elections, financial systems, and freedom of speech. These techniques are global, involve militarized organized crime and have the potential to spread far wider than the near abroad. Though class warfare has passed away, its spectre makes use of virtual societal warfare.[2] As Sir Rupert Smith, former Deputy Supreme Allied Commander Europe says"…we fight amongst the people. Literally, figuratively and virtually."[3] Though non-state actors such as terrorist groups and organized crime are also significant threats, we must be prepared to confront near-peer adversaries – not just on the conventional side – but in a cognitive domain that is manifesting itself in a virtual world. It is not coincidental that our primary adversaries evolved from a communist ideology, subsuming the individual within the group, and employing collectivist mechanisms of population control. These social manipulation techniques are well suited to exploit cyberspace.

3. Approach March. The threat cannot be overstated, and it is core business for the CA because the CA has the capacity, legitimacy and leverage to fight and fight hard within the cyber domain. It is as much a clash of ideals as arms. In contemporary society this plays out more and more in the borderless domain of cyberspace. The first step will

[1] Karl Marx. *The Communist Manifesto*. (New York: Enhanced Media, 2016), 1.
[2] Michael .J. Mazarr, Ryan Michael Bauer, Abigail Casey, Sarah Anita Heintz, Luke .J. Matthews. The emerging Risk of Virtual Societal Warfare: Social Manipulation In a Changing Information Environment. (RAND:2019)
[3] Rupert Smith. *The Utility of Force*. (London: Penguin, 2018), 433.

be to frame the problem of conflict, competition and confrontation within the cyber domain from both a cyber environment and adversary capabilities perspective. This will be followed by an examination of current Canadian joint cyber doctrine. The goal being to establish a rough division of labour between cyber operators and the CA cyberfighters responsible to patrol in combined cyber and physical domains - be it below the NATO Article 5 threshold or full-spectrum operations. With this in mind, this will naturally allow for a discussion of the utility of force and where the CA needs to prudently invest in the future, resulting in 5 recommendations for jump starting a cyberfighter program.

DISCUSSION

4. Problem Space: The Environment. All countries and their armies are struggling with developing a system to confront hostile social manipulation[4] in cyberspace. In LikeWar, Peter Singer describes the emerging conflict, where nations

> …fight to bend the global information environment to their will. The internet, once a light and airy place of personal connection, has morphed into the nervous system of modern commence. It has also become a battlefield where information itself is weaponized.[5]

This environment was created upon an architecture and instrumentation that is "primarily the result of service provisioning vice defensibility" and unable to adequately respond or detect adversarial activities.[6] These preexisting pressures produce the following characteristics:

a. Attribution. The inability to establish attribution of cyber-attacks or hostile social manipulation due to pervasive interconnectivity between friends and adversaries. The nervous system is systemic and exposed;

b. Low-cost entry. Operations in the cyber domain are inexpensive[7]. ISIS use of social media to attack the will of Iraq soldiers defending Mosul - leading to a full retreat and capture of the city - is a well-documented example of limited social media investment generating game changing outcomes;

c. Maintainance of technological overmatch. A competing but corollary trend with respect to low-cost entry will be the evolutionary tempo of technological advance, its high cost, and the ability to establish overmatch within the

[4] "Hostile Social Manipulation: the purposeful, systemic generation and dissemination of information to produce harmful social, political, and economic outcomes in a target country by affecting beliefs, attitudes, and behavior. Michael .J. Mazarr, Ryan Michael Bauer, Abigail Casey, Sarah Anita Heintz, Luke .J. Matthews. The Emerging Risk of Virtual Societal Warfare: Social Manipulation In a Changing Information Environment. (RAND:2019)XI.
[5] Peter Singer, Max Brooking. *LikeWar: The Weaponization of Social Media*. (New York: 2018) 46.
[6] Department of National Defence, *Joint Briefing Note: Cyber Operations*. (Ottawa: 2018) 1-1.
[7] Steve Winterfred, Jason Andreas. *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice* (Waltham: Elsevier, 2013) 15.

infosphere. As outlined in a recent final report co-chaired by the Mad Scientist Initiative and the Cockrell School of Engineering at The University of Texas, "…there is little space to patiently acquire and integrate increasingly rapid technological advances."[8]

d. Virality vs Veracity. The rules of influence within the cyber domain revolve around quantity and volume, that can be manipulated, supported and amplified through hostile botnets, but ultimately "social networks reward not veracity but virality. Online battles and their real-world results are therefore propelled by the financial and psychological drivers of the attention economy."[9] Viral memes carry payloads that excert overwhelming influence.

5. Problem Space: Adversary Capabilities. Any analysis of the problem space is incomplete without an understanding of how our adversaries will make use of the virtual space. Russian and Chinese government forays in the cyber domain telegraph their capability investments. On an Offensive Cyber Operation (OCO) side, Russian linked hackers attacked the Estonian financial and power network and targeted and triangulated Ukrainian civil and militaryover 3600 times.[10] In the infosphere specifically, Russia mix of avatars and botnets where successfully used during the 2016 U.S. election to sway public opinion.[11] On a Defensive Cyber Operations (DCO) side, China has established the Great Firewall, blocking their citizens from non-communist ideology. This is a critical indicator of intent, as LtGen Fogarty, Comd U.S. Army Cyber Command commented in a recent interview that "the defence is important. It actually gives you the ability to attack offensively."[12] Chinese DCOs are certainty not for the only purpose of setting the conditions for OCO against the West: it is foremost an internal virtual societal control mechanism. The legal and ethical thresholds for action are significantly lower and less demanding on kill chain processes for the Chinese. Current Chinese military doctrine is unequivocal: "War is accelerating its evolution to informatization."[13] As recently as June 2019, Chinese backed hackers conducted financial espionage against global telecommunication providers.[14] The four characteristics above are significant factors that must be taken into account prior to allocating investments in training or personnel.

6. Doctrine Review. An effect of a rapidly changing technological environment is the difficulty of doctrine to remain current. This effect has only compounded the confusion in terms and definitions surrounding the capabilities and trends within the

[8] Mad Scientist: "Disruption and the Future Operational Environment Final Conference Report" (Austin: 24 April 2019), 3.
[9] Peter Singer, Max Brookings. *LikeWar: The Weaponization of Social Media*. (New York: 2018), 46.
[10] Andy Greenberg, "How An Entire Nation Became Russia's Test Lab for Cyberwar," *Wired* (20 Jul 17) https://www.wired.com/story/russian-hackers-attack-ukraine/
[11] Mason Shuya. "Russian Cyber Aggression and the New Cold War." *Journal of Strategic Security* 11, no. 1 (2018): 4.
[12] "Ep. 84 – The future of Cyber Conflict, with Lt.Gen. Stephen Fogarty, Commander of U.S. Army Cyber Command," *The Modern War Institute,* Sep. 6, 2019
[13] Peter Singer, Max Brookings. *LikeWar: The Weaponization of Social Media*. (New York: 2018), 46.
[14] "Cyberwarfare Today." *Defence One Radio*, 12 Jul 19.

field.[15] Allied military publications alternatively highlight different capabilities and aspects of the digital domain under overlapping definitions.[16] That being said, the CAF cyber doctrine uses a taxonomy of mature, developing, conceptual framework. It is a start point for discussing where the CA can invest and build capabilities in the cyber domain, while allowing one to understand the uncertain ground they are on. The doctrine defines the cyber domain in five interconnected layers. Fig 1 depicts the layers and their interaction. This model is shared by Canada's allies; however, a few have an additional sixth 'social' that is contained in the Canadian Persona layer.

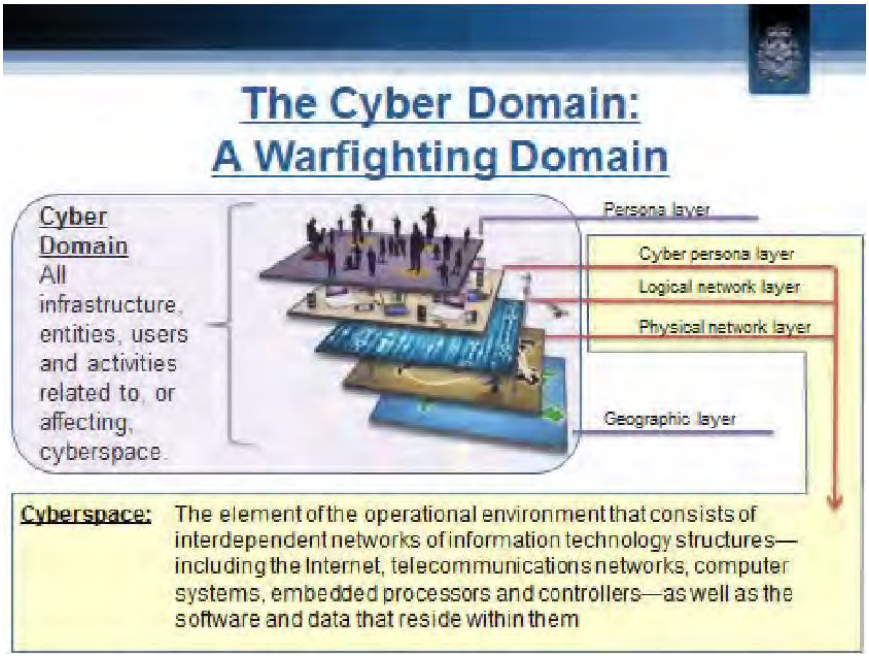

Fig 1. The Cyber Domain: A Warfighting Domain

Source: Canadian Armed Forces Joint Development Note: Cyber Operations

Though cyber officers conduct operations within all layers, it is in the persona and cyber persona layer where the CA can expect its soldiers to be patrolling, conducting operations, and fighting the virtual societal battles. The battles will consist of FakeNews, Botnets, Truth Decay and DeepFakes that manipulate the perceptions of CAF operations in the field. Within the persona layer, this can take place in two ways: (1) patrols can exist in the physical domain, yet layered with a virtual overlay only visual through augmented reality (AR) and depicting social media fields; or (2) patrols virtually through social media akin to investigative journalism as practiced by Bellingcat.[17] This patrol

[15] Brett Williams, "Cyberspace: What is it, Where is it, and Who Cares." *Armed Forces Journal*. (March 13, 2014) http://armedforcesjournal.com/cyberspace-what-is-it-where-is-it-and-who-cares/

[16] Steve Winterfred, Jason Andreas. *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice* (Waltham: Elsevier, 2013) 31.

[17] Bellingcat, https://www.bellingcat.com/

could be conducted prior to an insertion or infiltration phase, or could be a digital Named Area of Interest (NAI) until a cyber-operator with offensive capabilities turns it into a Targeted Area of Interest (TAI). This is the arena where the cyber persona layer is the complex area which includes avatars. Attribution is more difficult to establish requiring more sophisticated meta-data collection 'on the keyboard' able to program and implement a wide range of sophisticated algorithms.

7. CA Opportunity Space. There are many frameworks that categorize conflict in cyber domain: cyberwar, information warfare, virtual war, likewar, electronic warfare, virtual societal war, hybrid war, the list goes on. This has caused Col (ret'd) Steve Banach – former director of the U.S. Army SAMs and CO of the 75th Ranger Regiment - to comment that cyber terminology must be based in a military discourse framed around the contest of wills. In a SmallWars articles, he asks "What Virtual War non-standard doctrine and weaponry needs to be developed and fielded? When will our operators and agents be taught, armed and trained in their use?[18] This is a similar place that the CA finds itself, and within the problem space that it finds itself, it will be within the the CA has an opportunity now – before a doctrinal framework solidifies to take a crowdsourced and distributed training approach that generates critical mass through a bottom up reconnaissance patrolman mentality. The competitive advantage the CA has within this space is the volume of sensor/shooters and a high baseline warfighting standard to nest all cyber skillsets. This allows for both sousveillance[19] and surveillance at a scale above the capabilities of CAF cyber command, and interconnected with tradition army electronic warfare teams.

RECOMMENDATIONS

8. Armed with an understanding of the problem space, where cyber operations within CAF will focus its efforts, and an appreciation of the potential reconnaissance soldiers provide the CA, one can make initial recommendations. That being said, any recommendations in a field developing as rapidly as cyber warfare must be limited to conditions setting and not decisive action.

a. Recommendation 1: Patrolling Framework. Develop a virtual war nomenclature nested within preexisting army reconnaissance doctrine – regardless of army trade. This applies equally to armoured, infantry, engineer, FOO/FACs, signals, and logistics. This will ensure an iterative process that reinforces the coordination measures that make us successful: escalation-of-force, open-fire policy, ROE, emissions controls. This will decrease threat surface, while providing understandable control mechanism to mitigate risk. Each trade will add trade specificity, providing decision advantage to unit commanders or within a

[18] Steve Banach. Small Wars Journal 5

[19] "Sousveillance refers to the capturing of activity from "below," in such ways as capturing data on people's internet habits, recording their movements through cellphone locations, recording of audio by home-based sound-activated assistants." Michael .J. Mazarr, Ryan Michael Bauer, Abigail Casey, Sarah Anita Heintz, Luke .J. Matthews. The emerging Risk of Virtual Societal Warfare: Social Manipulation In a Changing Information Environment. (RAND:2019) 85

fusion cell. As Clausewitz remarked: "we shall not enter into any of the abstruse definitions of war used by publicists."[20]

b. Recommendation 2: Build Critical Mass. Initial implementation through Theatre Mission Specific Training (TMST) in deploying units. Concentrate the training in units that will reinforce it during deployment. The positive externalities of this approach is to concentrate and isolate expertise and apply it to below article 5 environments, while protecting the force and evolving tactics, techniques and procedures (TTPs). Finally, though the end-tour report these TTPs can be incorporated into training scenarios and non-standard professional development.

c. *Recommendation 3: Build a Cyberfighter Program:* From the cadre above build cyberfighter RSOs and ARSOs through civilian programs and organizations. This is analogous to the gunfighter program incorporation of urban operations instructors. In paragraph 6, it was noted that AR and the physical domain are simultaneous. The program should include technology like Microsoft HoloLens 2 so that headquarters can provide cyber enabler support to conventional patrols. Examples of this entrepreneurial experimentation exist in the CA. The current CO of the CAWC, LCol Aaron Luhning has been experimenting for a number of years with AR as a method for visualizing virtual social media within real world simulacrums.

d. *Recommendation 4: Decentralized Implementation.* Mission Command implementation of courseware and choice to the deploying units with the appropriate funding and delegation of financial authorities. They will be able to activate their college/university/NGO networks in their area or in cyberspace. Courses such as one's offered like bellingcat's soial media investigation course should be a priority.

e. *Recommendation 5. Connect the Synapses*. Unlike the U.S. Army, there is no intent to establish a cyber-component that nests within CFNOC. Within the cyber domain, the greatest risk to CA equities is within the social engineering where the attack vectors are through the wetware (people).[21] To reduce threat surfaces, bringing together all stakeholders (cyber operators and fighters, Intel, IA) and begin having professional symposiums with OGDs, NGOs, and universities. This will ensure dissemination of technical expertise to cyberfighters and commanders in order to mitigate strategic inversion.[22]

---

[20] Karl Von Clausewitz. *On War*.
[21] Steve Winterfred, Jason Andreas. *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice* (Waltham: Elsevier, 2013) 83.
[22] Brett Williams. "Cyberspace: What is it, Where is it, and Who Cares." *Armed Forces Journal*. (March 13, 2014) http://armedforcesjournal.com/cyberspace-what-is-it-where-is-it-and-who-cares/. In the article, the author defines strategic inversion as when "senior leaders become inappropriately engaged with the tactical and technical details to the detriment of effective decision-making."

CONCLUSION

9. In 2019, 49% of cyber operations conducted by the U.S. military were conducted by U.S. Armycyber.[23] The army is able to dominate the physical domain, generating the cyber responses. A clear challenge has been send by our adversaries; it is now the CA's time to frame a response. The recommendations are incremental in scope. They set the conditions through (1) establishing a cyberfighter lexicon nested in the patrolling spirit (2) a mission command startup approach (3) aggregating stakeholders periodically to ensure that the tactical and operational level capabilities align. Regardless of where the future operating environment takes us, the skills developed are applicable, contribute to overall readiness and increase our responsiveness to cyber threats. Ultimately, it is about decreasing the threat surface by increasing our force protection, and delivering decision advantage to commanders unaware of the spirits animating the infosphere. We should not be afraid of ghosts, but they should also not be in our houses.

[23] "Ep. 84 – The future of Cyber Conflict, with Lt.Gen. Stephen Fogarty, Commander of U.S. Army Cyber Command," *The Modern War Institute,* Sep. 6, 2019

BIBLIOGRAPHY

Books

Clausewitz, Karl. *On War*, Edited and translated. J.J. Graham. New York: Enhanced Media, 2016.

Marx, Karl.*The Communist Manifesto*. Edited and translated by Fredrick Engels, New York: New York Labour News Co, 1908.

Smith, Rupert. *The Utility of Force, Second Addition*. London: Penguin Press, 2018.

Singer, Peter, and Max Brookings. *LikeWar: The Weaponization of Social Media*. New York: HMH Publishing Co, 2018.

Winterfred, Steve and Jason Andreas. *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice.* Waltham: Elsevier Publishing, 2013.

Journals

Mazarr, Michael, Ryan Michael Bauer, Abigail Casey, Sarah Anita Heintz, Luke .J. Matthews. "The Emerging Risk of Virtual Societal Warfare: Social Manipulation In a Changing Information Environment." RAND:2019)

Shuya, Mason. "Russian Cyber Aggression and the New Cold War." *Journal of Strategic Security* 11, no. 1 (2018)

Electronic Sources

Banach, Steve. "Virtual War – A Revolution in Human Affairs." Small Wars Journal 5. https://smallwarsjournal.com/index.php/jrnl/art/virtual-war-revolution-human-affairs

"Ep. 84 – The future of Cyber Conflict, with Lt.Gen. Stephen Fogarty, Commander of U.S. Army Cyber Command," *The Modern War Institute,* Sep. 6, 2019. https://mwi.usma.edu/mwi-podcast-future-cyber-conflict-lt-gen-stephen-fogarty-commander-us-army-cyber-command/

"Ep. 48 - Cyberwarfare Today." *Defence One Radio*. 12 Jul 19. https://www.defenseone.com/ideas/2019/07/ep-48-cyberwarfare-today/158387/?oref=d-channelriver

Greenberg, Andy. "How An Entire Nation Became Russia's Test Lab for Cyberwar," *Wired* (20 Jul 17) https://www.wired.com/story/russian-hackers-attack-ukraine/

Lewis, Don. “What is NATO Really Doing in Cyberspace?” *War on the Rocks*. (Feb 4, 2019). https://warontherocks.com/2019/02/what-is-nato-really-doing-in-cyberspace/

Mad Scientist Initiative: “Disruption and the Future Operational Environment Final Conference Report” (Austin: 24April 2019) https://community.apan.org/wg/tradoc-g2/mad-scientist/m/disruption-and-the-future-operational-environment/287282

Williams, Brett. “Cyberspace: What is it, Where is it, and Who Cares.” *Armed Forces Journal*. (March 13, 2014) http://armedforcesjournal.com/cyberspace-what-is-it-where-is-it-and-who-cares/

Doctrine

Canada, Public Safety Canada. *National Cyber Security Strategy: Canada’s Vision for Security and Prosperity in the Digital Age*. Ottawa: Canada Communications Group, 2018.

Canada, Department of National Defence. JDN 2017-02. *Joint Doctrine Note: Cyber Operations Joint*. Ottawa: 2017.

Canada, Department of National Defence. *Strong, Secure, Engaged: Canada’s Defence Policy. Ottawa:2017.*