TRIPLE HELIX

Empowering Defence in the Digital Age

by VAdm (ret'd) Ron Lloyd

May 2025

POLICY PERSPECTIVE

EMPOWERING DEFENCE IN THE DIGITAL AGE

by VAdm (ret'd) Ron Lloyd

May 2025

Prepared for Triple Helix
Suite 200, 8 York Street, Ottawa, ON K1N 5S6 Canada
www.cgai.ca/triple_helix

ISBN: 978-1-77397-343-2

The most significant challenge facing the Canadian Armed Forces (CAF) is leveraging "digital" - technologies like cloud computing, artificial intelligence, augmented reality, virtual reality, and big data - to its advantage. No matter what combat capabilities, systems and platforms Canada acquires, they will not be optimized without the digital tools to enable effective pan domain command and control (PDC2). As the CDS notes "The CAF must be able to develop an effective PDC2 capability to be able to compete, contest, confront, and if necessary, defeat adversaries, or it risks becoming irrelevant to Allies." If we expect the CAF to be able to fight tonight and prevail, military leaders must be able to command and control (C2) their forces inside the decision-making cycle of our adversaries. This can only be accomplished if the PDC2 system of systems is modern, interoperable, secure and resilient. As one of many examples, we found out at the 2025 C4ISR and Beyond conference, the Canadian Joint Operations Command, Canada's global joint force integrator for all domestic and international operations, has an analogue system that does not effectively support C2 of operations in the current security environment. PowerPoint and Excel will not win the wars of the future. The CAF understands that our poor digital infrastructure jeopardizes its ability to contribute to coalition operations, and that neither our allies nor our adversaries are waiting for us to play catch up. The CAF is being left behind, and Canada's defence is at risk.

Unfortunately for the Defence Team , the vast majority of the barriers precluding the realization of their digital aspirations reside outside of their authorities, responsibilities, and accountabilities (ARAs). Despite enjoying some policy exemptions in recognition of their unique requirements, they still must comply with numerous other Government of Canada-wide policies which do not reflect or support defence and military needs. For example, one of those many policies is the current security classification policy that was introduced in the 1980s at a time when the only security considerations for data were physical. As such, the Defence Team's digital progress will be a direct reflection of the Government of Canada's ability to realize its digital ambitions. This aggregated approach to policy, (infra)structure, and requirements does not serve the unique needs of the CAF.

It is for this very reason that I have written a series of papers to underscore that Canada, as a nation, is failing to realize its digital ambitions. An important piece of what I have documented is that Canada's security classification framework is no longer fit for purpose. The obsolescence of such a fundamental structure for national security and defence has profound implications for interoperability with our allies, but more so for the integration of new capabilities in the first place. In addition, the framework imposes increased costs and it also reinforces a culture of overclassification and risk avoidance. I have also argued that the public service's focus on policy risk and its ineffective strategic governance are also contributing factors to failing to achieve Canada's digital ambition. The articles provide a number of recommendations to address these shortcomings. Absent implementing these recommendations, Canada will not be able to achieve its digital ambition with disastrous implications for the CAF and Canada's national security.

The goal of this piece is to lay bare the challenges of the current policy framework and their significant national security implications. Not only is Canada's cyber security posture sub-optimal, but we are also paying approximately a half billion-dollar premium (relative to our peers) for it. Understanding how we can increase our cyber security posture more affordably will be important. More importantly, however, is the adverse impact on the CAF's relevance and effectiveness in the digital age – and by consequence on the defence of Canada. If our government does not fundamentally address how defence idiosyncrasies fundamentally require a different digital policy, the CAF will not be able to catch up with its allies and surpass its adversaries. This greatly undermines our ability to contribute to coalition operations and to defend ourselves. In the rapidly changing geo-strategic environment in which we currently live, it is high time we recognized that the Defence Team should have its own digital policy framework.

Simply put, Canada's sailors, soldiers, aviators and special forces operators deserve to be digitally equipped and enabled. This capability is at the heart of their job: defend Canada and protect the international rules-based order Canadians have enjoyed for 80 years. If they are not, they will not stand a chance in the modern battlespace. It is completely unrealistic to believe that Canada, and specifically defence, can function as a 21st century digital enterprise on a 20th century digital policy foundation.

Cyber Security, Defined

In its 2025 National Cyber Security Strategy (NCSS), Canada defined cyber security as:

The protection of digital information, as well as the integrity of the infrastructure housing and transmitting digital information. More specifically, cyber security includes the body of technologies, processes, practices and response and mitigation measures designed to protect networks, computers, programs and data from malicious cyber activities, damage or unauthorized access so as to ensure confidentiality, integrity and availability.

Although reasonable, much like the widely accepted International Telecommunication Union (ITU) definition of cyber security, there are deficiencies.

Schalz et al.'s definition of the term overcomes these shortcomings. To them, cybersecurity is the approach and actions associated with security risk management processes followed by organizations and states to protect confidentiality, integrity and availability of data and assets used in cyber space. [It] includes guidelines, policies and collections of safeguards, technologies, tools, and training to provide the best protection for the state of the cyber environment and its users.

While similar to Canada's definition, this one is preferrable from a defence and security perspective as it is concise, articulates the importance of security risk management, specifically addresses guidelines, policies, and training, and recognizes the fact cyber security is about protecting the users, not just the data.

Canada's Cyber Security Strategy and Its "as is" Cyber Security Posture

In "A Comparative Study of National Cyber Security Strategies of Ten Nations," Odebade and Benkhelifa compare Canada's 2018 NCSS to those of the United Kingdom, the United States, France, Lithuania, Estonia, Singapore, Spain, Norway, and Australia. Canada was ranked 9 out of ten countries. The study noted that Canada's NCSS needed improvements particularly around governance, risk management, and preparedness and resilience. This study provided a useful report card to assess the recently released NCSS, *Securing Canada's Digital Future,* which articulates Canada's long-term plan to tackle increased cyber threats, "in partnership with provinces, territories, Indigenous communities, industry, and academia to secure Canada's digital future."

Analysing the 2025 NCSS based on the Odebade and Benkhelifa report card, reveals that Canada has not addressed significant deficiencies. Specifically, the strategy references governance only once, and merely in the context of the design, creation, and use of Artificial Intelligence (AI). The strategy states that threats and opportunities evolve at a rapid pace globally and it is critical for Canada to be equipped to respond to emerging risks as they occur, which sounds proactive. Yet in the very next sentence it indicates that the government will collaborate with stakeholders and set out a series of action plans *over the coming years*, which reads as delayed action. On a more positive note, the strategy does make numerous references to resilience and states that Public Safety Canada and the Canadian Centre for Cyber Security will establish a Canadian Cyber Defence Collective (CCDC). To understand how effective the 2025 NCSS will be, it will need to be measured against the "as is" cyber security posture. The document recognizes that the CAF has cyber security capabilities. However, due to the Defence Team's numerous dependencies on other government departments for the policies and frameworks that structure its approach to cyber and digital, the best baseline to assess the NCSS's usefulness for defence is the overall Government of Canada's "as is" cyber security posture.

The best assessment of the Government of Canada's cyber security posture is provided by the government itself, in the recently released *Government of Canada's Enterprise Cyber Security Strategy* (GCECSS). The GCECSS observes that while there are varying levels of cyber maturity across departments, they are on average providing ineffective defence against new and emerging threats. There is also a lack of comprehensive awareness of the cyber security risk environment; a significant legacy infrastructure footprint where departments continue to rely on manual processes that are time-consuming, error prone, and ineffective; a lack of coordination across security capabilities leading to blind spots in the government's overall security posture; and misalignment between traditional approaches for security assessments and agile delivery methodologies. Assessed against the United States National Institute of Standards and Technology (NIST) Cyber Security Framework 2.0, (upon which Canada based its 2025 NCSS), Canada's cyber security posture is in the bottom or second bottom tier of four tiers describing an organizations cybersecurity governance and risk management practices.

Figure 1: CSF Tiers for cybersecurity risk governance and management (source: NIST's CSF 2.0)

Canada is well aware of the deficiencies. The National Security and Intelligence Committee of Parliamentarians' *Special Report on the Government of Canada's Framework and Activities to Defend its Systems and Networks from Cyber Attack* identifies challenges and gaps as well and concludes that "the data of organizations not protected by the government cyber defence framework is at significant risk." The Report of the Standing Committee on National Defence *The Cyber Defence of Canada* echoes this concern and provides 37 recommendations to improve the situation.

Not only does Canada's sub-optimal cyber security posture present significant risks; it is also extremely expensive. A 2018 Shared Services Canada (SSC)-sponsored Gartner study "identified that SSC's network and security model is expensive to operate with a 19% or $427 million greater cost than peers." It is difficult to believe that the costs have not continued to increase in the intervening years. Thus, not only is Canada's cyber security posture sub-optimal, but Canadians are paying considerably more for it relative to our peers.

In order to address these deficiencies, the GCECSS defines a vision and a number of strategic objectives to realize that vision. Unfortunately, it will be difficult for the government to fully implement the GCECSS and reach its intended outcome because it anchors the strategy and its execution to the Canadian Centre for Cyber Security's (Cyber Centre's) IT Security Risk Management: A Lifecycle Approach (ITSG-33). So, what is ITSG-33 and what are the implications for defence?

ITSGG-33: An Obsolete Framework

The Communications Security Establishment (CSE) released ITSG-33 in November 2012. The purpose of the document is to "help government departments ensure security is considered right from the start." From a Deputy Minister's perspective, the implementation of the ITSG-33 is about complying with the Treasury Board Secretariat (TBS) risk management strategies policies, and requirements for IT security.

Through the ITSG-33, Canada (much like our non-U.S. Five Eyes partners) leverages the NIST frameworks and standards, which all American federal agencies must implement, with the exception of national security systems. The NIST released the Cybersecurity Framework (CSF) 2.0 in February 2024, which a comprehensive suite of documents ("Special Publications") supports and complements. Whereas our Five Eyes partners have all recently updated their direction and guidance to their departments, ministries, or agencies, Canada has not. The most recent update to ITSG was in 2015, when the security control profiles for Protected B and Secret were updated, seemingly the same year as the deletion of the Protected A security profile. The implications for Defence and all government departments of following direction and guidance that are over a decade old are significant.

In its first annex, ITSG-33 outlines a risk management process, its relationship with external processes, outlining IT security risk management activities and consolidating all of the roles and responsibilities of the various stakeholders. A clear shortcoming of this annex is how it defines injuries and threats (see Table 1).

There are innumerable challenges with this table. First, much of the terminology is open to significant interpretation. How does one define the threshold required to represent an impediment, damage, reduction, embarrassment or affect? The graduated levels of risk also ignore the realities that information not related to national security are in fact less risk than information associated with national security. As such, there should be significantly more high and very high risks that are blacked out. In addition, many of the graduations appear forced, such as program performance, outcomes, compromised and key programs. How can an adverse impact on project performance not adversely affect outcomes? What is the criterion by which a program is considered key? How is the determination made between affecting quality of life and financial security compromised? Finally, there are no examples that would inform defence. Given the risk aversion and overclassification tendencies within the public service, this table leaving room to such significant interpretation is extremely problematic.

Injury Type	Qualifier and Level				
	Very low	*Low*	*Medium*	*High*	*Very High*
Civil disorder or unrest	No reasonable or negligible expectation of injury	Civil disobedience, public obstructions	Riot	Sabotage affecting critical assets (e.g., critical infrastructure)	Large scale riot or sabotage requiring martial law
Physical harm to people	No reasonable or negligible expectation of injury	Physical discomfort	Physical pain, injury, trauma, hardship, illness	Physical disability, loss of life	Widespread loss of life
Psychological harm to people	No reasonable or negligible expectation of injury	Stress	Distress, psychological trauma	Causing a mental disorder or illness	Widespread psychological trauma
Financial loss to individuals	No reasonable or negligible expectation of injury	Causing stress or discomfort	Affecting quality of life	Financial security compromised	
Financial loss to Canadian companies	No reasonable or negligible expectation of injury	Affecting program performance	Reducing competitiveness	Viability compromised	
Financial loss to Canadian government	No reasonable or negligible expectation of injury	Affecting program performance	Affecting program outcomes	Program viability compromised	Key programs viability compromised
Harm to Canadian economy			Affecting performance	Reducing international competitiveness	Compromising key economic sectors
Harm to Canada's reputation	No reasonable or negligible expectation of injury	Loss of Canadian public confidence	Embarrassment (home or abroad)	Damage to federal-provincial relations	Damage to diplomatic or international relations
Loss of Canadian sovereignty			Impediment to the development of major government policies	Impediments to effective law enforcement Loss of continuity of government	Loss of territorial sovereignty

Table 1: Examples of Injury Types and Levels reproduced from ITSG-33

Once the level of risk is established, determining the corresponding security classification ITSG-33 requires a conversion of the level of injury to both the classification and confidentiality/integrity and availability of the information using a five-level scale table like the one above from a three-level scale (Confidential, Secret, Top Secret). Whereas ITSG-33 uses higher level policy as references for most of the document, in this conversion table a "subordinate" reference, *Harmonized TRA Methodology* (TRA-1), is used as opposed to the *Directive on Security Management – Appendix J: Standard on Security Categorization*. It appears that the government favours an 18-year-old "subordinate" reference because the *Directive* defines the same levels of injury for Protected A/Confidential, Protected B/Secret, and Protected C/Top Secret, causing significant confusion. However, using TRA-1 is just as challenging. One of the biggest concerns is that the Communications Security Establishment and the Royal Canadian Mounted Police released it in October 2007 and although the theory may still be relevant, the document is out of date. However, it is still listed as a cyber security tool on the Canadian Centre for Cyber Security website. It is perplexing at best to see it used in the cyber domain today and referenced four times in the 2025 ITSP.10.171, *Protecting controlled information in non-Government of Canada systems and organizations*.

The ITSG-33 Annex 2 "provides guidance to authorizers, project managers, security architects, security practitioners, security assessors, and members of IT operation groups," essentially defining what right looks like to every public servant associated with an IT project. In a nutshell, this 60-page document "described in detail" a "comprehensive approach" on how to implement cyber security in a waterfall manner. Following this methodology will help departments satisfy "the objectives and requirements" of various Treasury Board policies, directives, and standards on security and risk management (including in IT). It therefore should not be surprising that the GCECSS observes that there is a "misalignment between traditional approaches for security assessments and agile delivery methodologies."

Annex 3A provides a catalogue of 923 controls that serve as the "basis for developing departmental and domain security control profiles," intended to help practitioners comply with the law and Treasury Board policy suite. Because this annex overlaps about 98% of the controls outlined in the NIST SP 800-53 series, there are some useful strategic takeaways.

Despite the NIST only providing guidance for non-national security systems, the Committee on National Security Systems (CNSS) "collaborates with NIST to ensure NIST SP 800-53 contains security controls to meet the requirements of NSS and provides a common foundation for information security across the US Federal Government." The U.S. Department of Defense (DoD) also leverages the most recent revision of the NIST 800-53 low/moderate/high baseline, making it reasonable to map these baselines to Canada's Protected A, Protected B and Secret baselines in ITSG-33.

As ITSG-33 deleted the security profile for Protected A, it obviously cannot be compared to the NIST low baseline. The key takeaway from the deletion of the profile is that it reinforces a culture of overclassification. It also begs the question, is it realistic to believe that all IT systems in the Government of Canada's landscape need to meet the medium baseline requirement? NIST's

moderate (or medium) baseline profile identifies 257 controls whereas the Canadian Protected B profile has 436 controls. The NIST high baseline has 339 security controls whereas Canada's secret profile has 516. The Canadian moderate baseline has more security controls than the NIST high baseline.

In the context of defence, this begs the question: what are the implications of having approximately 180 additional security controls for "equivalent" baselines? Is it resulting in additional cost, less opportunity to leverage digital technologies, are there interoperability challenges and what is the impact on defence industry having to meet these standards? Finally, is having too many controls having a negative impact on the Defence Team's cyber security posture? Is this simply a result of the fact that the Canadian definition focuses solely on protection and mitigation as opposed to approaching it from a security risk management perspective?

Critical Shortcomings to the "as is" GC Cyber Security Posture

A. **Governance**

Based on how our Five Eyes partners approach cyber security, it makes perfect sense for the Canadian Centre for Cyber Security to be the authority for providing the recommended baseline controls for departments and government agencies. It also makes sense that they would provide that direction in a single document, similar to Australia and New Zealand and that it be updated regularly noting that all of the countries have updated their respective directives and guidelines in 2024. However, in Canada there is currently a patchwork quilt of policies, directives, playbooks and guidelines that provide central agency guidance on how departments are to secure their IT capabilities. Many have not been updated in years, most have no revision history, most are not available in pdf but rather in print version (probably not a digital best practice), and most do not identify how they derive their authority. It should therefore not be surprising that Defence finds itself struggling to keep pace with our allies who have a more current and progressive policy framework.

As a result of the current construct, it must be exceptionally challenging for the Defence Team to have to sift through these documents and understand what direction is complementary, which is in conflict, and which authority has precedence. As Figure 2 illustrates, NIST CSF 2.0 reinforces the central role governance plays from a cyber security perspective. Unfortunately, CGECSS did not reflect this recent change. More disappointingly, it also portrayed an overly simplistic articulation of the authorities, responsibilities and accountabilities (ARAs) in Canada's complex cyber security landscape.

Figure 2: NIST 2.0 Cyber Security Framework

There are innumerable examples of the complexity of Canada's ARAs with respect to cyber security/digital. An examination of the relationship between the Treasury Board Secretariat and CSE provides an illustrative example. Treasury Board is responsible for the "strategic direction, oversight and [government of Canada] cyber security event management," whereas "CSE is the lead technical authority for information and IT security including the provision of leadership, advice and guidance for technical matters related to IT security."[1] In keeping with the government's model, while Treasury Board operates at the strategic level, CSE stands between operational/tactical levels, and line departments act purely at tactical. However, in the *Policy on Service and Digital,* the responsibilities articulated for the Chief Information Officer of Canada and CSE lead to possible broad interpretations and overlap of responsibilities. Examples of this overlap are numerous.

The Directive's Appendix B*: Mandatory Procedures for Information Technology security control* states that departments are to "design and configure information systems to provide only required capabilities to specifically prohibit, disable or restrict the use of unnecessary functions, ports, protocols and services." ITSG-33 contains an entire family of controls dedicated to configuration management and more specifically how CM-2 applies to baseline configurations. The *Digital Standards Playbook* has a section titled "Address security and privacy risks" that recommends different processes and articulates additional controls. One of these recommendations include penetration testing. The ITSG-33 catalogue outlines three controls for penetration testing, none of which were selected for the Protected B profile. The point here is not

[1] The advice and guidance provided by CSE is not only upwards to TBS, but equally as important to line departments. Whereas timely advice and guidance at the beginning of a digital initiative is invaluable, if it is interpreted as a challenge function towards the end of an initiative, it results in departments wasting valuable time and resources.

to disagree with the requirement for penetration testing, but first to point out the disconnect between the ITSG-33 and the Digital Playbook, as well as and to highlight that penetration testing is not among the 436 controls recommended for Protected B.

Another example of redundant and/or potentially conflicting direction to departments is evidenced in Treasury Board's *User authentication guidance for information technology systems*. Once again, ITSG-33 has an entire control family dedicated to the Identification and Authentication Policy and Procedures with 59 available controls, 29 of which have been selected for the Protected B profile. The last example is from the *Directive on Service and Digital* which articulates a number of standards for departments. To gain a sense of the tactical detail provided, Appendix E*: Standard on Information Technology Provisions* reads that individuals are entitled to "two screen display (monitor) devices… screen displays have rotate, tilt, and height adjust capabilities and a minimum screen size of 22 inches per screen." The fact that Defence needs to navigate this patchwork of policies, directives, guidelines and playbooks must be an extraordinary challenge. While serving as the first Chief Data Officer for the CAF/DND, I repeatedly heard the Chief of Defence Staff and Deputy Minister indicate that for the Defence to succeed it needs to accept more risk. As much as the three stars and Assistant Deputy Ministers were prepared to accept that risk, little did I/we appreciate at the time that we were in a policy environment that dictated everything down to the number, capabilities and size of computer screens employees ought to use.

As much as one would hope there would be a lifting of the digital policy shackles on Defence since my retirement in 2019, unfortunately the trend is quite the opposite. For example, in July 2024 Treasury Board and SSC released the Application Hosting Strategy. The four broad goals are:

1. Provide robust governance and oversight of application hosting
2. Leverage competitive procurements that support long-term operations
3. Drive sustainable funding that is predictable and transparent
4. Promote cohesive and consolidated application hosting services to reduce burdens on federal institutions.

I would suggest that for the majority of government departments, these are admirable goals. However, they are constraining from Defence perspective. As much as some would argue that Defence possesses administrative back-office data[2] that should be treated no differently than any other government department, the reality is more complex. The administrative data versus operational data is an overly simplistic and a foolish characterization in keeping with those who believe that tooth and tail is a useful construct to use for characterizing defence expenditures. It is more useful to think of defence data as articulated in figure 3. The reality for defence is that at any given moment material, technical, financial or personnel data can become operational. It

[2] Administrative data would include personnel, material, technical and financial data as examples.

does not mean that it becomes secret, or even classified, it just means that it has to be secure and readily consumable to inform decision making.

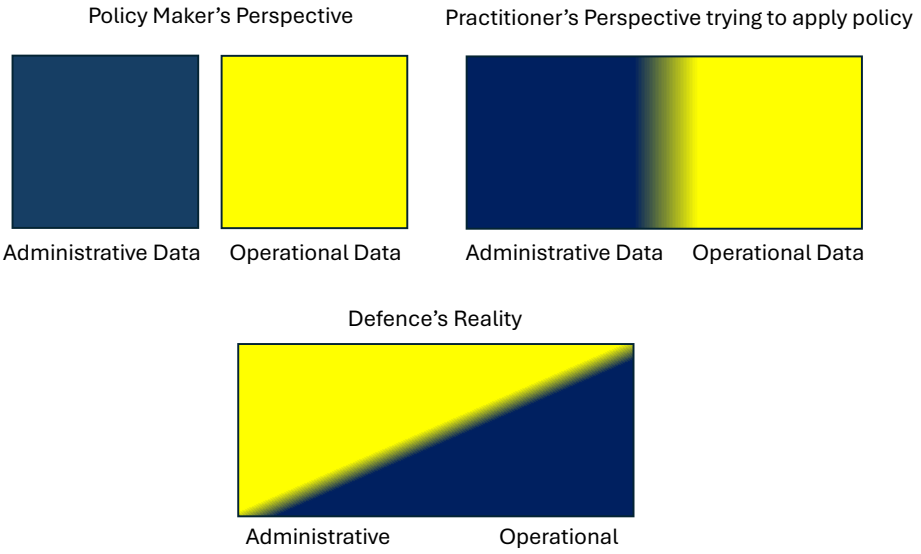

Figure 3: Different perspectives of administrative and operational data

As Defence owns the national security risk, surely, they should own the risk of where they host all of their data as opposed to having it approved by other departments/agencies trying to deliver on four broad goals that have nothing to do with national security.

B. Cloud

There is no debate that cloud technologies will be a decisive differentiator from a defence and security perspective in the battlespace of the 21st Century. Hence, the importance of ensuring cloud technologies are viewed or approached within the existing digital landscape of the nation. Unfortunately, whereas Canada had the opportunity to update or add a security profile to ITSG-33 for cloud and to update the many policies that would be implicated by cloud, it did not. Instead, Canada published the *Government of Canada Security Control Profile for Cloud-based GC Services* (authority of document not stated, original date not indicated, last date modified July 2016) which arguably achieved quite the opposite. The fact that one of the references to define the business context for this document is the Treasury Board's June 1995 Security Organization and Administration Standard is problematic. There are many occasions where this document contradicts or uses terminology not consistent with other existing policies and guidelines. In addition, some of the processes it defines, such as conducting a threat and risk assessment and defining information and IT security safeguards, are inadequate. With respect to the actual cloud

profiles articulated in the annex, they were recently updated and are found in the May 2020 Guidance on the security categorization of cloud-based services (ITSP.50.103).

Although ITSG-33 informed Canadian cloud profiles, "the NIST security control baselines under the Federal Risk and Authorization Management (FedRAMP) program" had a substantial influence on them. FedRAMP was established in 2011 (prior to the release of ITSG-33) to "provide a cost-effective, risk-based approach for the adoption and use of cloud services by the federal government" and leverages NIST standards and guidelines. The FedRAMP baselines can be downloaded from the internet as an excel spreadsheet as can Canada's Protected A and B profile. Canada's low baseline, based on the interpretation of the documents data classified as Protected A, has 253 controls and FedRAMP's low baseline has 156 controls. Once supply chain controls are taken into consideration, Canada's low (Protected A) baseline requires an additional 108 controls more than the FedRAMP low baseline. The question to be asked is why does Canada require almost double the controls for comparable low baselines? And why does it have a low baseline for cloud but not for on premise?

Canada's Protected B Medium Assurance Medium Integrity (PBMM) baseline consists of 357 security controls, while FedRAMP Moderate has 323. Once supply chain controls are taken into consideration, the PBMM baseline has an additional 46 controls. The controls also do not map across one for one and there are 80 controls in the PBMM baseline that do not map to FedRAMP Moderate. The question, once again, is what are the implications of having 20% control variance between FedRAMP moderate and PBMM? Is this resulting in increased costs for Defence with minimal return on investment, is it constraining the use of leveraging digital technologies, are the costs being passed on to industry to meet these additional requirements, and what are the implications of not meeting the additional FedRAMP security controls that Canada has not selected, particularly those that deal with supply chain?

C. Zero Trust & Data Centric Security

The legacy policy framework that has informed government's culture about cyber security is also problematic for Defence as they look to leverage modern cyber security solutions. As noted earlier, the current classification policy was introduced at a time when the only security considerations for data were physical. The security of the information dictated whether a locked filing cabinet, a filing cabinet with a bar and lock, or a Secret filing cabinet with a Secret lock was required. Unfortunately, this is the mental model that most have with respect to digital security. If you have access to the "filing cabinet," you can have access to everything that is in it. If the government is truly going to leverage their data to advantage securely in the 21st century, it will be essential that they embrace Zero Trust (ZT) and Data Centric Security (DCS), neither of which are referenced in ITSG-33.

Zero Trust is a security concept based around the idea that systems and users should not be given access to any information without verification, even when they are connected to internal networks. "Zero Trust looks to acknowledge that the previous concept and approach of using

perimeter defences and providing free access within the secure perimeter is no longer practical or appropriate for securing information assets." This is important because "with the growth of the internet and cloud services, the proliferation of data and the growth in malicious and cyber-criminal activities, older methods of enabling information security are "fragile," can be fragmented, and are in some cases, ineffective."

Whereas Zero Trust works on the principle of who accesses the system, data centric security works on the principle of what data that user has access to. "As part of a zero trust approach, data-centric security management aims to enhance protection of information (data) regardless of where the data resides or who it is shared with." ZT combined with DCS ensure that only authorized users can access the data they are allowed to access. As government looks to embrace hyperscale cloud that is comprised of thousands of servers and consumers it is not realistic to implement physical controls, air gapped networks, specialized facilities, and dedicated operations with unique Government security clearances.

Canada's Five Eyes partners' approaches to digital security from this perspective provide very useful context. The United States have mandated Zero Trust in Executive Order 14028, "Improving the Nation's Cybersecurity." Although, not as authoritative, Australia New Zealand, and the UK have also articulated strategic direction and guidance on progressing Zero Trust. Although Canada has articulated a cloud first mindset going back to 2018, it is unfortunate that government stakeholders were unable to communicate the complexities associated with cloud to the National Security and Intelligence Committee of Parliamentarians (NSICOP). In their 2021 Special Report on the Government of Canada's Framework and Activities to Defend its Systems and Networks from Cyber Attack, they described Canada's cyber defence system as follows:

In its purest form, the system can be distilled into a few key elements:

- government systems fall within a single perimeter
- the perimeter has a handful of access points to the Internet
- those access points are monitored by sophisticated sensors that are capable of detecting and blocking known threats
- defences are layered, with specialized sensors capable of detecting and blocking threats deployed on individual devices and to cloud environments
- anomalies in network traffic are analyzed for new threats, information that is used to continually update *** cyber defences for threat identification and blocking; and
- departments continually update and patch their devices and systems under the coordinated direction, advice and guidance of the three organizations.

The current cyber defence system has not yet achieved this ideal.

This characterization refers to the legacy government posture and does not take into consideration the significant amount of work government needs to do to realize a Zero Trust posture and data centric security that are essential considerations in the digital age.

The GCECSS reinforces this very point: "While the traditional perimeter-centric security model has served the GC well, the notion that digital assets and users within a defined boundary are trustworthy does not scale to the 'new digital world' where the trusted perimeter cannot be defined. Increased connectivity, the risk of insider threats, and the need to protect and store data in various in-house and third-party repositories (for example, cloud) have led to new security concepts that do not rely solely on a perimeter-centric security approach (that is, zero-trust)." As long as Defence is treated as every other government department and continues to be bound by a culture of legacy digital cyber security fears that exist in other departments and continue to be perpetuated in Defence, it will be a challenge for Defence to make the significant progress required.

In an effort to enable Defence to overcome the ever-expanding digital gap between our closest allies, partners and adversaries a number of recommendations are provided. It is assessed that absent the implementation of these recommendations Defence and government more broadly will continue to be afflicted by the same issues described in the GCECSS.

Recommendations

1. In recognition of the rapid evolution of digital technologies and the uniqueness of the Defence digital enterprise, it is recommended that the current digital policy suite be reviewed. A thoughtful updating of Defence domain specific policy can lead to an enduring and evolving framework that respects the government of Canada position/direction while focussing on defence specific needs to best mitigate national security risk at pace and at scale.

2. Canada revisit the responsibility sections of the various digital policies to remove ambiguity that currently exists between departments, CSE, SSC, and Treasury Board. If the latter is to provide strategic direction, then it should be the lens through which their responsibilities are articulated to all departments, and in particular Defence.

3. Adopt a new security classification framework of Official (Official: Sensitive), Secret and Top Secret. In the interim, Canada convene a government/industry working group to review the security profiles for Protected B, Secret in ITSG-33 and the cloud security profiles for Canadian Center for Cyber Security (CCCS) Low and CCCS Medium to understand the implications of having excessive control profiles and provide a report to TBS in 2025.

4. Recognizing that cyber security is foundational to our national security and that it not only informs Defence, but all government departments, it is recommended that the *Government of Canada's Enterprise Cyber Security Strategy* (GCECSS) (May 2024) be updated as follows:

    a. In figure 1, reflect the govern function as depicted in the NIST CSF 2.0 framework

    b. Direct CSE to draft a government of Canada information security manual as the authoritative document for line departments. It should articulate the cyber security framework, define common approaches, methodology, solutions and tools for assessing departmental GC cyber security postures.

    c. Direct departments to develop Zero Trust plans and submit them to TBS in 2025.

5. Having consulted with Dr. Schatz to validate their proposed definition of cyber security in 2017 is equally applicable in 2025, it is recommended that Canada amend its definition of cyber security as follows: "The approach and actions associated with security risk management processes followed by organizations and states to protect confidentiality, integrity and availability of data and assets used in cyber space. The concept includes guidelines, policies and collections of safeguards, technologies, tools, and training to provide the best protection for the state of the cyber environment and its users."

6. To mitigate the many misperceptions about the security of cloud it is recommended that the Canadian Center for Cyber Security promulgate a white paper for senior executives similar to the UK's *Security benefits of a good cloud service* (November 2020).

Conclusion

In light of the geo-strategic environment in which Canada finds itself, there is currently no better time than the present for Canada to (re)assess its realities. One of those realities is that we are falling behind our allies, partners, and adversaries digitally at an exponential rate. As antiseptic as this may sound, there are significant national security and economic implications for the defence and security of the nation.

As Canada looks at increasing its defence budget, there needs to be a significant investment in digital. The ability of a nation to leverage digital successfully in the modern battlespace will determine success from failure. *However, significant digital investments by Defence in the current digital policy paradigm will not deliver the outcomes required for Canada.* There is a word for doing the same thing over and over again expecting a different outcome: Insanity.

The perception of the Canadian Armed Forces and the Department of National Defence as any other government department has proven itself not to be effective, and even less so in the digital domain. If the Defence Team are responsible for the national defence and security of the nation, then they must be empowered to do so. The current accountability framework characterized by split accountabilities, unclear and often contradictory policies essentially delivers no accountability at all. I would surmise that this is a very frustrating construct for the Chief of the Defence Staff and the Deputy Minister of National Defence.

It is evident that there is much work to be done. Defence, as well as all other departments, are challenged to navigate a byzantine policy paradigm consisting of out of date polices, overlapping and conflicting guidance, and overly risk adverse baseline profiles. Whereas Canada's Five Eyes partners are routinely updating their departmental guidance and control profiles and have consolidated them into one or few documents, Canada does not. Much of the operational and tactical direction to Defence and other departments is over a decade old, do not reflect modern cyber security best practices, and is not consolidated in a single document, or even a few, but distributed across numerous policies, guidelines, directives, playbooks and other authoritative documents.

In the meantime, our Five Eyes partners are proactively embracing Cloud and modern digital security practices such as Zero Trust and Data Centric Security with a sense of alacrity. Canada, on the other hand, is falling behind. The net result of the aforementioned shortcomings is that Canada's cyber security posture is sub-optimal despite costing hundreds of millions of dollars more than our peers.

The GCECSS concludes:

An appropriate balance between security, the associated cost and the end user experience is required. While security is of paramount concern, the [government of Canada] must embrace a strong cyber risk culture to ensure that the necessary security controls commensurate with the sensitivity and value of the information are implemented in a cost-effective manner with minimal impact on the end user.

Truer words have never been spoken. Implementing the recommendations provided in this paper, in addition to those in this policy series will serve the national defence and security of the nation well.

About the Author

Vice-Admiral (retired Ron Lloyd) *was the 35th Commander of the Royal Canadian Navy from 2016-2019. During that time, he was also "double hatted" as the acting Vice Chief of the Defence Staff for almost half a year and as the first Chief Data Officer for the Department of National Defence and Canadian Armed Forces for a full year.*

During his 38-year career in the RCN, he was privileged to have commanded HMCS CHARLOTTETOWN, HMCS ALGONQUIN, the PACIFIC Fleet and the ATLANTIC fleet. He has extensive operational experience having deployed on numerous occasions globally.

Lloyd has over a decade of experience at National Defence Headquarters having also served as the Deputy Commander of the RCN, the Chief of Force Development for the Canadian Armed Forces, the Director General of Force Development for the RCN and Executive Assistant to the Commander of the RCN.

Lloyd holds a Bachelor of Arts in Military and Strategic Studies from Royal Roads Military College (1985) and a Master of Arts in War Studies from the Royal Military College (2004). He is a graduate of both the Command and Staff Course and the National Security Studies Course at the Canadian Forces College in Toronto. He has also attended the HARVARD Kennedy School, Executive Education, Senior Executives in National and International Security.

Today, as Principal of Leadmark Ventures, he shares his experience in leadership, strategic planning and digital transformation with organizations committed to providing innovative solutions that enhance public sector performance in defence and non- defence related activities.

Canadian Global Affairs Institute

The Canadian Global Affairs Institute focuses on the entire range of Canada's international relations in all its forms including trade investment and international capacity building. Successor to the Canadian Defence and Foreign Affairs Institute (CDFAI, which was established in 2001), the Institute works to inform Canadians about the importance of having a respected and influential voice in those parts of the globe where Canada has significant interests due to trade and investment, origins of Canada's population, geographic security (and especially security of North America in conjunction with the United States), social development, or the peace and freedom of allied nations. The Institute aims to demonstrate to Canadians the importance of comprehensive foreign, defence and trade policies which both express our values and represent our interests.

The Institute was created to bridge the gap between what Canadians need to know about Canadian international activities and what they do know. Historically Canadians have tended to look abroad out of a search for markets because Canada depends heavily on foreign trade. In the modern post-Cold War world, however, global security and stability have become the bedrocks of global commerce and the free movement of people, goods and ideas across international boundaries. Canada has striven to open the world since the 1930s and was a driving factor behind the adoption of the main structures which underpin globalization such as the International Monetary Fund, the World Bank, the World Trade Organization and emerging free trade networks connecting dozens of international economies. The Canadian Global Affairs Institute recognizes Canada's contribution to a globalized world and aims to inform Canadians about Canada's role in that process and the connection between globalization and security.

In all its activities the Institute is a charitable, non-partisan, non-advocacy organization that provides a platform for a variety of viewpoints. It is supported financially by the contributions of individuals, foundations, and corporations. Conclusions or opinions expressed in Institute publications and programs are those of the author(s) and do not necessarily reflect the views of Institute staff, fellows, directors, advisors or any individuals or organizations that provide financial support to, or collaborate with, the Institute.