



Members of HMCS Ottawa's operations department sit in the Operations Room of HMCS Ottawa while the ship sails in the South China Sea during Indo-Pacific Deployment on October 4, 2023.

Photo: Aviator Gregory Cole, Canadian Armed Forces Photo

Introduction to Government of Canada Cyber Basics: A Primer

ALEXANDRA GREEN AND DR. MATTHEW KELLETT

Alex Green served as the first ever Officer in Charge for the Fleet Cyber Team at Maritime Forces Pacific (MARFAC) from 2018 to 2020. She is currently pursuing a Ph.D. in War Studies at the Royal Military College of Canada, where she studies cyber terrorism. In 2024, she received the Franklin Pinch Award for her research on custom terrorist app development.

Dr. Matthew Kellett is Special Advisor, Canadian Armed Forces Cyber Command. He is a former commercial software programmer and defence scientist. His doctorate is in theoretical computer science, specifically on the design and analysis of distributed algorithms. He enjoys chess, running, and curling and is a former president of the Ottawa Curling Club.

The Canadian Armed Forces (CAF) and the Department of National Defence (DND) are rushing to meet the demand for cyber security capabilities. The CAF introduced the Cyber Operator trade in 2017,¹ and the Canadian Forces School of Communications and Electronics (CFSCE) announced the first graduating class in 2021.² Three years later, in September 2024, the CAF officially established the Canadian Armed Forces Cyber Command (CAFCYBERCOM). This command is the single DND/CAF authority for cyber operations, encompassing signals intelligence and joint electronic warfare. The creation of CAFCYBERCOM is significant because it consolidates several pan-domain efforts to leverage cyber capabilities into a single, transparent, unified chain of command, providing a “one-stop shop” for cyber expertise.

In the seven years leading to the stand up of the CAF Cyber Command, the CAF created a new trade and graduated its first Cyber Operator cohort. The CAF is investing in cyber capabilities. Staffing was once a challenge, but the number of qualified operators is growing. Despite this growth, a 2020 report by the Director General Evaluation, entitled “Evaluation of the Cyber Forces,” found that the “Cyber Forces have a sufficient number of positions; however, filling the positions has proven to be difficult” and points to challenges associated with hiring and retaining civilian talent, and matching cyber capability needs with the traditional approach to military professional development. The report specifically cited frustration associated with “the most experienced cyber personnel working for those who have little cyber experience.” The establishment of the Command should go a long way toward resolving these issues.

The situation is improving as the cyber operator trade matures and the Cyber Training Unit produces trained operators. While this capability is growing rapidly, basic cyber literacy in the rest of the DND/CAF has not kept pace. Defence Team members are often posted into positions requiring cyber knowledge without much background. Many of these uniformed members are not digital natives. It is understandable, given that the average age of a uniformed member in the CAF is 36 years old,³ and the World Wide Web became accessible to the broader public 30 years ago, meaning the average CAF member was not born into a world with the Internet. Most senior leaders in the Canadian Armed Forces are older than 30, so it is also fair to assume that many were not born into a fully Internet-connected and mediated world. They represent a generation of the CAF that must interact with cyber militarily, but for whom the Internet was once a novel idea that came about at the start of their careers. As the CAF expands and prioritizes cyber operations and capabilities, many CAF members must quickly adopt and understand cyber terminology.

There are, of course, many members of the Canadian defence community who are familiar with both technical and non-technical elements of cyber security. Those members might find this article to be a helpful refresher, although, for the most part, it is intended to serve as a welcoming primer to establish a baseline knowledge level for uniformed and non-uniformed members who have just been posted into a position where they engage with these concepts.

Aside from introducing some basic terms in a military framework, this article addresses common misconceptions these new team members might encounter. First, we discuss some common terms. While Government of Canada employees may have access to joint doctrine notes, the Defence Terminology Bank, and Termium, we believe that having terminology in one article, along with examples, will help new members adjust more quickly. We outline terms such as *cyberspace*, the *cyber environment*, the *cloud*, *cyber domain*, and *cyber* as an adjective. We then discuss how cyberspace is often viewed as a monolith and explain the nuances between different types of technology that fall under the

cyberspace umbrella. With these nuances in mind, we differentiate cyberspace from the information environment. The two are often confused because cyber teams are often asked to support information effects. We also explain the popular castle analogy, and how it can be used to understand the difference between cyber operations and network operations. The article finishes with two other key distinctions: the first between cyber security and cyber defence and the difference between a cyber event, cyber incident, and cyber attack. After completing this article, readers should have a solid foundation for more in-depth concepts and discussions.

Common Definitions and Terms

First, we explain common terms before diving into the nuanced differences between concepts. Any defence community member knows that the CAF and DND can be an alphabet soup full of acronyms and confusing terms. So, it is pertinent to address some standard terms readers might encounter in their work. For the CAF/DND, the *cyber operating environment*, *cyber environment*, or *cyberspace* for short, is a physical environment like sea, land, air, and space are physical environments. There is a physical infrastructure underlying and inseparable from the virtual world. Every piece of equipment a user touches is connected to another piece of physical equipment somewhere else, either through wires and fibre-optic cables or through photons sent through air and space. The cloud is not actually a cloud; it's usually a giant warehouse filled with networking equipment and computer servers running software that ensures data continues to survive even after the hardware it is stored on inevitably fails. So, instead of storing your data on your physical device, that data is stored on a server or group of servers and accessed over the Internet or some other large network. That's where our first buzzword, cloud, originated from. Network engineers, computer scientists, and other experts drawing network diagrams would conventionally use a cloud-like symbol to act as a placeholder for complex, underlying infrastructure that was outside of the organization's control. As organizations such as Amazon and Google began to offer computing resources remotely, the cloud was marketed as a new type of service delivery, as organizations would interact with those services without direct control of the infrastructure.

Next, the *cyber domain* is cyberspace, plus everything around it that supports it, including people, processes, and infrastructure. The Government of Canada uses this term to describe “all infrastructure, entities, users and activities related to, or affecting, cyberspace.”⁴ The cyber domain can include checking a new employee's identification before giving them their credentials to access the corporate network, the security of the rooms holding servers and networking equipment, and even the people who administer the network, which are all things vital to maintaining cyberspace, yet are not actually in cyberspace. Canada, NATO, and many allies have recognized the cyber domain as a

“*Cyber planning* is just military planning applied to the cyber domain; nothing is particularly cyber about it and it should just be called what it is: planning.”

domain of warfare, just like the maritime, land, air, and space domains. That recognition means the CAF must be prepared to carry out military operations in the cyber environment (i.e., cyberspace), and the CAF must be able to defend its part of the cyber domain.⁵

Cyber, then, is just an adjective, meaning that the thing it modifies is related to the cyber domain or cyberspace. Think about its use in terms of cyber security, cyber operations, and cyber incidents. *Cyber* also gets overused. In a military context, readers might hear people use the term *cyber planning* far too often. *Cyber planning* is just military planning applied to the cyber domain; nothing is particularly *cyber* about it and it should just be called what it is: planning. *Cyber* also should not be used as a noun or verb, although that often happens in informal speech. You should never write, “They should use cyber on this” or “We should cyber that.” In the next section, we will break down the *cyberspace* umbrella and then differentiate it from the information environment.

Breaking Down Cyberspace: OT, PT, and IoT Explained

While it is common practice to lump everything together under the term *information technology* or *IT*, the CAF/DND needs to be more precise about the components of cyberspace to manage them correctly. In CAF/DND, we use *IT* to refer to the traditional office and networking infrastructure to distinguish it from operational technology, which runs physical systems like pumps and heaters, and platform technology, which is operational technology on military platforms like ships, engine controls, and missile guidance systems. We can divide cyberspace into subcategories: information technology (IT), operational technology (OT), and platform technology (PT). It is also worth mentioning where Internet of Things (IoT) devices fit in among these categories. If you are new to the field, you will likely hear these terms used in reference to government assets. We’ve simplified the definitions below to help make the concepts more relatable.

Operational Technology (OT)

Operational technology is all about cyber-physical industrial systems. It includes industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems. In your home, the thermostat that controls your furnace is an example of OT. OT provides the interface between cyberspace and physical systems like valves, dampers, and fans on everything from heating, ventilation, and air conditioning (HVAC) equipment to fuel pipelines. While it is often possible to update the computer code of these systems, it usually only happens during infrequent overhauls or, in the worst case, when they are replaced. Sometimes, these systems are hard to update because they support critical systems. You wouldn’t want to shut down a water treatment plant or take safety systems offline at a nuclear power plant regularly to update their software.

In some cases, updating is difficult or impossible because the device is inaccessible. For example, you may have to drain portions of the water treatment plant to access certain equipment, or a critical control may be in a radioactive zone of a nuclear power plant. While OT systems connect cyberspace and physical systems, the best practice is to isolate them on their own networks and not, for instance, connect them directly to the Internet.

Platform Technology (PT)

Platform technology (PT) refers to the operational technology used on military platforms. It includes the hardware and software on ships, aircraft, vehicles, and weapon systems. Like your car, all the chips and wires used to control the functions of an armoured vehicle are examples of PT. PT often includes dedicated processors or chips that control the platform’s functions, like a missile guidance system. It is often nearly impossible to replace these chips, so any vulnerabilities in them exist for the lifetime of the equipment.

Because updating or replacing OT and PT is difficult, we need to ensure their security and ensure that updates don’t introduce vulnerabilities. This protection is part of a larger effort called *cyber mission assurance*, or CMA, which is defined by the Government of Canada as “a process to protect or ensure the continued function and resilience of mission-essential capabilities and assets, in the face of cyber threats or actions, in any operating environment or condition.”⁶ Essentially, CMA is the ability to conduct military operations with military capabilities that rely on cyberspace, which may be contested. In a Navy context, for example, a ship should still be able to use networks and technical capabilities to fight, float, or move in a cyber-contested environment. CMA can also mean ensuring these systems’ security and supply chains during their development and after they are fielded. Given that technical supply chains are often global in nature, there is always the risk that the systems, software, and technical capabilities the CAF acquires will eventually be



Members of 437 Transport Squadron help with the assisted departure of evacuees from Tel Aviv, Israel to Athens, Greece as part of Operation ION on October 15, 2023.

Photo: Corporal Charles Audet, Canadian Armed Forces Photo

exploited. Commanders who adhere to CMA principles must have contingencies to continue to pursue the mission regardless of the cyber threat.

Internet of Things (IoT)

Internet of Things (IoT) devices are becoming less expensive, more convenient, and easily adaptable, so it would not be surprising if IoT devices eventually provide some critical capability in a military operation. The Internet of Things includes low-end, consumer-grade IT and OT. Examples of IoT include smart lights, smart locks, smart appliances, Internet-connected thermostats, Internet-connected cameras, Internet-connected doorbells, and Internet-connected baby monitors. They often provide helpful capabilities, like using a camera to monitor your property or having your smart fridge order more milk when running low. IoT devices are often cheap, use low-powered processors, have minimal or no security, and can be difficult or impossible to update.

As the Canadian Armed Forces face a more complex threat environment and navigate challenging procurement processes, IoT devices, which were previously new and difficult to integrate, now offer easy solutions. However, these devices present a *cheap complexity problem*.⁷ Historically, if the Canadian Armed Forces wanted to acquire a specialized and complex machine or device, they would need to find a specialized supplier. The complex device would cost a great deal, given the effort and resources required to create it. However, things are different with IoT devices. Today, it's often less expensive to take a complex device and have it pretend to be simple, instead of actually building a simple device. By default, due to the economies of scale (it is cheaper to make millions of one item than to make a handful of bespoke items), vendors are incentivized to make IoT devices with

all the bells and whistles: WiFi, cloud storage, machine learning, complex software, Bluetooth, and microphones. But if an organization (such as the CAF) wanted that device for an operational capability without the WiFi connectivity, it is often cheaper and easier to turn off the WiFi connection than to manufacture a bespoke version without that feature. Nevertheless, that lingering feature is still a vulnerability, and as IoT devices are notorious for infrequent firmware updates, it may remain unpatched and open to exploitation.

These characteristics make IoT devices an ideal target for exploitation by malicious actors. For instance, the Mirai botnet was first noticed in August 2016. It took advantage of hundreds of thousands of poorly secured IoT devices, like baby monitors and Internet-connected cameras, to create a network that could flood targets with network packets in a distributed denial of service (DDoS) attack.⁸ While its initial target was *Minecraft*, it has been used for many other attacks and eventually had its source code released in an open-source code repository.⁹ Despite their security concerns, the use of these devices is increasing due to convenience. It would be unsurprising if they were to provide some critical capability in a military operation at some point in the future. If that's the case, we need to be aware of the risks involved, just as we should be of the risks involved in using them in our homes.

The Difference Between Cyberspace and the Information Environment

Readers new to the field might use *information environment* and *cyberspace* interchangeably. But, what is the information environment? The Government of Canada defines the information environment as "an environment comprised of the information itself, the individuals, organizations and systems that receive, process and convey the information, and the cognitive, virtual and physical space in which this occurs."¹⁰ Except that is not the only definition. There are several others, and the Canadian definition is not universal. For example, according to the Tallinn Manual, the comprehensive (but non-binding) academic survey of international law applicability to cyber warfare and cyber operations, the information environment is the "aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information."¹¹ The two definitions differ, as the Tallinn Manual description focuses on the actors and systems only, while the Government of Canada definition includes the actors, systems, and the environment they interact with. On that note, the Government of Canada definition explicitly mentions information as part of the system, while the Tallinn Manual definition does not mention information as a commodity. Furthermore, although the Government of Canada definition defines explicitly the information environment as an environment and emphasizes this context, the definition does not address the broader *environment* as a concept.

“ Unlike the maritime, land, air, space, and cyber environments, the information environment is not physical, although it does interact with the physical environment as a medium.”

Unlike the maritime, land, air, space, and cyber environments, the information environment is not physical, although it does interact with the physical environment as a medium. For example, if troops from country A deploy to allied country B to deter aggression from country C, and country C does not yet want to commit to traditional military action against country B, they can leverage the information environment. Country C could create social media accounts and bots to spread disinformation about country A's activities in country B: that country A troops are terrorizing the local population, leaving garbage, and committing crimes. In this example, all the comments the bots leave on social media are elements of the information environment. Country C uses hardware to enable the bots—servers to host the bot networks, store user data, logs, and power to integrate with social media apps—and that hardware is part of cyberspace. Some of that social media content might make its way to a newspaper, where those claims will be printed in physical form. Country B citizens will view those messages on physical devices, accessed via the Internet. Those devices are also part of cyberspace. If country B citizens believe those claims, and change their opinion about hosting country A, then the information environment has been altered.

This example also illustrates the distinction between information operations and cyber operations, which differ in their objectives and nature. Information operations are focused primarily on the information environment and changing how a target perceives information. Information operations are “coordinated information activities conducted in or through the information environment to create desired effects on the will, understanding and capability of individuals.”¹² There are a few critical elements to this definition: actions or operations must be deliberate and synchronized, with the intention to achieve specific outcomes or results and focus on people as the primary targets. Suppose Bob emails Alice about the highlights of his project with the intent to ask her for funding later. That email is an information operation because Bob positively changes her perception of the project.

While information operations intend to alter the subject's perception or behaviour, cyber operations are used to change the medium of cyberspace by allowing things that would usually be denied, intentionally or not, or to deny things that would usually be allowed, intentionally or not. Cyberspace is central to cyber operations. You cannot achieve a cyber operation without the infrastructure of cyberspace. Standard definitions highlight this connection. For example, the Government of Canada defines a cyber operation as a “set of planned actions in or through cyberspace intended to preserve freedom of action or create effects to achieve military objectives.”¹³ More plainly, the Tallinn Manual lists a cyber operation as “the employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace.”¹⁴ When we hear *cyber operations*, we tend to think of elaborate, Stuxnet-level capers. However, a cyber operation could be as simple as applying a patch to intentionally combat a known virus and, ultimately, changing cyberspace to improve network health.

Why are cyber operations and information operations often confused, and how do they relate? First, both aim to create effects, whether on the human psyche (information operations) or technical systems (cyber operations), and these effects can sometimes overlap. Some might assume that information operations are cyber operations because cyber operations could be used in conjunction with information operations. As mentioned, cyberspace is a medium that people use to access the information environment (e.g., using a computer to research). We often confuse cables, servers, and routers (the physical elements of cyberspace) with the information environment, because we can use them to communicate information. The two are also often confused because at one point, information operations and cyber operations were treated as the same category. The two concepts are further conflated because cyber-designated teams are usually tasked with affecting the information environment: a cyber operation can have information-related effects, and information operations can leverage cyberspace. For example, if Alice is still hesitant to fund Bob's project, Bob could hire Eve to send a key logger (a hidden app that records keystrokes and sometimes the screen) to infect Alice's computer and gather blackmail-worthy information. Bob could then use that information to influence Alice's decision. But it is possible to carry out that information operation entirely separate from cyberspace. For example, Bob could staple posters with disinformation about Alice's research to stir up unsupportive sentiment on campus.

There are ways to influence the behaviour or decisions of a target audience without cyberspace. We've used a fictional example here to demonstrate the difference between information and cyber operations, and the next section explores the popular castle metaphor to highlight the distinctions between cyber operations and network operations. The article then differentiates between cyber defence and cyber security.

“Beginners might encounter the fortress/castle metaphor as a simplified explanation of how a network or computer is secured.”

The Castle Metaphor: Cyber Operations and Network Operations

Beginners might encounter the fortress/castle metaphor as a simplified explanation of how a network or computer is secured. Using the metaphor, a defender can secure an asset behind layered defences, like medieval rulers who might fortify a structure with a moat and thick castle walls, perhaps rounded to prevent an adversary from scaling, with inner walls to zone the castle into different levels of access (outer bailey, inner bailey, keep). Even though the layers of defences reduce the risk of a breach, there is always the risk that an enemy force might try to breach the defences. Similarly, digging a moat and erecting castle walls does not mean the work is done. The defenders must evolve as their adversary evolves. If the walls protect from arrows and slings, there is no guarantee that the walls and moat will be sufficiently protected from catapults. Additionally, the defender must consistently maintain these defences. The walls must be repaired if damaged and manned to watch for enemies and anyone attempting to scale the walls.¹⁵

There are obvious parallels to a network. The castle walls are often likened to a firewall, allowing entrance to some but not others and providing a defensive perimeter. The inner castle walls are also similar to network zoning, in which different network parts are segmented according to privileged access. So, if an attacker breaches the castle walls, they may be unable to access the inner bailey or the keep. Requiring a password could be similar to lifting the portcullis. Like a castle, the network defences must constantly be updated as enemies evolve: network defenders must apply patches, update malware signature lists, and fine-tune their allow and deny lists. The process is never ending.

The defence can also be even more active. If you were to send your troops out beyond the wall to find the catapult and destroy it, we would call those actions *defensive cyber operations—response actions* (DCO-RA), which is just another way of saying self-defence in the cyber domain to ensure freedom of action.¹⁶ If you were to target the adversary's troops and to destroy their castle, or to capture their flag and plant your own, in the cyber world, we would call those *offensive cyber operations* (OCO), as it is an operation to “project power in or through cyberspace to achieve effects in support of military objectives.”¹⁷ In a cyber security context, that could look like overloading adversary

infrastructure with traffic to disrupt their ability to launch disinformation campaigns.

The castle analogy can also be used to articulate the differences between cyber operations and network operations. We've already touched on cyber operations, but network operations are understood to be the “activities undertaken to provision, secure, configure, operate, extend, maintain and sustain a network.”¹⁸ Following our castle analogy, these would be the general activities needed to sustain the castle: ensuring that the castle walls are maintained, resources such as food, water, and weapons are available, the doors function so people can enter and leave, and that guards are present to guard the castle walls and entrance. These functions are similar to the elements of network operations: firewalls, access control lists, bandwidth availability, and network administrators available to troubleshoot. If the castle walls are falling apart, it may be difficult to know if it is because of an attacker, or because the walls are so poorly maintained. The same can be said with network operations. If some devices are no longer connected to the network, it could be because a malicious actor has targeted them, or because the network operations centre did not update the firmware and the recent patch caused the devices to disconnect. If a network is poorly maintained, as a castle, then it is challenging to know readily whether an issue is routine or malicious.

However, there are general limits to the castle analogy. First, it establishes a dangerous dichotomy between *inside* and *outside*.¹⁹ Not all networks are clear-cut. For example, many networks have demilitarized zones (DMZs) where they host assets accessible to the Internet, yet cannot interact directly with internal databases. So, the DMZ is a type of intermediary zone that is protected by the firewall but is still not entirely internal. Second, the castle analogy suggests that all threats originate externally. While castles did not usually prioritize internal defences, modern networks often use role-based access controls to limit privileges once in the network. However, even with these controls, insider threats (Ortiz, Snowden, Reality Winner, Manning, etc.) prove that not all threats are external.²⁰

Cyber Security vs. Cyber Defence: Key Differences Explained

If you're new to cyber security in the Department of National Defence, you might've noticed that sometimes people use cyber security and defence interchangeably, despite the fact that they are entirely different terms within the department. Within the broader government, cyber security would be used to describe the processes for securing the IT portion of cyberspace. However, within DND, cyber security and cyber defence are divided. Unlike other departments, DND has platform technology and must defend that technology from adversaries in operational contexts. Cyber security provides the necessary foundation for all cyber defence activities, which could be part of the reason the

two terms often need clarification. Cyber security includes activities that ensure the health and safe storage of assets, regardless of the presence of a threat actor. Confidentiality, integrity, and availability are priorities. Confidentiality ensures that information is private and accessible only to the people granted permission to see it; integrity ensures that information stays accurate and unchanged; and availability means that users can access the information they need when needed, without delay or difficulty.²¹

In practice, cyber security could involve requiring users to use passwords to access assets or systems, using role-based access controls to control access and privilege (confidentiality), using checksums to check that the software is the proper version for download (integrity), requiring digital signatures (integrity), having a disaster recovery plan in the event of a natural disaster or emergency (availability), or monitoring the system's performance (availability).

So, how is cyber security different from cyber defence? Indeed, cyber security practices can help deter a threat actor from accessing, altering, or denying access to data. However, cyber defence is different because, unlike cyber security, it assumes the presence of a cyber threat actor and involves efforts to detect, prevent, and respond to threats against the network. A cyber threat or threat actor is central to this definition but absent from the cyber security definition.

While no analogy is perfect (as demonstrated earlier with the castle analogy), we can see the difference between the two concepts using a hockey reference. Cyber security is much like the net outside of a hockey game. The smaller the frame of the net, the harder it is for unwanted materials (including a puck) to enter the goal zone. Perhaps the net is still on the ice during public skate hours, and some toddlers wander in accidentally. Hopefully, rink maintenance staff will be present to keep the net intact and out of bounds. If an overzealous skater accidentally slammed into the goal and ripped the netting, rink maintenance staff would repair the tear so the net could function as needed. Maintenance staff will replace the frame if it rusts to preserve structural integrity. The same staff might then remove the net from the rink during public skating to ensure it is accessible for games. These practices are all similar to standard cyber security maintenance—ensuring that unwanted traffic is kept away from the network and that if the network is accidentally damaged, it is repaired and perhaps isolated from any other incidents that could impact network availability—all standard practices.

In contrast, cyber defence is analogous to a hockey game. The net can be thought of as cyber security. The better the cyber security, the smaller the net (and smaller the threat surface). The net can be made of better material, might have a robotic opening, replaced and renewed with every change, etc. All these adjustments make it more difficult for the opposing team to score. In this way, it is similar to cyber security practices, whereby network owners might adjust firewall rules and routinely apply patches to limit the network's threat surface. Nevertheless, like hockey, no

matter how well-crafted your net is (or cyber security practices), if you don't have a goalie, the adversary can easily score. Cyber defence is similar to adding a goalie. The home team puts a goalie in the net to keep pucks out. The bigger the goalie pads and the faster her reaction, the harder it is for the other team to score. The coach might brief the goalie and defence about the other team's forwards and the strategies or plays they like to use. The home team can then use this intelligence to prevent the other team from scoring. Similarly, with cyber defence, the network defenders can invest in malware signature detection tools (new equipment) to prevent a cyber threat actor from breaching the network. They might also use heuristic analysis, intrusion detection systems, or knowledge of techniques, tactics and procedures to identify specific threat actors, mitigate the threat, or improve response times. In this example, the team must take specific defensive actions to protect itself from the other team. However, unlike in a hockey game, cyber defence and cyber security are 24-hour efforts that never truly end. The difference between the two will also be useful for the next section, which outlines the gradient of cyber events, incidents, and compromises.

Distinguishing Cyber Events from Cyber Attacks: Understanding the Scale

Cyber activities or oddities sometimes get lumped together in the *cyber attack* pot. However, there are technical differences. We must distinguish between types of activities so we can scale responses. For example, if you're new to a team and get a phishing email (but didn't click on it) and claim that there's been a cyber attack, that label is wrong and also incorrectly escalates the activity. The Government of Canada uses definitions in the Government of Canada Cyber Security Event Management Plan to differentiate between types of activities.²² The main difference between the categories is the level of severity and our certainty that there was a compromise.

On the less significant end of the scale, we have a *security event*, which is any event that may have resulted in a compromise.^{23,24} Examples of security events include a spear phishing email that the target did not click on or unusual requests stopped by a firewall. While some of these events could be malicious, it's essential to recognize that an event is not the same as a compromise. If an organization treats every event as a breach, it will be overwhelmed by the number of alarms, leading to alarm fatigue, and precious resources will be stretched thin.

A security event can become a *security incident* when a breach occurs, and the system is compromised.²⁵ For example, if a cyber threat actor sends a spear phishing email to an employee and the employee clicks on an embedded malicious URL or opens an infected attachment and downloads malware, the security event (the email) becomes a security incident (successful malware download). The event transitions to an incident as soon as the network is compromised.

Conclusion

We have written for an audience new to the Government of Canada's cyber security community in the hopes of helping those readers identify common misconceptions they might encounter. After reading this article, we believe everyone should have the same foundational knowledge. Readers should see that cyberspace is a physical thing, mundane and unexciting as that might seem to some. The cyber domain is cyberspace and all the things that go around it. It is also one of the five recognized domains of warfare, one that the Canadian Armed Forces is actively operationalizing.

Is this article just splitting hairs? Why do we need an entire article to outline definitions already used in a web of Joint

Doctrine Notes, policy papers, annexes, glossaries, and slide shows? Why does it matter if we say *cyber operation* instead of *information operation* if most people know what we truly mean, anyway? The truth is that the CAF/DND are in a unique situation. Unlike the US, China, and Russia, they are building the foundation of critical military cyber capabilities. As CAF CYBERCOM stands up and several teams interact with this capability, it's important that everyone speaks the same language and uses terms appropriately to avoid confusion and miscommunication. Hopefully, the simplified explanations presented in this article provided a better understanding of how the cyber domain is put together, its relation to the other domains, and why it may actually be more straightforward than people believe it is.

Notes

- 1 Government of Canada, "Cyber Operator: The New Canadian Armed Forces Trade Badge," The Maple Leaf, January 11, 2022. Originally found at: <https://www.canada.ca/en/department-national-defence/maple-leaf/defence/2022/01/cyber-operator-canadian-armed-forces-trade-badge.html>.
- 2 "Congratulations to the First Cyber Operator Graduates from the CFSCE," The Maple Leaf, September 21, 2021. Originally found at: <https://www.canada.ca/en/department-national-defence/maple-leaf/defence/2021/09/congratulations-first-cyber-operator-graduates-cfsce.html>.
- 3 Government of Canada, "March 2020 - Canadian Armed Forces 101," Defence 101- Transition Binder 2020, n.d., 2. Originally found at: <https://www.canada.ca/en/department-national-defence/corporate/reports-publications/transition-materials/defence-101/2020/03/defence-101-caf-101.html>.
- 4 Government of Canada, "Cyber Operator: The New Canadian Armed Forces Trade Badge." Originally found at: <https://www.canada.ca/en/department-national-defence/maple-leaf/defence/2022/01/cyber-operator-canadian-armed-forces-trade-badge.html>.
- 5 Statistics Canada, "On Guard for Thee: Serving in the Canadian Armed Forces" (Government of Canada, July 13, 2022). Originally found at: <https://www150.statcan.gc.ca/n1/daily-quotidien/220713/dq220713c-eng.htm>.
- 6 Government of Canada, "Cyber Mission Assurance," in *Defence Terminology Bank*, n.d. Originally found at: https://www.btb.termiplus.gc.ca/tpv2alpha/alpha-eng.html?lang=eng&i=1&srchtxt=cyber+mission+assurance&codom2nd_wet=1#resultrecs
- 7 Bruce Schneier, "Security and Cheap Complexity," *Schneier on Security* (blog), August 26, 2022. Originally found at: <https://www.schneier.com/blog/archives/2022/08/security-and-cheap-complexity.html>.
- 8 "Heightened DDoS Threat Posed by Mirai and Other Botnets," CISA, n.d. Originally found at: <https://www.cisa.gov/news-events/alerts/2016/10/14/heightened-ddos-threat-posed-mirai-and-other-botnets>.
- 9 Scott J. Shackelford and Scott O. Bradner, "Have You Updated Your Toaster? Transatlantic Approaches to Governing the Internet of Everything," *Hastings Law Journal* 72, no. 2 (2021). Originally found at: https://repository.uchastings.edu/cgi/viewcontent.cgi?article=3921&context=hastings_law_journal.
- 10 Government of Canada, "Information Environment," in *Defence Terminology Bank*, n.d. Originally found at: <https://www.btb.termiplus.gc.ca/tpv2alpha/alpha-eng.html?lang=eng&i=1&srchtxt=information+environment>.
- 11 "Glossary," in *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press, 2013), 282.
- 12 Government of Canada, "Information Operation," *Termium Plus*, n.d.
- 13 Government of Canada, "Cyber Operation," *Termium Plus*, n.d.
- 14 "Glossary."
- 15 Deborah A. Frincke and Matt Bishop, "Guarding the Castle Keep: Teaching with the Fortress Metaphor," *IEEE Security & Privacy*, 2, no. 3 (2004): 69-72.
- 16 Government of Canada, "Defensive Cyber Operation - Response Action," *Termium Plus*, n.d.
- 17 Government of Canada, "Offensive Cyber Operations," *Termium Plus*, n.d.
- 18 Government of Canada, "Network Operations," in *Defence Terminology Bank*, n.d.
- 19 Christian Leuprecht, David B. Skillicorn, and Victoria E. Tait, "Beyond the Castle Model of Cyber-Risk and Cyber-Security," *Government Information Quarterly* 33, no. 2 (n.d.): 250-57.
- 20 Christian Leuprecht, David B. Skillicorn, and Victoria E. Tait.
- 21 National Institute of Standards and Technology, "NIST Special Publication 1800-26A" (National Cybersecurity Center of Excellence, 2020). Originally found at: <https://www.nccoe.nist.gov/publication/1800-26/VolA/index.html>.
- 22 Government of Canada, "Government of Canada Cyber Security Event Management Plan (GC CSEMP)" (Government of Canada, 2019). Originally found at: <https://www.canada.ca/en/government/system/digital-government/online-security-privacy/cyber-security-guidance-policy/management-security-incidents/government-canada-cyber-security-event-management-plan.html>.
- 23 Government of Canada.
- 24 National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," NIST, n.d. Originally found at: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>.
- 25 National Institute of Standards and Technology.