National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

DEVELOPING THE CAF CYBER CAPABILITY: THE NEED TO INTEGRATE THE RESERVE

LCol Malcolm Day

JCSP 43 DL

Exercise *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.

PCEMI 43 AD

Exercice *Solo Flight*

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 43 DL – PCEMI 43 AD
2017 – 2018

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

DEVELOPING THE CAF CYBER CAPABILITY: THE NEED TO INTEGRATE THE RESERVE

LCol Malcolm Day

Word Count: 3215

Compte de mots: 3215

DEVELOPING THE CAF CYBER CAPABILITY: THE NEED TO INTEGRATE THE RESERVE

Over the last few years, the pace of technological change in society has accelerated, and many facets of society have become increasingly dependent on the flow of data, and the supporting electronic data systems and networks that facilitate this flow. In most developed nations, industry, finance, and government have all reached the point where they simply cannot function without data networks. As data networks have proliferated and dependence on them has grown, so too has the ability of various actors to attack, breach and exploit these data systems. The news has been rife with incidents of critical network breaches, and many who depend on these networks have been slow to realize and defend the vulnerabilities of these networks. This trend also applies to governments and the defence sector. As dependence and vulnerabilities have increased, many nations have been rushing to develop cyber capabilities, both to defend their own networks, and to attack and exploit those of their adversaries. Canada is no exception. Cyber is uncharted territory to a great extent however, and the Canadian Armed Forces have been slow to create a cyber capability to keep up with both allies and adversaries. Cyber is a challenging and expensive capability to force generate. Much of the expertise in Canada is resident in industry, with people who would not normally be attracted to the CAF by virtue of the nature and restrictions of military service and compensation, or in the civilian skill sets of Reservists. In recent years however, the CAF has been fundamentally ineffective at developing, equipping and employing its Reserve Force (Res F), and currently has no effective mechanism to track and exploit the civilian skills of its members. This paper will demonstrate, through the examination of industry and allied practices, that the development of an effective cyber capability will only be successful and sustainable in the long run, through the development of a robust cyber force within the reserve components. This will require a fundamental change in the vision for, and terms of service and employment of the CAF Reserve, if it is to have any real chance of success.

If one looks at the news today in virtually any country, one will see stories of attacks on corporate or government data networks, and will hear the term cyberspace used frequently. Cyberspace as a definition can mean different things to different people and sectors however. In to order to set a common definition for discussion purposes, it useful to look to Ridout, who defines cyberspace as: "a global 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] Ridout goes on to define kinetic effects as physical outcomes or motion or impact as a result of networks or systems that command physical machinery or adjust energy flows in human systems, while information effects are those produced by systems or networks whose primary purpose is knowledge or storage, sharing or communication, that is of direct use to humans as information or sensory input. Ridout also points out that the internet and cyber space are not the same thing, but that the connected networks of the internet are simply one of the most common means of transferring data within cyberspace, and others do exist.[2]

In order to then understand the threats that use of cyberspace present, one can look at the proliferation and influence of systems that exist in cyberspace in the daily lives of increasing percentages of the world population. The entire world financial system, including all banking, property ownership, and industrial production and commerce is reliant on information networks. Most critical public infrastructure including transportation, hospitals, policing, and food

[1] Tim Ridout, "Building a Comprehensive Strategy of Cyber Defense, Deterrence, and Resilience," *The Fletcher Forum of World Affairs* 40 (Summer 2016): 65.

[2] Ridout, 65.

distribution are heavily dependent on electronic communication and data networks, while energy, water and utility systems are completely reliant on both electronic data networks, but also networked supervisory control and data acquisition (SCADA) equipment, or controllers, that operate the physical machinery. The Internet of Things (IoT) is the growing trend of connecting physical devices that have kinetic effect to the Internet, particularly in consumer categories. Of course, there one must also take into consideration the increasingly wide spread use of mobile telecommunications. Many of these networks use cellular communications technologies to move data over distances and to remote areas not serviced by landlines, and older physical telephony systems that have redundancy and physical backups built in are being phased out. People now use handheld communications devices that have arguably thousands of multiples of the computing power that NASA used to launch spacecraft in the 1960s.[3] These devices have become some ubiquitous that people conduct much of their daily lives on them, including accessing many of the critical systems above, such as banking, without truly understanding the mechanics of their devices, or the risks inherent in mobile communications.[4]

Where there are networked systems, there are attempts to access or "hack" them and create disruption, either through data theft, denial of service, ransom for service, or outright sabotage. In 2017, estimates put US consumer losses to fraud and identity theft, much of through cyber activity, at more than $16 Billion.[5] There have been many famous examples of this, and

[3] Tibi Puiu, "Your Smartphone Is Millions of Times More Powerful That All of NASA's Combined Computing in 1969," *ZME Science* (blog), October 13, 2015, https://www.zmescience.com/research/technology/smartphone-power-compared-to-apollo-432/.

[4] Stacy Collett, "Five New Threats to Your Mobile Security," CSO Online, August 1, 2017, https://www.csoonline.com/article/2157785/data-protection/five-new-threats-to-your-mobile-security.html.

[5] Kelli B. Grant, "Consumers Lost More than $16B to Fraud and Identity Theft Last Year," accessed May 29, 2018, https://www.cnbc.com/2017/02/01/consumers-lost-more-than-16b-to-fraud-and-identity-theft-last-year.html.

many companies have been slow to react, as in the case of Target Corporation, which suffered multiple data breaches through the same vulnerability[6]. Additionally, the Commission on the Theft of US intellectual Property estimates the 2017 losses to the US economy reach at least $600 Billion.[7] Extrapolating, the impact globally could be reaching more than $1 Trillion.

Governments are also affected by cyber risk. Confidential employee and taxpayer data is at risk, which can then be leveraged for further criminal exploitation. Both the US Internal Revenue Service and the Office of Personnel Management have suffered recent data breaches that have allowed straight fiscal theft from the US government, but have also opened millions of US Government (USG) employees to follow on espionage attempts.[8] In Canada, the Government of Canada (GoC) has suffered breaches across multiple departments, either through employee error or criminal intent,[9] such that, as of 2018, the GoC has implemented mandatory breach notification policies.[10]

As departments of government, Defence and Security agencies are also heavily influenced by the cyber threat, both via their own data systems and in the operating environment.

[6] Xiaokui Shu et al., "Breaking the Target: An Analysis of Target Data Breach and Lessons Learned," *ArXiv:1701.04940 [Cs]*, January 17, 2017, http://arxiv.org/abs/1701.04940.

[7] Paul Wiseman, "Counterfeiters, Hackers Cost US up to $600 Billion a Year," Phys.org, February 27, 2017, https://phys.org/news/2017-02-counterfeiters-hackers-billion-year.html.

[8] Brendan Koerner, "Inside the OPM Hack, the Cyberattack That Shocked the US Government," WIRED, accessed May 29, 2018, https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/; Elizabeth McKee, "IRS Data Breach Allows Hackers to Steal $30 Million from Taxpayers," Americans for Tax Reforms, accessed May 29, 2018, /irs-data-breach-allows-hackers-steal-30-million-taxpayers.

[9] Dean Beeby, "Revenue Canada Privacy Breach Leaks Prominent Canadians' Tax Details | CBC News," CBC, November 25, 2014, http://www.cbc.ca/news/politics/canada-revenue-agency-privacy-breach-leaks-prominent-canadians-tax-details-1.2849336; Dean Beeby, "Almost 13,000 Federal Employees' Salaries Exposed by Privacy Breach at Public Services | CBC News," CBC, June 2, 2017, http://www.cbc.ca/news/politics/privacy-breach-therrien-public-services-procurement-spreadsheet-personal-workers-1.4141297.

[10] Josh O'Kane, "Federal Government Debuts Data-Breach Reporting Rules," accessed May 29, 2018, https://www.theglobeandmail.com/business/article-federal-government-debuts-data-breach-reporting-rules/.

According to a senior USG Cyber advisor testifying before the Senate Armed Services Committee, over 100 foreign intelligence services and other actors currently make millions of probes or attempted incursions to US Defense networks each day.[11] Analyses of future operating environments by Canada, Australia, and the UK, all indicate that the proliferation of technology, and the growth of various networks, both technical and human, will greatly complicate future operations. On one hand, military reliance on technical equipment, weapons, and data and GPS networks will create risks to operational capability in the event of network breach or disruption. On the other, the easy access to increasingly inexpensive and sophisticated technologies will allow both state and non-state actors to leverage their capability far beyond their nominal military power, through "weaponization" of multiple technologies (e.g. cellular triggered IED, drones), illicit gathering and movement of funds, and secure communications.[12] All of these factors will serve to increase the complexity and potential cost of military operations, in both blood and treasure.

It is worth noting at this point, that the issue of cyberspace activities used in conjunction with military and other actions has given rise to increased focus on the concept of hybrid warfare. The example of Russian use of cyber network attack, misinformation, diplomatic posturing and both covert and overt military action in the annexation of the Crimea and conflict in eastern Ukraine has not only alarmed western nations, but has caused a great deal of analysis

[11] William Matthews, "Military Battles to Man Its Developing Cyber Force," GovTechWorks by General Dynamics IT, n.d., https://www.govtechworks.com/military-battles-to-man-its-growing-cyber-force/#gs.ukQkiDM.

[12] Australia. Department of Defence, "Future Operating Concept 2035" (Vice Chief of Defence Force, 2016), https://www.cove.org.au/wp-content/uploads/2017/03/Future-Operating-Environment-2035.pdf; United Kingdom. Ministry of Defence, *Global Strategic Trends: Out to 2045* (Swindon: MoD, 2014); Canada. Department of National Defence, *The Future Security Environment 2013-2040* (Ottawa: Chief of Force Development, 2014).

in NATO and military academic circles.[13] The US federal investigation into allegations of Russian employment of cyber activities to influence election results has only fuelled this concern.

The issue of cyber has such significance to defence, that in the 2009 Integrated Capstone Concept, the Department of National Defence (DND) labeled cyberspace as a military operational domain, the fifth domain, stating that "[t]he cyberspace domain will be a mechanism for integrating all of the domains at the strategic level resulting in one common operational picture. This functionality will be complemented by the facility of the cyberspace domain to merge the strategic functions, producing integrated effects."[14]

It goes on to say however, that:

> Cyberspace has unique vulnerabilities. Accessible and affordable technology has made this the easiest domain for adversaries to exploit. In this domain, the distinction between criminal activity and threat to national security can be difficult to ascertain. Cyberspace recognizes no borders; servers located in neutral or friendly nations can be used by an adversary to conduct cyber attacks. The temporal aspects required to conduct cyber defence are extremely compressed. A continuing challenge will be to ensure our policy and doctrine keep up with the pace of change in the cyberspace domain.[15]

[13] Şafak Oğuz, "The New NATO: Prepared for Russian Hybrid Warfare?," *Insight Turkey* 18, no. 4 (Fall 2016), https://www.insightturkey.com/cyber/the-new-nato-prepared-for-russian-hybrid-warfare; Dr. Patrick J. Cullen and Erik Kjennerud-Reichborn, "MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare" (Multinational Capability Development Campaign, 2017 2016).

[14] Canada. Department of National Defence, *Integrated Capstone Concept* (Ottawa: Chief of Force Development, 2009), 28–30, http://publications.gc.ca/collections/collection_2012/dn-nd/D2-265-2010-eng.pdf.

[15] Canada. Department of National Defence, 30.

In order to address the threats, and opportunities that the growth of the cyberspace domain present, following the example of many of our principle allies, DND has decided to establish a internal cyber capability. In 2011, the VCDS directed the establishment of a Cyber Task Force (Cyber TF). Recognizing that several cyber-related capabilities already existed within the CAF, The Cyber TF was tasked with examining current and future DND/CAF Cyber capabilities, develop operating concepts, design the DND/CAF capability set and governance structures, and provide pan-organizational coordination and leadership to all cyber issues. Since that time, work has been progressing, and a Director General Cyber was established under Chief of Force Development (CFD). In 2014, CFD released the CAF Cyber Force Development Program (CFDP), which laid out a road map and mission for development of an operational cyber capability, to reach Initial Operational Capability (IOC) by 2016, with Full Operational Capability to be reached by 2021.[16] The objectives of the CFDP were effects based and designed to address strategic vulnerabilities, with desired effects expressed as a cyber-aware CAF, a secure and resilient cyber environment, CAF freedom of action in the cyber environment, integration of cyber into CAF operations, and DND/CAF as a credible GoC and Coalition partner. The CFDP also addressed gap analysis. Recognizing that the CAF cyber team must be multi-disciplinary, including electronics and signals experts, system technicians, operational planners and targeteers, and intelligence personnel in addition to those with dedicated, technical cyber operations capabilities, in 2017 the CAF formally established a dedicated Military Occupational Structure Identifier

[16] Canada. Department of National Defence, *Canadian Armed Forces Cyber Force Development Program* (Ottawa: Chief of Force Development, 2014), 9.

(MOSID), or occupation, for Cyber Operators.[17] In 2017, CAF doctrine was updated with the publication of Joint Doctrine Note or JDN 2017-02, Cyber Operations.[18]

The issue of dedicated "cyber warriors" is a challenge for DND, however, as it is for most western nations. The challenge comes in the form of finding or training personnel with the right education and experience in the technical cyber fields.

Because of the technical nature of cyber network operations, extensive training is required, and must be combined with both experience and currency because or the rapidly evolving environment. One RAND corporation study showed that the required training for cyber resembles the same immersive training required for language training and linguists. The same study identified that cyber proficiency may be as much about innate aptitude and critical thinking, skills which are difficult to inculcate in through pedagogy alone[19]. In addition, in a defence context, cyber operators as uniformed military personnel are expected to meet enrolment standards for fitness and drug use, and must go through the lengthy process to obtain security clearance.

Perhaps most serious of all concerns, is that the skills DND and Allied defence sectors require, are the exact skills that industry also need. Given that industry can often offer high salaries than government, militaries face "talent bleed" as soldiers who have been trained at public expense, reach then end of initial commitments, and then leave the military for greener pastures. For the same reasons, militaries are often not the first choice of employer for those trained in universities, especially given the additional requirements and

[17] Canada. Department of National Defence, *Military Employment Structure Implementation Plan (MESIP) for the CYBER OPERATOR Occupation* (Ottawa: Military Personnel Command, 2017).

[18] Canada. Department of National Defence. JDN 2017-02, *Joint Doctrine Note: Cyber Operations* (Canadian Forces Warfare Center, 2017).

[19] Jennifer J. Li and Lindsay Daugherty, "Training Cyber Warriors: What Can Be Learned from Defense Language Training" (Santa Monica, CA: RAND Corporation, 2015), 45–47.

constraints outlined above. Many cyber experts that operate at the highest level, especially those with experience in designing and reverse engineering malware or Computer Network Exploitation, have backgrounds (e.g. hacking or recreational drug use) that may actually disqualify them from obtaining security clearance. Understanding that cyber skills cover a wide range of technical areas, a growing shortage of cyber professionals is fuelling the competition. A RAND corporation study has identified that the global cyber security professional shortfall could reach one million by the end of 2017[20], while another estimates that for the highest tier professionals, there are perhaps 1,000 persons with the right skill sets against a global requirement of 10,000 to 30,000.[21]

The competition with industry has led both the US and UK to explore options for obtaining the necessary skilled personnel. In addition to looking at alternative compensation and skill bonuses, both have begun putting significant emphasis on the use of the reserve as part of the total force to enhance cyber capabilities. In the US, the Army Reserve (USAR) and Army National Guard (ARNG) have dedicated cyber units. These units actively recruit reservists who already have the necessary skills form civilian industry, or allow active component or Regular Force (Reg F) soldiers to continue to serve after transitioning to higher paying primary civilian work, retaining expensive skill sets.[22] In the UK, the Land Information Assurance Group is a dedicated reserve unit that allows civilians with required

[20] Isaac R. III Porche et al., "Cyber Power Potential of the Army's Reserve Components" (Santa Monica, CA: RAND Corporation, 2017), 18.

[21] Joel Dreyfuss, "The Cybersecurity Talent War You Don't Hear About," *CNBC Online*, May 13, 2015, https://www.cnbc.com/2015/05/12/the-cybersecurity-talent-war-you-dont-hear-about.html.

[22] Noel K. Hannan, "Using Reserves in Support of Cyber-Resilience for Critical National Infrastructure: US and UK Approaches," *RUSI Journal (Royal United Services Institute for Defence Studies)* 160, no. 5 (October 2015): 46–51; Porche et al., "Cyber Power Potential of the Army's Reserve Components."

skills to serve without meeting normal military enrolment fitness standards.[23] Both the US and UK have found that while regular access to secure military systems is required to maintain experiential currency, reservists are ideally suited for specialist roles with the cyber force that leverage civilian skills learned in industry. In both countries, the focus on hiring industry trained specialists into the reserves:

> …bolsters the argument that military service is hugely beneficial to employers. While an employer may occasionally take the impact of a long-term mobilization during a reservist's career, there are huge benefits to be reaped from cross-training; skills development and maintenance; exposure to other domains and disciplines (the military environment and ethos encourages knowledge sharing and cross-domain education, for resilience and redundancy on operations); networking in the human sense; and the less tangible soft skills of leadership, management and crisis planning.[24]

The US Army has conducted extensive consultation with industry, and feedback from silicon valley is that many would consider serving if they did not have to meet common enrolment standards, lured by the call to serve the nation, and the chance to conduct operations that in the civilian sector would be illegal.[25]

Given the similarities in situations between Canada and its principle allies, and the examples they are already setting, the use of the reserve in building the CAF cyber capability would seem to be obvious. In fact, the CDS is pushing for this and 50 reserve

[23] Ben Farmer, "Fitness Tests Waived for MoDs New Reservist Cyber Warriors," *The Daily Telegraph*, n.d., https://www.telegraph.co.uk/news/uknews/defence/11360976/Fitness-tests-waived-for-MoDs-new-reservist-cyber-warriors.html.

[24] Hannan, "Using Reserves in Support of Cyber-Resilience for Critical National Infrastructure: US and UK Approaches," 48.

[25] David Crowe. Conversation between the Director Cyber Division, USARNG and the author , 7 March 2018.

positions were designated for cyber when new force structure was announced in his 2015 Strategy to strengthen the Primary reserve.[26] There are however, some systemic challenges in the CAF that are standing in the way of embracing this course of action.

Through most of Canada's military history, the reserve has formed the backbone of the force, with the Reg F serving as a kernel or contingency force that could be augmented by mobilization. During the cold war however, this changed, and the Reg F assumed primacy. Gradually, the size and importance of the reserve was eroded under regular leadership, despite studies and multiple efforts to revitalize the Reserve as a necessary component of the total force.[27] Repeated reports from both the Auditor General and the CAF Ombudsman have pointed out that there are serious issues with reserve management. The Reserve lacks clearly defined roles, equipment, funds and training. There are substantial artificial policy differences between the Reg F and Res F, including pay rates and total compensation, recruiting initiatives, and education, medical and death benefits.[28] In recent years things have begun to change for the better, with emphasis in the CDS 2015 strategy,

[26] Canada. Department of National Defence, *CDS Initiating Directive Reserve Strategy 2015: Strengthening the Primary Reserve* (Chief of Defence Staff, 2015), http://www.ducimus.com/wp-content/uploads/2015/11/CDS-Initiating-Directive-Reserve-1.pdf.

[27] Dr. John English, *The Role of the Militia in Today's Canadian Forces*, Strategic Studies Working Group Papers (Canadian Defence and Foreign Affairs Institute, 2011), http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.588.7141&rep=rep1&type=pdf.

[28] Canada. Office of the Auditor General, "Report 5 - Canadian Army Reserve - National Defence," in *2016 Spring Reports of the Auditor General of Canada* (Ottawa: OAG, 2016), http://www.oag-bvg.gc.ca/internet/English/parl_oag_201602_05_e_41249.html?wbdisable=true; National Defence Government of Canada, "Annual Report | Ombudsman | National Defence | Canadian Armed Forces," November 24, 2017, http://www.ombudsman.forces.gc.ca/en/ombudsman-reports-stats-reports/2016-2017-annual-report.page; "Myth Busting – Reserve Vs Regular Force Benefits - Veterans Ombudsman," accessed March 3, 2018, http://www.ombudsman-veterans.gc.ca/eng/blog/post/286.

and a complete section dedicated to the Res F in the newly issued Canada's Defence Policy: Strong, Secure, Engaged.[29]

Despite this leadership emphasis, a significant challenge is that reserve bias either still exists, or perhaps worse, the personnel making policy, most of whom are Reg F, simply do not consider the reserve in their policy processes. Take for example the MESIP for Cyber Operator. Despite the CDS designating reserve involvement in cyber, the initial MESIP studies were conducted with consideration for the Reg F only. Rather than simply evaluating the requirements and then determining which functions could or should be conducted by reservists and Reg F in a holistic process, reserve involvement was designated to a secondary spiral that was planned for some years later. It was only after that the CDS personally and forcefully intervened,[30] that a reserve amendment to the Cyber Operator MESIP was hastily implemented in September 2017.[31]

The CAF has the opportunity to be able to leverage the civilian skills of reservists to build a robust cyber force. This could be done with uniformed personnel serving in the Primary Reserve, or following the UK example of a Special Reserve without common enrolment standards. There is existing precedent for making use of specialist skills in a special reserve, in the form of the Canadian Rangers. Since 1947, the Rangers have provided

[29] Canada. Department of National Defence, *Strong, Secure, Engaged: Canada's Defence Policy* (Ottawa: Department of National Defence, 2017), 67.

[30] NDHQ Staff Officer. Conversation between a staff officer witnessing the results of the CDS decision brief who wished to be unnamed, and the author, 22 June 2017.

[31] Canada. Department of National Defence, *Military Employment Structure Implementation Plan (MESIP) for the CYBER OPERATOR Occupation (Reserve Amendment)* (Ottawa: Military Personnel Command, 2017), 1.

unique skills to DND/CAF, all while serving under unique terms of service, without meeting universality of service rules, age restrictions, and under unique compensation[32].

There is now significant movement within DG Cyber to build a reserve aspect of the cyber force, albeit eight years late. Consultation with industry and academia is ongoing to determine the best methods of partnership. DG Cyber is also moving towards the first reserve cyber operators, and is working to determine the best force structure and governance for reserve cyber. Currently, however, the CAF does not have a mechanism to track civilian skills of reservists, and in order to bring in specialists, or train them in partnership with external partners, would also need to update policies surrounding terms of service, compensation, recruiting, and education, among others. Sadly, Military Personnel Command, the agency that owns, and is responsible for updating all personnel policy, is slow moving, and has no dedicated reserve advisors to push for change. Recent moves to update reserve death benefits as a result of the Ombudsman's reports have been shelved pending an initial review of Reg F benefits[33], and the compensation and benefits review mandated in SSE is now looking to be years to conclusion. While the CAF can move ahead to develop Reg F cyber forces, this institutional inertia in policy change creates serious risk to the ability to employ specialists in the reserve, which would bring depth and expertise to the DND/CAF cyber capability.

The cyberspace domain, and its impact on society, is growing at an exponential rate. So too are the threats to society from those who would exploit vulnerabilities and cyber capabilities to steal, or otherwise damage our way of life. These threats are of significant

[32] P. Whitney Lackenbauer, "The Canadian Rangers: A 'Postmodern' Milita That Works," *Canadian Military Journal* Winter 2005-2006 (n.d.): 49–60.

[33] MGen J. Milne. Conversation between the Senior Reserve Advisor to Veterans' Affairs Canada and the author, 7 Feb 2018.

enough concern to Canada and its allies to warrant the creation of dedicated cyber forces to defend from cyber threats, and if necessary exploit them in return. Recent efforts to build cyber capability have shown however, that it is difficult and expensive to train and then retain those with the requisite training and expertise in competition with a growing demand from industry. To help in dealing with this challenge, Canada’s principle allies have begun to implement innovative ways to leverage skills found in industry and academia, through service in their reserve components. The CAF has the same opportunity, but in order to do so effectively, will need to overcome bureaucratic inertia and previous institutional mindsets regarding the reserve. While the Regular Force can generate a cyber capability for the CAF, without fully integrating the reserve as a part of the total force, DND and the CAF will continue to bleed money and people, and will lack the specialist skills available through those working in industry, and will ultimately fail to provide Canadians with the robust defence cyber capability in the holistic and cost effective manner they deserve.

Bibliography

Australia. Department of Defence. “Future Operating Concept 2035.” Vice Chief of Defence Force, 2016. https://www.cove.org.au/wp-content/uploads/2017/03/Future-Operating-Environment-2035.pdf.

Beeby, Dean. “Almost 13,000 Federal Employees’ Salaries Exposed by Privacy Breach at Public Services | CBC News.” CBC, June 2, 2017. http://www.cbc.ca/news/politics/privacy-breach-therrien-public-services-procurement-spreadsheet-personal-workers-1.4141297.

———. “Revenue Canada Privacy Breach Leaks Prominent Canadians’ Tax Details | CBC News.” CBC, November 25, 2014. http://www.cbc.ca/news/politics/canada-revenue-agency-privacy-breach-leaks-prominent-canadians-tax-details-1.2849336.

Canada. Department of National Defence. *Canadian Armed Forces Cyber Force Development Program*. Ottawa: Chief of Force Development, 2014.

———. *CDS Initiating Directive Reserve Strategy 2015: Strengthening the Primary Reserve*. Chief of Defence Staff, 2015. http://www.ducimus.com/wp-content/uploads/2015/11/CDS-Initiating-Directive-Reserve-1.pdf.

———. *Integrated Capstone Concept*. Ottawa: Chief of Force Development, 2009. http://publications.gc.ca/collections/collection_2012/dn-nd/D2-265-2010-eng.pdf.

———. *Military Employment Structure Implementation Plan (MESIP) for the CYBER OPERATOR Occupation*. Ottawa: Military Personnel Command, 2017.

———. *Military Employment Structure Implementation Plan (MESIP) for the CYBER OPERATOR Occupation (Reserve Amendment)*. Ottawa: Military Personnel Command, 2017.

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

———. *The Future Security Environment 2013-2040*. Ottawa: Chief of Force Development, 2014.

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

Canada. Office of the Auditor General. “Report 5 - Canadian Army Reserve - National Defence.” In *2016 Spring Reports of the Auditor General of Canada*. Ottawa: OAG, 2016. http://www.oag-bvg.gc.ca/internet/English/parl_oag_201602_05_e_41249.html?wbdisable=true.

Collett, Stacy. “Five New Threats to Your Mobile Security.” CSO Online, August 1, 2017. https://www.csoonline.com/article/2157785/data-protection/five-new-threats-to-your-mobile-security.html.

Cullen, Dr. Patrick J., and Erik Kjennerud-Reichborn. “MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare.” Multinational Capability Development Campaign, 2017 2016.

Dreyfuss, Joel. “The Cybersecurity Talent War You Don’t Hear About.” *CNBC Online*, May 13, 2015. https://www.cnbc.com/2015/05/12/the-cybersecurity-talent-war-you-dont-hear-about.html.

English, Dr. John. *The Role of the Militia in Today’s Canadian Forces*. Strategic Studies Working Group Papers. Canadian Defence and Foreign Affairs Institute, 2011. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.588.7141&rep=rep1&type=pdf.

Farmer, Ben. “Fitness Tests Waived for MoDs New Reservist Cyber Warriors.” *The Daily Telegraph*, n.d. https://www.telegraph.co.uk/news/uknews/defence/11360976/Fitness-tests-waived-for-MoDs-new-reservist-cyber-warriors.html.

Gibney, Alex. *Zero Days*. Documentary. Magnolia Pictures, 2016.

Government of Canada, National Defence. “Annual Report | Ombudsman | National Defence | Canadian Armed Forces,” November 24, 2017. http://www.ombudsman.forces.gc.ca/en/ombudsman-reports-stats-reports/2016-2017-annual-report.page.

Grant, Kelli B. “Consumers Lost More than $16B to Fraud and Identity Theft Last Year.” Accessed May 29, 2018. https://www.cnbc.com/2017/02/01/consumers-lost-more-than-16b-to-fraud-and-identity-theft-last-year.html.

Hannan, Noel K. “Using Reserves in Support of Cyber-Resilience for Critical National Infrastructure: US and UK Approaches.” *RUSI Journal (Royal United Services Institute for Defence Studies)* 160, no. 5 (October 2015): 46–51.

Koerner, Brendan. “Inside the OPM Hack, the Cyberattack That Shocked the US Government.” WIRED. Accessed May 29, 2018. https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/.

Lackenbauer, P. Whitney. “The Canadian Rangers: A ‘Postmodern’ Milita That Works.” *Canadian Military Journal* Winter 2005-2006 (n.d.): 49–60.

Li, Jennifer J., and Lindsay Daugherty. “Training Cyber Warriors: What Can Be Learned from Defense Language Training.” Santa Monica, CA: RAND Corporation, 2015.

Matthews, William. “Military Battles to Man Its Developing Cyber Force.” GovTechWorks by General Dynamics IT, n.d. https://www.govtechworks.com/military-battles-to-man-its-growing-cyber-force/#gs.ukQkiDM.

McKee, Elizabeth. “IRS Data Breach Allows Hackers to Steal $30 Million from Taxpayers.” Americans for Tax Reforms. Accessed May 29, 2018. /irs-data-breach-allows-hackers-steal-30-million-taxpayers.

“Myth Busting – Reserve Vs Regular Force Benefits - Veterans Ombudsman.” Accessed March 3, 2018. http://www.ombudsman-veterans.gc.ca/eng/blog/post/286.

Oğuz, Şafak. “The New NATO: Prepared for Russian Hybrid Warfare?” *Insight Turkey* 18, no. 4 (Fall 2016). https://www.insightturkey.com/cyber/the-new-nato-prepared-for-russian-hybrid-warfare.

O’Kane, Josh. “Federal Government Debuts Data-Breach Reporting Rules.” Accessed May 29, 2018. https://www.theglobeandmail.com/business/article-federal-government-debuts-data-breach-reporting-rules/.

Porche, Isaac R. III, Caolionn O’Connell, John S. II Davis, Bradley Wilson, Chad C. Serena, Tracy C. McCausland, Erin-Elizabeth Johnson, Brian D. Wisniewski, and Michael Vasseur. “Cyber Power Potential of the Army’s Reserve Components.” Santa Monica, CA: RAND Corporation, 2017.

Puiu, Tibi. “Your Smartphone Is Millions of Times More Powerful That All of NASA’s Combined Computing in 1969.” *ZME Science* (blog), October 13, 2015. https://www.zmescience.com/research/technology/smartphone-power-compared-to-apollo-432/.

Ridout, Tim. “Building a Comprehensive Strategy of Cyber Defense, Deterrence, and Resilience.” *The Fletcher Forum of World Affairs* 40 (Summer 2016): 63–83.

Shu, Xiaokui, Ke Tian, Andrew Ciambrone, Danfeng, and Yao. "Breaking the Target: An Analysis of Target Data Breach and Lessons Learned." *ArXiv:1701.04940 [Cs]*, January 17, 2017. http://arxiv.org/abs/1701.04940.

United Kingdom. Ministry of Defence. *Global Strategic Trends: Out to 2045*. Swindon: MoD, 2014.

Wiseman, Paul. "Counterfeiters, Hackers Cost US up to $600 Billion a Year." Phys.org, February 27, 2017. https://phys.org/news/2017-02-counterfeiters-hackers-billion-year.html.