National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

DECENTRALIZED CYBER FORCES: CYBER FUNCTIONS AT THE OPERATIONAL AND TACTICAL LEVELS

Maj Howard Yu

JCSP 44

Exercise *Solo Flight*

PCEMI 44

Exercice *Solo Flight*

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.

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 44 – PCEMI 44
2017 – 2018

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

DECENTRALIZED CYBER FORCES: CYBER FUNCTIONS AT THE OPERATIONAL AND TACTICAL LEVELS

Maj Howard Yu

"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: 4526

"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: 4526

DECENTRALIZED CYBER FORCES: CYBER FUNCTIONS AT THE OPERATIONAL AND TACTICAL LEVELS

> *In the very near future many conflicts will not take place on the open field of battle, but rather in spaces on the Internet, fought with the aid of information soldiers, that is hackers. This means that a small force of hackers is stronger than the multi-thousand force of the current armed forces.*
>
> — Nikolai Kuryanovich, Russian State Duma deputy and member of the Security Committee, in 2006 letter of appreciation to hackers against Israeli websites, www.georgiaupdate.ge

INTRODUCTION

It is widely recognized that the era of cyber warfare has arrived. Our allies and adversaries have been busy building up cyber forces and honing their tradecraft for virtual war already taking place in cyberspace. The Canadian Armed Forces (CAF) is a relative newcomer to this domain; although the CAF has been conducting network operations—the set up, operation, and maintenance of information system networks—and defensive cyber operations (DCO) to protect them for some time, the idea of engaging in cyber warfare has not been accepted in Canada until more recently. On 3 November 2017, the CAF stood up the Cyber Operator occupation, [1] heralding the overdue establishment of a modern cyber warfighting capability. These developments, however, represent only the first steps to building a robust force that can meet the security challenges of the twenty-first century.

The initial CAF cyber organizations and command and control structures—namely the Cyber Force Commander, the Cyber Component Commander, and the Cyber Task Force—have been centralized at the strategic level, with limited tasks to support operational commanders for specific assigned missions, and rightly so. This approach allows the CAF to conduct deliberate

[1] Government of Canada, "Cyber Operator Occupation," last modified 3 November 2017, http://dgpaapp.forces.gc.ca/en/canada-defence-policy/themes/canada-new-vision-defence/cyber-operator.asp.

force development, to carefully build up the core competencies, tools and capabilities necessary to succeed in this highly complex, competitive and volatile battlespace. That said, the next logical step is to decentralize these forces and to embed them into the services and respective component commands, as there is not an element of the CAF that does not in some way operate in the cyber domain.

As the emerging CAF cyber operations doctrine notes, "There is growing recognition that cyber operations are required at decentralized tactical levels (ships, aircraft, vehicles, networks, etc.) where the networks and/or systems are not connected to centralized systems monitored by the cyber operations task force." Although immediate reaction teams have been employed to good effect on CAF operations—Operation IMPACT in Iraq and Operation UNIFIER in Ukraine—this is only an interim measure that must eventually be replaced by an integral capability.[2]

This paper will look ahead at this next bound of cyber force development and analyze the functions of a cyber force at the operational and tactical levels. It will examine where cyber capabilities are needed and how they can be integrated within a deployed joint task force or operational component command to provide force multiplying effects within a force employment context. It argues that the true payoff for a CAF cyber force will be realized at the operational and tactical levels, where it can protect our soldiers, sailors and aviators from the physical and psychological harm that malicious cyber attacks can cause. This paper will examine each component of the joint force according to the CAF's five operational functions—Command,

[2] Canada, Department of National Defence, JDN 2017-02, *Canadian Armed Forces Joint Doctrine Note: Cyber Operations* (Ottawa: Canadian Forces Warfare Centre, 2017), 6-3.

Sense, Act, Shield and Sustain—to identify some of the key terrain and functions that tactical cyber forces are critically needed to protect and fulfill respectively.

MARITIME COMPONENT

At first glance, the Maritime Component would be the least susceptible to cyber threats or attacks. It operates mainly in the open seas, far from the terrestrial cables and network infrastructure on which most of the Internet and the military information environment reside. Looking more carefully at how modern navies fight, however, one can quickly discern the extent to which the Navy is dependent on information systems and cyberspace for its command and control, intelligence, and protection, and even its engagement of targets.

Command

It is precisely due to their distance from fixed communications infrastructure that the Maritime Component is vulnerable to cyber warfare. It relies heavily on wireless and space-based communications for its command and control, which are inherently susceptible to interception, disruption or denial. In addition, the convergence of communications and information systems on board ships means that the vulnerabilities of one network are often shared with other networks operating within the same spaces or over the same channels. The Royal Canadian Navy (RCN) recognizes that space-based communications will remain vital to all maritime warfare disciplines, and their vulnerabilities will need to be mitigated in a contested space and electromagnetic spectrum environment.[3]

The Chinese People's Liberation Army (PLA), for one, trains and equips its forces to conduct integrated network and electronic warfare, interfering with and disrupting data links between terrestrial control stations and satellites. By hijacking a satellite's control systems or preventing ground control from issuing instructions, it is effectively neutralized.[4]

Sense

More often than not, the Maritime Component operates in busy commercial shipping lanes or in the littorals, necessitating strong situational awareness, or the Recognized Maritime Picture (RMP). The RMP depends on a vast network of shored-based, sea-based, and airborne sensors processing thousands of contacts daily. It also receives a large amount of self-reported information from Automated Identification Systems (AIS).[5] Disruption or denial of this network, or the spoofing of AIS signals, could have a significant impact on naval operations and a naval task group's (NTG) ability to identify friend from foe. A maritime cyber force could assist in safeguarding this network's integrity, identifying false data sources, and stopping the adversary's cyber attacks.

[3] Canada, Department of National Defence, *Canada in a New Maritime World: Leadmark 2050*, last modified March 2017, http://navy-marine.forces.gc.ca/assets/NAVY_Internet/docs/en/rcn_leadmark-2050.pdf, 54.

[4] Dean Cheng, *Cyber Dragon: Inside China's Information Warfare and Cyber Operations* (Santa Barbara, CA: Praeger, 2017), 167.

[5] NATO Review, "Keeping the Med safe – how it's done," accessed 7 May 8, 2018, https://www.nato.int/docu/review/2010/Maritime_Security/Safe_Mediterranean/EN/index.htm.

Act

Defending the network is also critical to enabling naval operations. Many of the Maritime Component's platforms and smart munitions depend on the network to function. As the RCN's strategy document, Leadmark 2050, recognizes, "Each 'node' in the joint force, from major platforms through unmanned and autonomous vehicles (UAV), down even to the level of individual munitions once launched, will need to 'plug into' the operational network."[6] If an adversary is successful in disrupting this network, the Maritime Component risks losing control of its UAVs, or worse, its guided missiles.

The physical dislocation and thin reach back channel of the Maritime Component's networks does not lend itself to central monitoring and necessitate a co-located cyber capability. An integral cyber force can monitor the naval task group's network activity in real-time and be able to take timely response actions to protect the Maritime Component's ability to act.

Shield

In the Maritime Component's context, the Shield function is closely linked with the Sense function in terms of ships' automated close-in weapon systems that protect it from incoming missiles or aircraft. System malfunction or misidentification of a ship or aircraft could have grave and tragic consequences in a theatre of operations. For example, in 1988 the Aegis cruiser USS *Vicennes* mistakenly shot down an Iranian airliner and killed 290 civilian passengers

[6] Canada, Department of National Defence, *Canada in a New Maritime World: Leadmark 2050*, last modified March 2017, http://navy-marine.forces.gc.ca/assets/NAVY_Internet/docs/en/rcn_leadmark-2050.pdf, 54.

and crew.[7] Equally chilling is the possibility of the adversary denying or disabling its air defence systems, which would leave the ship a sitting duck and vulnerable to attack.

Sustain

Not only are cyber operators required to sustain a ship's communications and information systems, they must ensure the integrity and availability of its many automated and computerized control systems. Many of these systems enable a ship to float, move and fight, including automated damage control systems, propulsion control systems, and weapon systems. Denial, disruption or manipulation of any of these systems could result in the "mission kill" of a vessel. A software error triggered by the entry of faulty data in a database in the USS *Yorktown* missile cruiser, for example, caused its propulsion control system to crash, leaving it "dead in the water for almost three hours."[8] Worse, false activation of the fire suppressions systems could irreparably damage a ship and knock it out of the fight.

Summary

Due to Maritime Component's distance from shore and the relatively thin channel through which it reaches back, cyber operations cannot be conducted centrally on its behalf. In addition, its advanced war ships have a myriad of communications, information and automated control systems that a non-sailor would have a difficult time understanding, let alone defending.

[7] Encyclopaedia Britannica, "Iran Air flight 655," accessed 6 May 2018, https://www.britannica.com/event/Iran-Air-flight-655.

[8] Peter G. Neumann, "Risks of Computer-Related Technology," in *Cyberwar, Netwar and the Revolution in Military Affairs,* eds. Dr Edward Halpin et al (New York: Palgrave Macmillan, 2006), 76.

Hence an integral, maritime cyber force is necessary for monitoring and defending the Maritime Component's digital systems that help its ships Float, Move and Fight.

The United States Navy, for instance, has already taken the step of creating a Fleet Cyber Command; furthermore, it is integrated with its 10th Fleet, consolidating the full spectrum of computer network operations, cyber warfare, electronic warfare, information operations and signal intelligence capabilities and missions across the cyber, electromagnetic and space domains.[9]

LAND COMPONENT

Similar to the Maritime Component's challenges in the littorals, the Land Component's need for a cyber force is even more pronounced. The ubiquity of cyberspace in the land domain presents both risks and opportunities for a land force. The availability of fast and cheap commercial communications infrastructure in many of the places where land forces operate, make it an attractive option for reach back and soldier welfare capabilities. Due to its proximity to the adversary, the potential for compromise of its computer systems is the highest out of all the components. At the same time, it provides touch points of the adversary's cyber networks, facilitating a level of knowledge and access to their physical, logical and cyber persona layers that a centralize cyber force cannot possess.

[9] United States, U.S. Strategic Command, "Navy Stands Up Fleet Cyber Command, Reestablishes U.S. 10th Fleet," last modified 29 January 2010, http://www.stratcom.mil/Media/News/News-Article-View/Article/983834/navy-stands-up-fleet-cyber-command-reestablishes-us-10th-fleet/.

Command

In addition to the obvious need to defend the Army's Land Command Support System (LCSS), integral cyber forces are needed to protect its mission-specific or stand-alone systems that cannot be monitored centrally. Systems such as the Remotely Operated Video Enhanced Receivers (ROVER) and Digital Gun Management Systems are critical to the Land Component's unmanned aerial vehicle reconnaissance and artillery functions respectively, but are separate from the LCSS network and need to be defended independently. The deployed Land Component headquarters represents a large, signal emitting target that adversaries would likely attempt to strike.

The land cyber force could also be called upon to protect Canadian commanders' credibility. In a society where the reputations of military officers has been besmirched by breach of trust and sexual harassment scandals, the credibility of the Task Force Commander must be unassailable. In response to information attacks such as the Russian propaganda against the Canadian task force in Latvia using photos of the cross-dressing Russell Williams, [10] a deployed cyber team would be required to disrupt or take down the website to limit its distribution or counter its message.

Conversely, land forces are generally within striking distance of enemy command and control systems and can apply kinetic means to achieve effects in cyberspace. Support cyber operations could identify, locate key commanders/personas and command and control nodes, and nominate targets as part of the intelligence collection and targeting processes. A cyber advisor,

[10] Chris Brown, "Anti-Canada propaganda greets troops in Latvia," *CBC News,* last modified 16 Jun 2017, http://www.cbc.ca/news/world/latvia-propaganda-1.4162612.

integrated into the Land Component Commander's staff, could advise on the adversary's critical vulnerabilities and nominate targets that would have the highest payoff against the adversary's command and control and information capabilities. In 2016 for example, British forces used its offensive cyber capabilities for the first time to jam phone and computer networks to disrupt Daesh's ability to command and control its defence of Mosul, leading to the successful liberation of that city.[11]

Sense

Support cyber operations could also contribute to the overall Intelligence function. Especially in a counter-insurgency operation requiring higher fidelity intelligence of individuals and insurgent networks, a tactical cyber operator could collect information from local Internet cafés or hotspots—the aptly named method of 'wardriving.' Similarly, the Russians have used cyber espionage in eastern Ukraine to gain location data from mobile phones and Wi-Fi networks that aided in targeting Ukrainian army units.[12] In addition, a deployed cyber operator could conduct digital forensics to glean even more information from captured cell phones or computers, alleviating the need to send it back to Canada for examination.

[11] David Willetts, "CYBER STRIKE HAVOC: Britain 'causing chaos' by jamming ISIS jihadis' mobiles and disrupting their computer networks," *The Sun*, last modified 21 October 2016, https://news.sky.com/story/british-military-carrying-out-cyberattacks-on-is-forces-in-mosul-10625959.

[12] Kenneth Geers, "Cyber War in Perspective: Russian Aggression against Ukraine," in Canada, Department of National Defence, JDN 2017-02, *Canadian Armed Forces Joint Doctrine Note: Cyber Operations* (Ottawa: Canadian Forces Warfare Centre, 2017), 4-17.

Act

Cyber attacks can also be synchronized with ground manoeuvres and used as a force multiplier. A precisely timed cyber attack could cripple an adversary's ability to communicate and hinder a coordinated response. In Russia's conflict with Georgia in 2008, for instance, they implemented a "cyber blockade" that was synchronized with the ground invasion, which prevented the Georgian government from coordinating its response and communicating with the international community and its population.[13]

Shield

Of key importance, a tactical cyber team will be essential to force protection. Deployed soldiers are the weakest link in the Land Component's cyber security, both in terms of endangering the Canadian Army's communications and information systems, and as targets themselves. The insider threat, both deliberate and inadvertent, remains the greatest risk to cyber security writ large. Hence training and auditing soldiers on cyber hygiene and preventing them from bringing threats into the network are a critical part of defensive cyber operations.

Furthermore, some adversaries would not hesitate to target our soldiers with cyber attacks directly. As such, the cyber force would need to protect our soldiers from phishing attacks, password theft, extortion, and other threats that could result from compromising their personal information.

[13] Alison Lawlor Russell, *Cyber Blockades* (Washington, D.C.: Georgetown University Press, 2014), 103-108. A cyber blockade is a situation rendered by an attack on cyber infrastructure or systems that prevents a state from accessing cyberspace, thus preventing the transmission (ingress and egress) of data beyond a geographical boundary.

Sustain

Applicable to the other components, but even more so for the Land Component, a cyber force needs to ensure that LCSS and other digital land control systems are patched and secured on a regular basis. The same applies to soldier systems, and even their personal devices, as they have a way of getting into the network, e.g. someone plugging their cell phone in to a CAF computer to charge.

Summary

Due to its proximity to the adversary's cyber networks and effects, the Land Component is at the greatest risk from, and has the greatest opportunity to leverage, cyber war capabilities. The Land Component's ability to affect the adversary's cyber infrastructure both physically and logically lends it a distinct advantage over the other components and the centralized cyber force in achieving objectives in cyber space and their attendant second and third order effects in support of the commander's plan. Therefore the development of a land cyber force should be considered as a matter of priority.

AIR COMPONENT

While the Land Component is the most susceptible to cyber attacks, it is the Air Component for which the impact of an effective cyber attack is the most severe. The Air Force is arguably the most dependent on advanced, digital technology, and therefore the most vulnerable to cyber aggression. Modern aircraft are comprised of highly sophisticated software to control everything from the flight management system to missile defence counter-measures. Many aviation disasters have resulted from poor design or errors in flight software, and in one case, malware on Spanair Flight JK 5022 led to a crash that killed 154 people.[14] A deliberate cyber attack could potentially have the same effect on our air platforms, disrupting their missions or causing combat casualties.

Command

Beyond the same issues of protecting its command and control networks, the Air Component's dependence on tactical data links makes it susceptible to cyber attacks. Link 16 in particular, although it was state of the art when it was first fielded, is now showing its age after more than three decades in operation. Older technologies, in general, allow hackers and advanced persistent threats (APT) more time to find vulnerabilities and develop exploits to be used at an opportune moment. Once compromised, the adversary could manipulate data on C2, intelligence, surveillance, and reconnaissance systems; inject false data into C2 networks and tactical data links; remove data from those links; or isolate systems from their associated networks.

Sense

The Air Component is also reliant on radar networks to produce its Recognized Air Picture. Similar to the problems with the RMP, but compounded by the problem of the high

[14] Best Computer Science Degrees, "10 Air Disasters Caused by Computer Errors," accessed 7 May 7, 2018, https://www.bestcomputersciencedegrees.com/10-air-disasters-caused-by-computer-errors/.

speed of air travel, the RAP is sensitive to the slightest disruption or distortions in the network. The Chinese PLA's information operations doctrine, for example, considers radar networks as priority targets and would employ an integrated network and electronic warfare approach to disrupt or neutralize these networks in support of local superiority for their forces.[15] Cyber forces are needed to ensure the integrity of the RAP and the Air Component's ability to tell friend from foe.

Act

In the air domain, cyber actions could likely produce physical results to devastating effect. Once control is gained, physical disruption or destruction is possible by manipulating the digital control systems of platforms such as satellites, remotely piloted aircraft, and fly-by-wire systems.[16] One such target would be the command-and-control links connecting operators in the Nevada desert to the MQ-9 Reapers circling the plains of Syria and Iraq.[17] Research into counter-drone technology, supported by the U.S. Defense Advanced Research Projects Agency, has already produced systems that can take over a drone, capturing its telemetry data and video feed, or tracking down its operator.[18] The compromise of an armed drone by hackers or advanced

[15] Dean Cheng, *Cyber Dragon: Inside China's Information Warfare and Cyber Operations* (Santa Barbara, CA: Praeger, 2017), 132.

[16] William J. Poirier and James Lotspeich, "Air Force Cyber Warfare: Now and the Future," *Air & Space Power Journal*, September-October 2013, 90. http://www.airuniversity.af.mil/Portals/10/ASPJ/journals/Volume-27_Issue-5/F-Poirier_Lotspeich.pdf.

[17] Patrick Tucker, "How the US Air Force is Rapidly Mobilizing for Cyber War," *Defense One*, last modified 22 September 2016, https://www.defenseone.com/technology/2016/09/how-us-air-force-rapidly-mobilizing-cyber-war/131746/.

[18] Paul Szoldra, "This company can 'hack' and completely take over enemy drones for the US military," *Business Insider,* last modified 6 January 2017, http://www.businessinsider.com/department-13-mesmer-drones-2017-1.

persistent threats could have severe consequences; hence the security of these assets, and the communication links and information systems that control them, is paramount.

Shield

Many other systems integral to air platforms also need to be defended from cyber attacks. Critical components such as position, navigation and timing (PNT) systems, avionics, embedded controls, flight planning systems, and many more provide numerous “attack surfaces” for the adversary.[19] Hence a vigilant mindset and an active defence in depth are even more important, especially when one considers that advanced persistent threats have already compromised many of these platforms’ designs, including the Joint Strike Fighter project.[20]

Sustain

Lastly, cyber warfare could affect the repair and maintenance of the Air Component’s platforms. The automatic test equipment commonly used to diagnose maintenance issues on complex, modern aircraft is a potential “line of attack” due to exploitable bugs or poorly defended systems, according to U.S. Air Force General Ellen Pawlikowski, who leads Air Force Materiel Command.[21] If compromised, these systems could hide or spoof error codes, which

[19] Patrick Tucker, “How the US Air Force is Rapidly Mobilizing for Cyber War,” *Defense One*, last modified 22 September 2016, https://www.defenseone.com/technology/2016/09/how-us-air-force-rapidly-mobilizing-cyber-war/131746/.

[20] Jason Andress and Steve Winterfeld, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners,* 2nd ed. (Waltham, MA: Elsevier, 2014), 47.

[21] Patrick Tucker, “How the US Air Force is Rapidly Mobilizing for Cyber War,” *Defense One*, last modified 22 September 2016, https://www.defenseone.com/technology/2016/09/how-us-air-force-rapidly-mobilizing-cyber-war/131746/.

would lead to no or incorrect maintenance being done on the aircraft and affect its air worthiness. In the worst case, it could result in the loss of the aircraft or even the death of its pilot(s), crew and passengers. Regular calibration and audits of the build version by cyber operators could ensure the integrity of the software and that it has not been tampered with.

Summary

Due to its reliance on digital technology, the Air Component is the most susceptible to cyber attacks, and the impact of such an attack could potentially be devastating. At the same time, the Air Force has the most technically competent personnel who are technology savvy and understand its value and its vulnerabilities. An Air Component cyber force would be more intimately familiar with the complex systems and technology in use on its various airborne platforms and would be much better equipped to identify vulnerabilities and defend against attacks from a determined adversary.

SPECIAL OPERATION FORCES COMPONENT

The Special Operation Forces (SOF) Component has similar cyber challenges and opportunities to the Land Component, just at a smaller scale. Its covert and mobile nature could enable physical access to an adversary's systems that no other component can achieve (at least surreptitiously), facilitating effects in cyberspace. However, this advantage is balanced by the risk and potential impact of discovery, which necessitate the protection of Special Operations Forces personnel's identities and cyber personas.

Moreover, the Special Operations Forces Component may be the most *culturally* adept at operating within cyberspace. Unlike conventional warfare, conflict in cyberspace is mostly ambiguous, obfuscated and non-attributable. The lines between defensive, support and offensive cyber operations are often blurred, and the same action could be considered any one of these types depending on the context and last key stroke. Such ambiguity defies clear rules and procedures, and requires a flexibility in thought and action that are similar to the characteristics of special operations. Special Operations Forces "are experts at exploiting the psychological, cultural, and societal factors that drive human behavior and are masters in unconventional warfare…and are better-adapted to counter adversaries in the 'gray zone.' [of cyberspace]."[22]

Command

To enable operational flexibility and freedom of manoeuvre, the Special Operations Forces Component espouses a culture of a flat hierarchy with very few hops between the commander and the operator. Combined with its independence from large support structures, the Special Operations Forces Component relies on space or readily available commercial communications means. Though encrypted, such communications could produce signatures that are detectable by advanced adversaries, reveal the presence of a Special Operations Forces team and/or the commander(s) with whom it communicates. A Special Operations Forces Component cyber operator could employ location and identity spoofing techniques to obfuscate and avoid detection by adversary cyber forces.

[22] Patrick Duggan, "Why Special Operations Forces in Cyber-Warfare?" *The Cyber Defense Review,* vol. 2, ed. 3, last modified 8 January 2016, http://cyberdefensereview.army.mil/The-Journal/Article-Display/Article/1136057/why-special-operations-forces-in-us-cyber-warfare/.

Conversely, a Special Operations Forces Component cyber force could attack a target's communications and/or security systems, especially at the critical timeframe before a breaching operation, denying the adversary early warning and the means to call for help.

Sense

Support cyber operations and computer network exploitation could support the intelligence gathering process and provide potentially rich and detailed information on a target based on his or her cyber persona(s). Infiltration of adversary systems to could also provide information of strategic value. In addition, integral cyber operators could enhance the exfiltration of data from a site exploitation by examining available digital sources, such as personal computers, servers, mobile devices, access control systems, and so forth.

Act

Like the Land Component, the Special Operations Forces Component could also employ cyber effects as a force multiplier. Similar to the British forces in Mosul, U.S. Cyber Command worked with their Special Operations Command to disrupt Daesh's propaganda machinery. Task Force Ares prevented Daesh's messaging by changing passwords on their social media accounts and deleting battlefield videos from YouTube.[23]

As well, the Special Operations Forces Component is uniquely capable of infiltrating and physically accessing adversary systems and networks. Special operations could be conducted to

[23] Dan Lamothe, "How the Pentagon's cyber offensive against ISIS could shape the future for elite U.S. forces," *The Washington Post*, last modified 16 December 2017, https://www.washingtonpost.com/news/checkpoint/wp/2017/12/16/how-the-pentagons-cyber-offensive-against-isis-could-shape-the-future-for-elite-u-s-forces/?utm_term=.a9b65364e82e.

physically deliver cyber payloads. This would overcome one of the key challenges in cyber tradecraft of jumping the air gap to the target network, which in many cases are closed networks separate from the Internet. An embedded cyber operator could more efficiently launch the payload, or destroy, disrupt, or manipulate the system directly. Alternatively, the system could be destroyed or removed, achieving an effect in cyberspace with a physical action.

Shield

The Special Operations Forces Component uses different systems from the conventional forces, and often employ commercial off the shelf (COTS) equipment, which are not as secure as military grade equipment, or their vulnerabilities are publicly known. As such, it is even more important for the Special Operations Forces Component to have integral cyber operators who are familiar with this equipment and can defend them effectively.

Integrating cyber functions within the Special Operations Forces Component could also minimize the collateral damage and unintended consequences of employing cyber weapons. The physical delivery of a cyber weapon, as previously mentioned, is a more precise and targeted attack on an adversary, whereas many cyber weapons can be arbitrary or indiscriminate in its spread. Although the Stuxnet worm, for example, was successful in reaching its target of the Iranian nuclear enrichment facility in 2010, it also infected an estimated 100 000 systems in the process.[24] A targeted, Special Cyber operation, on the other hand, could avoid this kind of collateral damage.

Sustain

Lastly, as Canadian Special Operations Forces Command also conducts its own force development, cyber expertise is required to ensure that new equipment, technologies and procedures are not compromised and are resistant to cyber attacks. They need to work with industry partners to ensure that each piece of equipment and its components are sourced from reliable suppliers, i.e. supply chain security. They also need to conduct testing of new capabilities to ensure that they cannot be disrupted or manipulated by advanced persistent threats or other threat actors.

Summary

The Special Operations Forces Component is the most similar in form and function to how the Cyber Component works. Their personnel are highly trained and specialized, and work in small teams in the 'gray zones' of conflict to achieve their objectives. The Special Operations Forces and Cyber components can and should be mutually supporting to multiply their effects in the physical, logical and psychological domains. A cyber force in the Special Operations Forces Component could assist in protecting its systems and facilitating strategic reconnaissance and direct actions; conversely, Special Operations Forces operators in Cyber Command could assist

[24] William D. Bryant, *International Conflict and Cyberspace Superiority* (Abingdon, U.K. and New York: Routledge, 2016), 151-156.

in resolving problems and taking action in a complex, ambiguous environment, especially during this nascent stage of Cybercom's development.

A CYBER PEARL HARBOR?

Despite the many examples of effective cyber warfare, there remain many who believe cyber war is a myth and doubt the possibility of a 'cyber pearl harbor,' an epic cyber attack causing widespread damage that would prompt a massive (kinetic) military response. These critics point to previous incidents like the cyber attack on Estonia in 2007 and argue that they were not as significant as a physical attack like the terrorist attack of 9/11. In the former case, a scientist at the NATO Co-operative Cyber Defence Centre of Excellence, which was established in Tallinn in response to that attack, has written that the immediate impacts of those attacks were 'minimal' or 'nonexistent', and that 'no critical services were permanently affected'.[25] Others argue semantically and point out that cyber war does not meet Clausewitz's criteria of being violent, instrumental, and politically attributed.[26] It cannot be called a war if no one is killed to achieve some political end.

While it is true that most cyber effects are non-persistent and leave no permanent damage, some can be persistent and devastating. The attack on Estonia lasted over twenty-one days, disrupting many government services, and shut down one of the major banking services in the country during that period. Although no essential services were targeted in this attack, other

[25] Sean Lawson, "Cyber Attack Scenarios and Evidence of History," in *Cyber Warfare: Critical Perspectives,* eds. Paul Ducheine, Frans Osinga, and Joseph Soeters (The Hague: Asser Press, 2012), 280.

[26] Thomas Rid, "Cyber War Will Not Take Place," in *Cyber Warfare: Critical Perspectives,* eds. Paul Ducheine, Frans Osinga, and Joseph Soeters (The Hague: Asser Press, 2012), 96.

cyber attacks have affected systems like 911 communications, hospitals, and nuclear facilities. Furthermore, the political message of Russia's displeasure over Estonia's removal of a Soviet monument was received loud and clear. At the individual level, the victims of the Ashley Madison hack, which revealed the names and addresses of many cheating spouses (including many military personnel), would definitely attest to the persistent and devastating nature of that effect.

This paper also provided many examples where, at the operational and tactical levels, a targeted cyber attack conducted at the right moment could cause deadly effects in the context of a military operation. So while cyber war is not the same as conventional, kinetic warfare, it is certainly an integral element of modern warfare that could be employed to advantageous and potentially deadly effect.

CONCLUSION

This paper has demonstrated that decentralized cyber forces at the operational level are a critical requirement for the CAF. It has described, though not exhaustively, the many functions that these cyber forces need to perform in order to enable the operations of the component commands, and to actively defend the numerous digital systems and system of systems that they operate. These examples show, in the words of General Raymond A. "Tony" Thomas III, the head of U.S. Special Forces Command, the "devastating effects on the adversary" cyber attacks can have when combined with traditional military operations. [27] They also show the potential

[27] Dan Lamothe, "How the Pentagon's cyber offensive against ISIS could shape the future for elite U.S. forces," *The Washington Post*, last modified 16 December 2017,

consequences of failing to mitigate security risks and shore up cyber vulnerabilities in our tactical platforms and personnel.

Although cyber forces at the strategic level has an important role in defending Canadian critical infrastructure, central planning, and liaison with other government department partners, they eventually need to be pushed down to the operational and tactical levels. Each service and component requires their own integral cyber force that is familiar with and can defend their unique systems and platforms, and understand their adversaries' systems and how to exploit their vulnerabilities. Otherwise, the CAF will remain vulnerable to cyber attacks from advanced persistent threats and other cyber threats in current and future operations. At the end of the day, safeguarding the lives of CAF soldiers, sailors and aviators on operations is the most important investment we can make.

https://www.washingtonpost.com/news/checkpoint/wp/2017/12/16/how-the-pentagons-cyber-offensive-against-isis-could-shape-the-future-for-elite-u-s-forces/?utm_term=.a9b65364e82e.

BIBLIOGRAPHY

Andress, Jason and Steve Winterfeld. Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners, 2nd ed. Waltham, MA: Elsevier, 2014.

Auman, Jerome R. "Cyber War Tactics or Clever Behavior: Understanding Cyber Deception Techniques in the Fight Against Cyber Warfare." Ann Arbor, MI: ProQuest LLC, 2014.

Bloomberg. "Britain Carried Out a Major Cyber-Attack Against ISIS in 2017." Fortune. Last modified 12 Apr 2018. http://fortune.com/2018/04/12/uk-isis-cyberattack/.

Bryant, William D. International Conflict and Cyberspace Superiority. Abingdon, U.K. and New York: Routledge, 2016.

Canada. Department of National Defence. Canada in a New Maritime World: Leadmark 2050. Last modified March 2017. http://navy-marine.forces.gc.ca/assets/NAVY_Internet/docs/en/rcn_leadmark-2050.pdf.

Canada. Department of National Defence. JDN 2017-02, Canadian Armed Forces Joint Doctrine Note: Cyber Operations. Ottawa: Canadian Forces Warfare Centre, 2017.

Cheng, Dean. Cyber Dragon: Inside China's Information Warfare and Cyber Operations. Santa Barbara, CA: Praeger, 2017.

Dotterway, Kristen Ann. Systematic analysis of complex dynamic systems: the case of USS Vicennes. Monterrey, CA: Naval Postgraduate School, 1992.

Duggan, Patrick. "Why Special Operations Forces in Cyber-Warfare?" The Cyber Defense Review, vol. 2, ed. 3. Last modified 8 January 2016. http://cyberdefensereview.army.mil/The-Journal/Article-Display/Article/1136057/why-special-operations-forces-in-us-cyber-warfare/.

Encyclopaedia Britannica. "Iran Air flight 655." Accessed 6 May 2018. https://www.britannica.com/event/Iran-Air-flight-655.

Gould, Joe. "Former NSA Chief: Follow SOCOM Model for Cyber." Defense News. Last modified 15 April 2015. https://www.defensenews.com/opinion/intercepts/2015/04/17/former-nsa-chief-follow-socom-model-for-cyber/.

Lawson, Sean. "Cyber Attack Scenarios and Evidence of History." In Cyber Warfare: Critical Perspectives. Edited by Paul Ducheine, Frans Osinga, and Joseph Soeters, The Hague: Asser Press, 2012.

NATO Review. "Keeping the Med safe – how it's done." Accessed 7 May 2018. https://www.nato.int/docu/review/2010/Maritime_Security/Safe_Mediterranean/EN/index.htm.

Neumann, Peter G. “Risks of Computer-Related Technology.” In Cyberwar, Netwar and the Revolution in Military Affairs, edited by Halpin, Edward, Phillippa Trevorrow, David Webb, and Steve Wright, 72-81. New York: Palgrave Macmillan, 2006.

Poirier, William J. and James Lotspeich. “Air Force Cyber Warfare: Now and the Future.” Air & Space Power Journal, September-October 2013, 73-97. http://www.airuniversity.af.mil/Portals/10/ASPJ/journals/Volume-27_Issue-5/F-Poirier_Lotspeich.pdf.

Rid, Thomas. “Cyber War Will Not Take Place.” In Cyber Warfare: Critical Perspectives. Edited by Paul Ducheine, Frans Osinga, and Joseph Soeters, The Hague: Asser Press, 2012.

Russell, Alison Lawlor. Cyber Blockades. Washington, D.C.: Georgetown University Press, 2014.

Slabodkin, Gregory. “Software glitches leave Navy Smart Ship dead in the water.” GCN.com. Last modified 13 July 1998. https://gcn.com/Articles/1998/07/13/Software-glitches-leave-Navy-Smart-Ship-dead-in-the-water.aspx.

Szoldra, Paul. “This company can 'hack' and completely take over enemy drones for the US military.” Business Insider. Last modified 6 January 2017. http://www.businessinsider.com/department-13-mesmer-drones-2017-1.

United States. FM 3-38, Cyber Electromagnetic Activities. Washington, D.C.: Department of the Army, 2014. https://armypubs.us.army.mil/doctrine/index.html.

United States. Joint Publication 3-12 (R), Cyberspace Operations. Joint Chiefs of Staff, 2013.

United States. U.S. Fleet Cyber Command/TENTH Fleet. Strategic Plan 2015-2020.

Walsh, Edward J. “Navy postmortem tries to pinpoint what went wrong with the 'Smart Ship'.” Military & Aerospace Electronics. Last modified 1 Mar 2001. http://www.militaryaerospace.com/articles/print/volume-12/issue-3/news/navy-postmortem-tries-to-pinpoint-what-went-wrong-with-the-smart-ship.html.