National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

From Fields to Firewalls: Unlocking Reservists' Talents

Major Brian MacLennan

JCSP 49 DL

Exercise Solo Flight

Disclaimer

PCEMI n° 49 AD

Exercice Solo Flight

Avertissement

Canada

CANADIAN FORCES COLLEGE - COLLÈGE DES FORCES CANADIENNES

JCSP 49 DL - PCEMI n° 49 AD
2022 - 2024

Exercise Solo Flight – Exercice Solo Flight

From Fields to Firewalls: Unlocking Reservists' Talents

Major Brian MacLennan

From Fields to Firewalls: Unlocking Reservists' Talents

In the cyber realm, knowledge is armor, collaboration is strength, and vigilance is our shield.

In an era dominated by digital interconnectedness, the security landscape has expanded beyond conventional borders into the cyber domain. Cyber threats pose significant risks to national security, critical infrastructure, and individual privacy. As technology advances at an unprecedented pace, cyber capabilities that were once rare and expensive have become commonplace and affordable. Sophisticated tools, such as artificial intelligence (AI), have enabled a growing number of nation-states and malicious actors to establish a significant presence in the cyber domain. It is estimated that in as little as four years, cyber-attacks could disable critical infrastructure.[1] The necessity for a robust cyber capability within the military becomes increasingly urgent. The Canadian Armed Forces (CAF) is facing tough hurdles in establishing, developing, and sustaining this capability, placing them noticeably behind our crucial allies.[2] Central to this challenge is the deficiency in current recruitment and training strategies tailored specifically for cyber operators within the CAF.

The Canadian Armed Forces Reserve Force emerge as a cornerstone of proficiency and commitment. Beyond merely offering skilled soldiers in the field, the Reserve Force enriches the military with a wealth of professional experience drawn from various areas such as medicine, law enforcement, information technology (IT), and software development. This diverse cadre of reservists bring multifaceted expertise to the table, fortifying our capabilities with a breadth of specialized knowledge and skills. Among those reservists, there are also cyber security specialists who play an increasingly vital role in confronting the evolving threats of the digital age. These reservists play a critical role in protecting their organizations. They respond to cyber security incidents, actively monitor for real time threats, manage, and configure firewalls, respond to incidents, vulnerabilities, and provide security related training. They contribute to safeguarding the confidentiality, integrity, and availability of vital systems and data. However, despite their undeniable importance, the current framework for employing, recruiting, training, and retaining military cyber operators continues to face considerable challenges.

To fully harness the wealth of talent within the CAF Reserve Force, innovative integration of reservists into the Cyber Assurance Task is essential. This approach can create a dynamic and agile force capable of effectively addressing the ever-evolving cyber landscape, significantly boosting our response abilities and capabilities. Integrating

---

[1] Federal Panel Lists 35 'plausible' future threats to Canada and the World. Zimonjic, Peter. Accessed May 21, 2024. https://www.cbc.ca/news/politics/next-disruptions-on-the-horizon-1.7207915

[2] Canada's Active Cyber Defence is Anything But Active. Rudolph, Alexander. Accessed Apr 21, 2024. Canadian Global Affairs Institute 10.

reservists not only enhances the task's overall effectiveness but also provides a vital pathway for these individuals to contribute their specialized skills to national security.

This paper advocates for the integration of part time Reservists into Canada's cyber protection efforts, identifying key areas where they can address gaps within the Regular Force: enhancing cyber abilities, enabling flexible expertise deployment, augmenting capacity during crises, and promoting collaboration and information sharing. It addresses potential concerns about security clearances, training, and operational readiness while emphasizing the overarching benefits of this integration, domestically and internationally. Termed 'From Fields to Firewalls: Unlocking Reservists' Talent,' it underscores the essential shift from traditional roles to cyber defense.

Utilizing Reservist Expertise to Enhance Canada's Cyber Capabilities

Reservists, hailing from various civilian professions within the Information Technology (IT) industry, possess a treasure trove of specialized knowledge and skills. These professionals are at the forefront of cutting-edge fields such as information technology (IT), software development, and cybersecurity. Their current expertise serves as a beacon of preparedness, swiftly deployable to address emerging cyber threats. Unlike regular force personnel, who may be tied to other duties and responsibilities, reservists can dedicate themselves wholly to cyber operations when the need arises. This flexibility not only ensures a more agile and responsive cyber defense posture but also harnesses the latest advancements in technology to safeguard Canada's digital frontier.

In addition to their readiness and flexibility, the integration of reservists into the CAF cyber operations provides a crucial bridge for addressing the skills gap in a rapidly evolving cyber landscape. Reservists serve as a conduit for knowledge transfer, bringing fresh insights and expertise that has been honed in the current tech industry. Their civilian experience complements the training provided to regular force cyber operators, enriching the overall capability of the CAF's cyber defense apparatus. By sharing best practices, industry standards, and real-world case studies, reservists bolster the collective proficiency of cyber operators, ensuring readiness to face the ever-changing cyber threat landscape head-on.

Building on the enhanced capabilities provided by reservists, their participation in training and exercises becomes crucial for developing cyber skills and preparedness. Reservists can play a pivotal role in this aspect, by contributing their unique expertise to enrich the realism of scenarios and ensure that cyber operators are well-prepared for real-world operations. Their involvement in exercises extends beyond mere participation; many reservists can take on the role of the "red team," simulating adversarial attacks to challenge and sharpen the skills of regular force cyber operators. This practical experience not only enhances the effectiveness of training exercises but also fosters a culture of continuous improvement within the cyber defense domain.

Beyond their critical role in training and exercises, reservists also play a vital part in outreach and recruitment. By actively engaging with the technology community, they serve as ambassadors for the CAF's cyber capabilities, participating in conferences,

workshops, and industry events to highlight exciting military opportunities. While Regular Force cyber operators at the Corporal level earn about $72,000 annually, the average starting salary for a civilian cyber specialist range from $78,000 to $125,000, making retention challenging. This retention issue is often offset by the challenging nature of the work and the pride associated with serving in the CAF, especially among Generation X personnel. According to "Strong, Secure, Engaged," the CAF's defense policy[3], the emphasis on professional development, unique experiences, and a sense of purpose are significant factors that help retain talent. Reservists further support retention by showcasing the meaningful work in defending the nation's digital infrastructure, inspiring aspiring cyber professionals to consider a career in the CAF. Their involvement in community events and direct interactions with potential recruits not only helps in building a robust talent pool but also ensures that the CAF's cyber defense capabilities remain strong and adaptive to evolving threats. This dual role of reservists in both operational and outreach capacities is essential for maintaining a resilient and well-staffed cyber defense force. Considering the challenges in recruiting cybersecurity specialists, the CAF might consider maintaining connections with former members[4]. This practice would enable them to potentially re-engage these individuals during emergencies, even after their official military service has ended. Such initiatives would grant the CAF access to a supplementary, familiar pool of trusted experts on an as-needed basis.

Flexibility and Scalability

Part-time reservists distinguish themselves from regular military personnel by balancing civilian careers with military commitments, granting them unparalleled flexibility and scalability in cyber defense operations. This unique balance allows reservists to bring a diverse blend of skills and perspectives to the cyber realm, drawing from expertise in technology, finance, academia, and various industries. Their comprehensive understanding of cyber threats and solutions enables them to devise innovative strategies to mitigate emerging risks in the digital realm. Reservists contribute to a wide range of cybersecurity measures, including implementing robust protocols, creating secure systems, conducting risk assessments, employing advanced encryption techniques, establishing incident response protocols, and promoting cybersecurity awareness and education. This breadth of experience enhances the adaptability and effectiveness of the cyber force, enabling them to safeguard critical assets with innovative strategies.

Moreover, the mobilization of reservists during emergencies underscores their crucial role in bolstering cyber defenses in the same way. When faced with emerging cyber threats, reservists can transition from their civilian roles to military duty, ensuring a rapid and coordinated response. The United Kingdom (UK) under their Joint Cyber Reserve Force[5] have specifically developed a specialized team that enhances their Defence Cyber Capability. Comprising of high-caliber cyber professionals selected from

---

[3] Government of Canada. *Canada Defence Policy, Strong Secure Engaged*. 2017.

[4] Baezner, Marie. "*Study on the use of Reserve Forces in Military Cybersecurity" 2020, Accessed Apr 21, 2024.* http://hdl.handle.net/20.500.11850/413590 Pg 32

[5] United Kingdom. *"Reserves Day: Our Joint Cyber Reserve Force."* June 23, 2023. Accessed April 2024.

industry, academia, and ex-military backgrounds, the force defends and assures platforms, networks, and territories when required. The commitment is similar to that of the Soldier Readiness Policy – Reserve and could equally be further developed to form the basis of a Cyber Reservist[6], that can be surged to meet immediate demand.

Reservists' civilian expertise complements their military training, fostering a holistic approach to cyber defense that integrates both technical proficiency and strategic thinking. Their exposure to diverse industries provides fresh perspectives and insights, enhancing cyber defense strategies. Many reservists have careers in IT, enabling them to rapidly integrate and apply their civilian-acquired skills within the military context. In some instances, these civilian recruits may possess more current knowledge and cutting-edge skills than their full-time military counterparts, thanks to their ongoing private sector experience. By leveraging this wealth of knowledge, the cyber force can stay ahead of evolving threats and effectively adapt to the ever-changing cyber landscape.[7] This synergy between civilian and military expertise not only strengthens the cyber defense capabilities but also ensures a dynamic and responsive approach to national security challenges. Reservists can also be integrated into the Canadian Cyber Security Centre (CCCS) and the Communications Security Establishment (CSE) to fully leverage their expertise and contribute to the resilience of Canada's cyber infrastructure. This agility in deployment allows for the timely reinforcement of cyber defenses, minimizing potential damage and disruption caused by cyber incidents.

In essence, the unique balance maintained by reservists between civilian careers and military commitments empowers them to excel in cyber defense operations. Their diverse backgrounds, mobilization capabilities, and ability to integrate civilian expertise into military operations make them indispensable assets in safeguarding Canada's digital infrastructure against cyber threats either responding to or proactively protecting systems and networks.

Enhanced Collaboration and Information Sharing

Cyber defense operates in a complex and interconnected landscape where collaboration and information sharing among various stakeholders are paramount. In this context, reservists emerge as key facilitators, bridging the gap between the military and private sector entities. Their dual roles within the CAF and civilian organizations position them as invaluable conduits for seamless coordination in cyber defense initiatives. This dual role aligns with the goals outlined in Canada's National Cyber Security Strategy[8],

---

[6] Ibid.

[7] Williams, Bill. *"Cyber Warriors: Army Reserve units take up Mission task of Cyber Operators."* https://canadianarmytoday.com/cyber-warriors-army-reserve-units-take-up-mission-task-of-cyber-operators

[8] Government of Canada, "*Enterprise Cyber Security Strategy"* May 2024. Accessed May 24, 2024. https://www.canada.ca/en/government/system/digital-government/online-security-privacy/enterprise-cyber-security-strategy.html

which emphasizes the importance of partnerships across all sectors to enhance national security.

Transitioning from the discussion on the importance of reservists' industry-specific knowledge and collaboration, it is evident that their integration significantly enhances the capacity to defend against cyber threats and aligns with the recommendations outlined in the 2024 Government of Canada (GC) Enterprise Cyber Security Strategy[9]. Part time reservists, often working within civilian organizations, possess a deep understanding of industry-specific challenges and vulnerabilities. This knowledge allows them to effectively communicate and collaborate with private sector partners, fostering a mutual exchange of insights and expertise. By leveraging their connections and networks within the civilian sphere, reservists can facilitate the flow of information between disparate entities, creating synergies that strengthen the collective defense against cyber threats. Without the integration of reservists, there is a significant impact on the capacity to defend against cyber threats due to the lack of such vital industry-specific knowledge and collaboration. This approach supports the recommendations from the 2024 GC Enterprise Cyber Security Strategy[10], which calls for a whole of government approach with increased collaboration between government, academia, and the private sector to build a robust cybersecurity framework.

Military personnel benefit from robust privacy protections outlined in several key legislative frameworks. The Privacy Act governs the handling of personal information by federal institutions such as the Department of National Defence (DND) and the CAF, ensuring strict adherence to principles regarding collection, use, disclosure, and retention. Reservists, beyond fostering collaboration, play a crucial role in the effective exchange of intelligence. With access to both military and civilian domains, they act as skilled information brokers, discerning and disseminating relevant insights to the appropriate stakeholders. This capacity supports timely response efforts and aligns with the strategic goals outlined in the GC Cyber Security Strategy[11], which emphasizes the importance of accurate and rapid information sharing to combat cyber threats.

By fostering partnerships and promoting information sharing, reservists help create a robust collaborative ecosystem aimed at collectively mitigating cyber threats. Their dual roles, combined with their expertise and civilian sector connections, position them as pivotal elements in the nation's cyber defense strategy. Through their efforts, reservists enhance Canada's cyber resilience and ensure the effective protection of critical infrastructure and assets against evolving cyber threats. This collaborative model is essential for achieving the comprehensive cyber defense objectives set forth in both the

[9] Ibid.
[10] Ibid.
[11] Ibid.

GC Enterprise Cyber Security Strategy[12] and the Nielsen Cyber Review[13], calling for the use of skilled cyber security personnel.

Strategic Talent Pipeline and Recruitment

Canada has a thriving technology workforce, which outpaced the United States in growth rate over the last year. It also has five of the top 50 ranked universities for computer science and information systems[14], tied with the United Kingdom for second-most of all North Atlantic Treaty Organization (NATO) countries. Canada also has a strong cyber security private sector. In 2020, Canada's cyber security industry outperformed[15] the information and communications technology sector across industrial indicators and Canada's cyber research and development intensity was 2.5 times greater[16] than the Canadian information and communications technology industry's overall average.

Countries worldwide recognize the importance of cybersecurity in national defense and have integrated part-time Reserve Force soldiers to enhance their talent pool. Notable examples include the United States, United Kingdom, Estonia, Israel, and Germany, which have actively developed their cyber strategy[17] to maximize the capabilities of their Reserve Force[18]. Building and maintaining a dedicated cyber force from scratch is a resource-intensive endeavor, requiring significant financial investment in recruitment, training, and infrastructure. However, by harnessing the existing pool of reservists—many of whom already possess specialized training and experience from their civilian careers—the CAF can optimize resources and minimize the financial burdens associated with training soldiers from scratch. Reservists receive continuous training in their civilian roles, translating into cost savings for the military, as less investment is needed for initial training. The CAF must capitalize on this unique resource and the dual nature of reservists, not only strengthening Canada's cyber capabilities but also emphasizing the nation's commitment to leveraging all available resources to safeguard national security.

The CAF has made strides in recent years by prioritizing the development of cyber capabilities — in line with NATO's emphasis on cyber defense. Canada emphasized cyber defense in its 2017 defense policy: Strong, Secure, Engaged[19]. In 2018, Canada also published a National Cyber Security Action Plan[20] for 2019 to 2024, emphasizing defensive cyber security, the promotion of an innovative cyber ecosystem,

---

[12] Ibid.
[13] Nielsen, *"Cyber Review Consultations Report".* April 4, 2024. Public Safety Canada.
[14] "*Top 50 World Ranked Universities",* Apr 18, 2024. https://search.proquest.com/docview/3040071221
[15] CADSI, "*State of Canada's Cyber Security Industry"* Fall 2022.
[16] Ibid.
[17] Baezner, Marie. "*Study on the use of Reserve Forces in Military Cybersecurity" 2020, Accessed Apr 21, 2024.* http://hdl.handle.net/20.500.11850/413590 Pg 32
[18] Sprenger, Sebastin. "Services Weighting the Role of Their Reserves in Cyber Operations" July 29 2013.
[19] Government of Canada. *Canada Defence Policy, Strong Secure Engaged.* 2017.
[20] Government of Canada. *Our North, Strong and Free: A Renewed Vision for Canada's Defence*. April 8 2024.

and effective governance and collaboration with international allies and the private sector. Reservists can play this proactive role in outreach and recruitment efforts, a key component of this policy and strategy. By engaging with the civilian community and participating in industry events, reservists raise awareness about career opportunities in cybersecurity and inspire aspiring professionals to join the CAF.

Challenges

Critics may raise valid concerns regarding the integration of reservists into cyber protection roles, highlighting potential challenges such as security clearance, training, and operational readiness. However, these concerns can be effectively mitigated through proactive measures and strategic planning. Rigorous vetting processes can ensure that reservists possess the necessary security clearances and qualifications to handle sensitive cyber operations effectively. Non-disclosure agreements as well as monitored working environments can mitigate the risks of leaks.[21] Specialized training programs tailored to reservists' unique skill sets can further enhance their proficiency in cyber defense tactics, techniques, and procedures. By investing in ongoing readiness exercises, the CAF can ensure that reservists are prepared to respond to cyber threats swiftly and decisively.

Moreover, the benefits of leveraging reservists for cyber protection far outweigh the perceived drawbacks. Reservists offer flexibility in the deployment of expertise, drawn from their diverse backgrounds and experiences in the civilian sector. Their ability to bring fresh insights and specialized knowledge to cyber defense operations enhances the agility and responsiveness of the CAF. During times of heightened cyber threats or national emergencies, reservists provide a crucial augmentation to the Regular Force's capacity, enabling Canada to rapidly scale up its cyber defense capabilities.

Additionally, reservists' unique position as bridges between the military and civilian sectors fosters enhanced collaboration and information sharing. Their dual roles could enable them to facilitate coordination among various stakeholders, including government agencies, private sector[22] partners, and international allies. By leveraging reservists' connections and networks within the civilian sphere, the CAF can establish robust ecosystems of collaboration aimed at collectively addressing cyber threats. Through effective partnerships and shared intelligence, reservists contribute to the creation of a more resilient cyber defense posture for Canada.

While critics may raise concerns about integrating reservists into cyber protection roles, proactive measures can address these challenges effectively. The benefits of leveraging reservists' flexible deployment of expertise, augmented capacity during crises, and enhanced collaboration abilities far outweigh any perceived drawbacks. By harnessing reservists' unique skills and experiences, Canada can strengthen its cyber

---

[21] Baezner, Marie. "*Study on the use of Reserve Forces in Military Cybersecurity" 2020, Accessed Apr 21, 2024.* http://hdl.handle.net/20.500.11850/413590 Pg 32

[22] Baezner, Marie. "*Study on the use of Reserve Forces in Military Cybersecurity" 2020, Accessed Apr 21, 2024.* http://hdl.handle.net/20.500.11850/413590 Pg 33

defense capabilities and ensure the security and integrity of its digital infrastructure in an increasingly complex and interconnected world.

Despite concerns regarding training, integration, and potential strain, proactive measures can effectively address these challenges and facilitate the smooth incorporation of part-time reservists into cyber defense operations. Cyber capabilities, whether defensive or offensive, serve as powerful force multipliers, requiring minimal initial infrastructure investment and offering unparalleled operational flexibility. By embracing reservists as key contributors to its cyber defense strategy, Canada demonstrates its dedication to preempting cyber threats, adjusting to changing circumstances, and taking decisive action to safeguard its digital infrastructure and sovereignty in this unique uncontested battlespace.

Through a holistic and forward-thinking strategy, Canada and the CAF can lead in cyber defense, safeguarding national interests and building resilience against evolving threats. By recognizing and utilizing the unique contributions of reservists, they demonstrate a commitment to creating a comprehensive and dynamic cyber defense force for the digital age.

BIBLIOGRAPHY

Cybersecurity Industry - Industry Report - M2 2022. https://www.emis.com/php/search/doc?pc=XX&dcid=753869484&primo=1.

Four Top-50s and 43 World-Ranked Subjects for UCD in 2024 QS World University Rankings by Subject. News Bites - Private Companies, Apr 18, 2024a. https://search.proquest.com/docview/3040071221.

Government of Canada Enterprise Cyber Security Strategy. Accessed May 24, 2024. https://www.canada.ca/en/government/system/digital-government/online-security-privacy/enterprise-cyber-security-strategy.html.

Government of Canada, Our North, Strong and Free: A Renewed Vision for Canada's Defence. Ottawa: His Majesty the King Right of Canada, 2024b.

Government of Canada, Policy Horizons The Disruptions on the Horizon 2024 His Majesty the King in Right of Canada, 2024c.

Government of Canada, Strong Secure Engaged Canada's Defence Policy Government of Canada, 2017.

United Kingdom: Reserves Day: Our Joint Cyber Reserve Force. Asia News Monitor, Jun 23, 2023. https://search.proquest.com/docview/2828439757.

Baezner, Marie. Study on the use of Reserve Forces in Military Cybersecurity: Center for Security Studies (CSS), ETH Zürich, 2020a. doi:10.3929/ethz-b-000413590. http://hdl.handle.net/20.500.11850/413590.

Baram, Gil and Isaac Ben-Israel. "The Academic Reserve." Israel Studies Review 34, no. 2 (Sep 1, 2019): 1-17. doi:10.3167/isr.2019.340205. http://dx.doi.org.cfc.idm.oclc.org/10.3167/isr.2019.340205.

CGAI. "Canada's Active Cyber Defence is Anything but Active." CE Think Tank Newswire, Jul 28, 2021. https://search-proquest-com.cfc.idm.oclc.org/docview/2556256153.

Hamilton, John, Montrez DeMarcus, and Patrick Pape. "Commercial Cyber Certifications for Military Reserve Components." American Society for Engineering Education-ASEE, Jun 23, 2018.

MacKenzie, Rob and Howard Coombs. Canadian Armed Forces: A New Vision for the Reserves. Vol. 20. Ottawa: ROYAL MILITARY COLLEGE OF CANADA, 2020.

Nag, Abhijit, Vikram Bhadauria, Camille Gibson, Daniel Creider, and Ram Neupane. "A Conceptual Learning Framework of Cybersecurity Education for Military and Law Enforcement: Workforce Development." International Journal of Smart Education and Urban Society 13, no. 1 (Sep 8, 2022): 1-14. doi:10.4018/IJSEUS.309953. http://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/IJSEUS.309953.

Nielsen. Cyber Review Consultations Report. Ottawa: Public Safety Canada.

PAPENFUS, JOSEPH A. Total Army Cyber Mission Force: Reserve Component Integration, 2016a.

Platt, Victor. "Still the Fire-Proof House? an Analysis of Canada's Cyber Security Strategy." International Journal (Toronto) 67, no. 1 (Dec 22, 2011): 155-167. https://www.jstor.org/stable/23265971.

Rudolph, Alexander. 2021. "Canada's Active Cyber Defence is Anything But Active." Canadian Global Affairs Institute 10.

Sprenger, Sebastian. "Services Weighing the Role of their Reserves in Cyber Operations." Inside the Pentagon's Inside the Army 25, no. 30 (Jul 29, 2013): 15. https://www-jstor-org.cfc.idm.oclc.org/stable/24835366.

Tomczyk, Andrzej, Melissa Ziegler, Brandon Cromwell, Ernest Wong, James Comstock, and Steven Song. "A Systems Framework to Integrate a Civilian Reserve Cyber Force for the Us Army." American Society for Engineering Management (ASEM), Jan 1, 2018.

Williams, Bill. 2020. Cyber Warriors: Army Reserve units take up mission task of cyber operators. 02 10. Accessed 02 2024. https://canadianarmytoday.com/cyber-warriors-army-reserve-units-take-up-mission-task-of-cyber-operators/.

Zimonjic, Peter. "Federal panel lists 35 'plausible' future threats to Canada and the world" CBC (May 21, 2024). https://www.cbc.ca/news/politics/next-disruptions-on-the-horizon-1.7207915.