



435 Transport and Rescue Squadron transports evacuees from Norway House, Manitoba, due to forest fires during Operation LENTUS, Northern Manitoba on May 30, 2025.

Photo: Aviator Nicholas Zahari, 17 Operations Support Squadron Imaging, Winnipeg

The SIGINT-Cyber Nexus in the Canadian Armed Forces

LIEUTENANT-COLONEL L. J. REDIGER

Lieutenant-Colonel (LCol) Leslie Rediger joined the Canadian Armed Forces as a communications and electronics engineering officer in 2001, graduating in 2006 with a bachelor's in mechanical engineering from the Royal Military College of Canada. For the first 15 years of her career, she enabled air operations as a communications and information systems officer at various RCAF wings and at 1 Canadian Air Division Headquarters. She deployed multiple times in support of Op ATHENA and Op REASSURANCE. In 2016, LCol Rediger transitioned to Signals Intelligence (SIGINT) Operations, serving as officer commanding the support squadron and as deputy commanding officer at Canadian Forces Station (CFS) Leitrim, and as chief of staff of Signals Intelligence at Canadian Forces Information Operations Group Headquarters. She was promoted to her current rank in 2020 and commanded Canadian Forces Station Leitrim from June 2023 to October 2025. She is currently the CAF CYBERCOM liaison officer to the United Kingdom. LCol Rediger holds a Master of Arts in Leadership from Royal Roads University and a Master's in Defence Studies from the Canadian Forces College.

Strong, Secure, Engaged: Canada's Defence Policy, released in 2017, frames the "rapid evolution of technology" as a central driver of change in the global security environment, reshaping the character of conflict.¹ It also notes that the Canadian Armed Forces' (CAF) use of cyberspace and emerging technology "brings significant operational benefits, but also creates critical vulnerabilities."² This means that, to be competitive and to defend Canada's interests, the CAF must be able to protect its assets, defend its freedom to manoeuvre in cyberspace, and be able and ready to leverage that operating environment to carry out its directed mandate.³

To “maximize Canada’s effectiveness in cyberspace” in *Our North, Strong and Free: A Renewed Vision for Canada’s Defence*, the Government of Canada directed the CAF to establish the Canadian Armed Forces Cyber Command (CAFCYBERCOM).⁴ This new command is intended to “improve the CAF’s ability to conduct cyber operations” and “enable the military to generate and employ cyber forces and other specialized capabilities on short notice and contribute to advancing Canadian interests and protecting Canadian, Allied and partner militaries at home and abroad.”⁵

On 26 September 2024, CAFCYBERCOM was established, elevating and transforming the Canadian Forces Information Operations Group from a level-three formation to a command, administratively supported by the Digital Services Group but reporting directly to the Chief of the Defence Staff.⁶ As the defence authority for cyber operations, it is responsible for the employment, generation, sustainment, management, and development of its allocated cyber forces, including signals intelligence (SIGINT) and joint electronic warfare.⁷

Although it is relatively well known in the defence community that the Communications Security Establishment (CSE) is the Government of Canada’s foreign signals intelligence agency,⁸ it is less well known that the CAF has its own integral SIGINT unit. Canadian Forces Station Leitrim has been conducting signals intelligence operations in the defence of Canada for almost 85 years.⁹ The inclusion of the CAF’s SIGINT organization into the new cyber command may, on the surface, seem unusual, given that it is an intelligence function and the CAF already had an intelligence command. However, SIGINT has a particularly important nexus with cyber operations. A nexus that is only growing and gaining relevance in the interconnected, technology-rich world in which the CAF operates. SIGINT and cyber are two sides of the same coin; although they have different purposes, authorities, and capabilities, they are inexorably linked and mutually reinforcing. This article serves as an introductory discussion of the relationship between SIGINT and cyber operations in the military context, with

the aim of illustrating their interdependencies and reinforcing nature, as they make their home in the new CAFCYBERCOM.

Lexicon

To begin this discussion, it is important to first define the terminology. Technological advancements in the information world tend to outpace doctrinal evolution. This means that there are no universally agreed-upon definitions for terms such as “cyberspace,” “cyber operations,” or the “cyber domain.” NATO, allies and partners have slightly different interpretations of these terms, and they are frequently used interchangeably. For this discussion, this article will reference the Department of National Defence’s Defence Terminology Bank for continuity.

Cyberspace and the Cyber Domain

Cyberspace is the “physical environment consisting of all assets that process, store or communicate digital data.”¹⁰ Unlike the other operational environments in which the CAF operates—land, sea, air and space—cyberspace is “omnipresent within all other environments.”¹¹ The cyber domain is a broader term that encompasses not only cyberspace but also the infrastructure that supports and enables it, as well as its users and their related activities.¹²

Cyberspace encompasses the cyber persona layer, which includes online profiles and other ways that people and things are represented online, while the cyber domain extends outward to include the actual humans who interact with cyberspace. Likewise, cyberspace encompasses the physical layer, including all computing hardware, phones, sensors, and data storage devices, while the domain captures that layer as well as the geographical layer, which represents the physical locations hosting the network devices and their surrounding environments.¹³

Cyber Operations

The term “cyber operation” encompasses a wide range of activities conducted in cyberspace aimed at achieving strategic and tactical objectives, which are subdivided into defensive cyber operations (DCO) and offensive cyber operations (OCO). DCO focuses on activities to preserve and ensure freedom of action within cyberspace,¹⁴ such as defending networks and data from adversaries. In contrast, OCO focuses on activities that project power through cyberspace to achieve specific effects.¹⁵ The intent of OCO is to disrupt, degrade, and/or destroy the adversary’s freedom of movement in cyberspace or to affect adversary activities or capabilities in other ways via cyberspace.

The growing dependence of state and non-state actors on cyberspace, its integrated information systems, and sensors has necessitated a proportional increase in cyber operations capabilities within the CAF. It is critically important that the CAF be able to defend its territory in cyberspace and leverage this

“Cyberspace encompasses the cyber persona layer, which includes online profiles and other ways that people and things are represented online, while the cyber domain extends outward to include the actual humans who interact with cyberspace.”

“It is critically important that the CAF be able to defend its territory in cyberspace and leverage this terrain to reach out and affect its adversaries.”

terrain to reach out and affect its adversaries. *Strong, Secure, Engaged: Canada's Defence Policy* sets out the expectation that the CAF's cyber forces are able “to target, exploit, influence, and attack [in cyberspace] in support of military operations”¹⁶ by leveraging emerging platforms across the land, sea, air and space domains for integrated sensor systems.¹⁷ The defence policy also highlights the requirement for the CAF to deny the adversary the ability to affect the CAF's command, control, communication, intelligence, surveillance, and reconnaissance (C4ISR) capabilities, which are necessary to enable CAF operations globally.¹⁸

Signals Intelligence

The term “signals intelligence” encompasses everything from the intelligence discipline itself and the activities conducted to collect information from cyberspace and other parts of the electromagnetic spectrum to the end products fed into the broader intelligence system.¹⁹ In essence, SIGINT is the interception, collection, decryption, translation, and analysis of communications and non-communications signals, as well as the production of

reports to enable the overall intelligence-gathering process.²⁰ Due to the sensitivity of this work, the processes, capabilities and products require special protection and handling and thus cannot be openly discussed.²¹

SIGINT is further broken down into three subcategories: communications intelligence (COMINT), electronic intelligence (ELINT), and foreign instrumentation systems intelligence (FISINT). COMINT is comprised of intelligence gathered from the interception of electromagnetic communications, such as voice or text, other than by the intended recipient.²² ELINT focuses on electromagnetic non-communications transmissions, such as from radar systems.²³ These types of transmissions can provide information about their source, such as the frequency used, pulse rate, and direction of arrival, among other characteristics.²⁴ The final category, FISINT, is a more specific field and is defined as “intelligence derived from the intercept of foreign electromagnetic emissions associated with the testing and use of aerospace, surface and subsurface systems.”²⁵ FISINT is used to collect intelligence concerning transmissions and data from missile and control systems, for example.²⁶ The three subcategories of SIGINT work together to provide the critical intelligence necessary to enable national and continental defence objectives and to inform national security operations, foreign policy, and cybersecurity.²⁷

SIGINT has a long, clandestine history, closely guarded by those charged with its execution, operating from the shadows to enable CAF operations since the Second World War.²⁸ A cornerstone of military operations, SIGINT provides insight into adversary intentions, capabilities, and activities, underpinning strategic decision-making, defending the continent, and enhancing situational awareness for deployed forces worldwide.²⁹

Like cyber operations, the role that SIGINT plays in CAF operations has only grown in relevance in the context of modern warfare, where technological advancements have reshaped the battlefield, military strategy and intelligence-gathering activities. The increasingly interconnected information environment creates vulnerabilities, allowing the SIGINT enterprise access to adversary communications, sensors and weapons systems to produce critical intelligence on capabilities and intentions. The dramatically increased use of information technology systems, integrated sensors, and command and control systems have compounded the relevance of SIGINT in the defence of CAF assets and the exploitation of our adversaries, paving the way for active defensive and offensive cyber activities to exploit these same adversary vulnerabilities.

The SIGINT-Cyber Nexus

SIGINT operations leverage cyberspace and its embedded technologies to exploit the adversary's reliance on digital communications, interconnected devices, and the pervasive use of sensors to generate intelligence across all operational domains, including cyberspace. Intelligence generated by these processes



A member of the Canadian Armed Forces parachute team, the SkyHawks, gives a wind reading before the parachute show on the beach in Cobourg, Ontario, on May 24, 2023.

Photo: MCpl Nedja Coutinho, Canadian Armed Forces

enables CAF operations at all levels, from the tactical to the strategic. The interception of adversary communications and sensor data provides real-time intelligence on adversary locations and movements across all domains (air, land, sea, space, and cyberspace), informing threat assessments and targeting cycles for decision-makers. At the strategic level, it shapes situational awareness by discovering adversary intentions, capabilities and emerging threats.³⁰

While SIGINT and cyber operations both involve the use of digital technologies and operate in the cyber domain, they differ in scope, methodology and objective. SIGINT is primarily focused on the passive collection of information and the analysis of signals, whereas cyber operations can be both passive and active. Defensive cyber operations focus on safeguarding information and communications systems from intrusion, proactively protecting and securing them and responding to attacks, while offensive cyber operations aim to penetrate, manipulate and exploit adversarial systems. However, conducting cyber operations requires a deep understanding of threat actors, digital infrastructure, and its potential vulnerabilities. SIGINT can support these activities by providing the intelligence needed to identify targets and assess threats.

SIGINT-enabled Cyber Operations

Cyber operations, whether defensive or offensive, rely heavily on accurate and timely intelligence. SIGINT serves as a foundational element in informing cyber operations by intercepting and analyzing communications and non-communications signals to identify vulnerabilities in systems, detect patterns of cyber activity and better understand threat actors. CAF cyber operators must be able to understand the topology of target networks, including how

“ SIGINT serves as a foundational element in informing cyber operations.”

systems are interconnected, the protocols used, and the locations and nature of vulnerabilities within these networks.³¹

For defensive cyber operations, SIGINT can be used to reveal the structure and behaviour of the digital environment, as well as the intent and capabilities of adversaries and other cyber threat actors. Moreover, SIGINT can contribute to threat intelligence by identifying indicators of compromise, allowing the CAF to harden systems, deploy countermeasures and respond to intrusions. For offensive cyber operations, SIGINT can inform target selection, timing and tactics to ensure that cyber actions are precise and effective.

SIGINT can also facilitate attribution—the process of determining who is behind a cyberattack. Attribution is achieved by correlating intercepted communications with known threat actor behaviour. This is especially important in the modern threat landscape, where state and non-state actors employ sophisticated methods to obfuscate their identities.

SIGINT is essential for mapping network topology and understanding cyber threats. Its role in cyber operations extends beyond interception, as it enables comprehensive analysis to inform strategic planning and shape situational awareness for decision-makers. For the CAF, this relationship is underscored by the grouping of both SIGINT and cyber units under the same command. The establishment of CAFCYBERCOM enables better communication and cooperation between these strategically essential capabilities.

Cyber Support to SIGINT

Canada's initial SIGINT evolution was based on two main objectives: leveraging its unique geography to enable sovereign defence and utilizing that unique geography, along with homegrown collection initiatives, to contribute to and benefit from the Five Eyes intelligence partnership with the United States, the United Kingdom, Australia, and New Zealand.³² These requirements still exist today. SIGINT is a team sport because the prevalence of information systems, sensors, and transmitters makes it nearly impossible to parse the digital tsunami generated from all these sources. Finding, decrypting, analyzing, and reporting on the right information to satisfy intelligence requirements to enable CAF operations is immensely challenging. Being able to share that burden with like-minded, collaborative nations increases the amount of data that can be processed and exploited. Without the partnership of Canada's allies, that challenge would likely be insurmountable, particularly when operations take place in cyberspace. Canada's size and proximity to adversarial countries provide a geographic advantage that is leveraged to deliver unique contributions, enhancing relevance in this domain, facilitating access to partner intelligence, and positioning Canada to utilize the full might of the Five Eyes, enabling CAF operations around the world.³³ In the evolving digital landscape, this partnership is more important than ever. By investing in both sovereign and integrated SIGINT infrastructure, Canada ensures that its contributions are not only supplementary but also provide distinct and valuable intelligence to both CAF and Five Eyes operations. These sovereign capabilities enable Canada to align its operations with national security priorities, thereby enhancing the relevance and impact of its intelligence. Their integrated nature also allows Canada to strengthen collective defence and information-sharing across the alliance.

SIGINT operations rely heavily on secure network infrastructure, telecommunications and radio-frequency communications, data flow from sensors, complex computing

functions, automation, data analysis and, most importantly, integration and communication with partners and allies. This infrastructure is spread across the nation and the world, creating a significant and enduring technical and security challenge. All this leverages cyberspace, and none of it would be possible without support from cyber operations. Adversary cyber operations pose a significant threat to CAF operations, including SIGINT, by denying or manipulating information, conducting rapid or sustained collection, or engaging in deception activities.³⁴

It is defensive cyber operations that ensure the freedom of manoeuvre in cyberspace for SIGINT operations while protecting the critical assets, systems and facilities required to seek out, find, analyze and disseminate SIGINT. Moreover, SIGINT and offensive cyber operations work together to identify access points and understand the terrain in cyberspace, enabling intelligence collection and the delivery of effects. This critical nexus between cyber and SIGINT operations ensures that both are effective and sustainable.

Conclusion

The establishment of CAFCYBERCOM reflects a deliberate recognition by the Government of Canada and the CAF that cyberspace is a contested operational environment in which the CAF needs to be able to manoeuvre, defend its terrain, and

deliver effects. In this context, integrating SIGINT and cyber capabilities under a single command is a logical response to the realities of modern conflict. As this article has demonstrated, SIGINT and cyber operations are deeply interdependent. SIGINT provides the intelligence foundation that enables effective defensive and offensive cyber operations, while cyber capabilities protect, enable and amplify SIGINT collection and analysis. Together, they form a mutually reinforcing cycle that enhances situational awareness, supports decision-making, preserves the CAF's freedom of action in all domains, and facilitates the projection of military power through cyberspace.

As threats continue to evolve in scale, sophistication and speed, the importance of this SIGINT-cyber nexus will only increase. Co-locating expertise, authorities and capabilities within CAFCYBERCOM positions the CAF to better integrate signals intelligence and cyber operations, strengthen partnerships with allies, and respond decisively in the omnipresent cyber domain. Ultimately, the effectiveness of the CAF's cyber forces will rest not in the strength of individual capabilities, but in the power of collaboration, integration and innovation.

Notes

- 1 Canada, *Strong, Secure, Engaged: Canada's Defence Policy* (Ottawa: Department of National Defence, 2017), 14.
- 2 Canada, *Strong, Secure, Engaged*, 72.
- 3 Canada, *Joint Doctrinal Note (JDN): Cyber Operations 2017-02 2-0* (Ottawa: Department of National Defence, 2017) 1-1.
- 4 Canada, *Our North, Strong and Free: A Renewed Vision for Canada's Defence* (Ottawa: Department of National Defence, 2024), 26.
- 5 Canada, *Our North, Strong and Free*, 26.
- 6 Canadian Armed Forces, *Military Organization Order 2025001-2025006*, 14 July 2025.
- 7 Department of National Defence, "DM/CDS Messages: A New Era for the Cyber Domain: Launch of the CAF Cyber Command, *The Maple Leaf*, 26 Sep 2024, Originally found at: <https://www.canada.ca/en/department-national-defence/maple-leaf/defence/2024/09/a-new-era-cyber-domain-launch-caf-cyber-command.html>.
- 8 Communications Security Establishment, "Mandate," Government of Canada, last modified 7 April 2021, <http://www.cse-cst.gc.ca/en/corporate-information/mandates>.
- 9 George T. Fraser and Rober Lynn Wortmann, *History of Canadian Signals Intelligence & Direction Finding* (self-published, 2005).
- 10 "Cyberspace," *Defence Terminology Bank*, record 694338, accessed 6 Feb 2026.
- 11 Canada, *JDN: Cyber Operations*, 2-1.
- 12 "Cyber Domain," *Defence Terminology Bank*, record 694360, accessed 6 Feb 2026.
- 13 Canada, *JDN: Cyber Operations*, 2-3-2.4.
- 14 "DCO," *Defence Terminology Bank*, record 693742, accessed 18 September 2025.
- 15 "OCO," *Defence Terminology Bank*, record 693752, accessed 18 September 2025.
- 16 Canada, *Strong, Secure, Engaged*, 65.
- 17 Canada, *Strong, Secure, Engaged*, 39, 109.
- 18 Canada, *Strong, Secure, Engaged*, 56.
- 19 Canada, *CAF SIGINT Primer* (Department of National Defence, April 2021), 1.
- 20 Canada, *B-GL-005-200/FP-001, Canadian Forces Joint Doctrine 2-0* (Ottawa: Department of National Defence, 2011) 1-16.
- 21 Canada, *CAF SIGINT Primer*, 1.
- 22 "COMINT," *Defence Terminology Bank*, record 3843, accessed 18 September 2025.
- 23 "ELINT," *Defence Terminology Bank*, record 507, accessed 18 September 2025.
- 24 Canada, *CAF SIGINT Primer*, 21.
- 25 "FISINT," *Defence Terminology Bank*, record 695891, accessed 18 September 2025.
- 26 Canada, *CAF SIGINT Primer*, 21.
- 27 Canada, *B-GL-005-200/FP-001, Canadian Forces Joint Doctrine 2-0*, 1-4.
- 28 Fraser and Wortmann, *History of Canadian Signals Intelligence & Direction Finding*.
- 29 Communications Security Establishment, "Foreign Intelligence," *Government of Canada*, last modified 6 April 2023, Originally found at: <http://www.cse-cst.gc.ca/en/mission/foreign-intelligence>.
- 30 Communications Security Establishment, "Foreign Intelligence." Originally found at: <http://www.cse-cst.gc.ca/en/mission/foreign-intelligence>.
- 31 Canada, *JDN: Cyber Operations*, 5-14.
- 32 Wesley Wark, "Favourable Geography: Canada's Arctic Signals Intelligence Mission," *Intelligence and National Security* 35, No. 3 (2020): 319-30, DOI: 10.1080/02684527.2020.1724629.
- 33 Maria A. Robson, "The Third Eye: Canada's Development of Autonomous Signals Intelligence to Contribute to Five Eyes Intelligence Sharing," *Intelligence and National Security* 35, No. 7 (2020), 954-69, DOI: 10.1080/02684527.2020.1768477.
- 34 Canada, *JDN: Cyber Operations*, 1-1.