CYBER SECURITY AND THE RCN

Technology has always been a factor in how warfare evolves. Over the years, warfare changed as technology changed – new weapons meant increased range, speed, accuracy and lethality. Like civilians, militaries have increasingly come to rely on technology/computers, and cyber-security has become a major concern. Banks, businesses, industrial complexes, infrastructure, hospitals, airlines have all been hacked. Individuals and organizations have fallen victim to ransomware extortion, and government secrets have been leaked to the 'dark web.' Digital technology/computers are not inherently weapons. But as technology develops, so do ways of using them to gain advantage.

What exactly are we talking about when we discuss this topic? *Cyber-space* consists of interdependent Information Technology (IT) networks including the internet, telecommunication networks, computer systems, embedded microprocessors and controllers as well as the software and data that reside within them.[1] The *cyber-domain* includes all infrastructure, entities, users and activities related to, or affecting, cyber-space. A *cyber-threat* "is an activity intended to compromise the security of an information system by altering the availability, integrity, or confidentiality of a system or the information it contains."[2] *Cyber-security* is commonly defined as the protection of internet-connected systems such as hardware, software and data from cyber-threats. As new Royal Canadian Navy (RCN) ships are being built and the government adds cyber-warfare into defence policy, it's timely to look at this topic.

Is the RCN in danger? Is cyber-security applicable to the navy? What threatens Canadian warships? Who may exploit vulnerabilities, and under what circumstances? What is the RCN doing about all of this?

Cyber-security and the RCN

In the military context, the use of cyber-space has become crucial to operations. Warships require multiple computer networks. In warships, command and control, navigation, communication, mechanical equipment, propulsion, surveillance, situational awareness, emergency response and weapons are all tied into computers. Networks on warships facilitate communications with other ships, aerial assets and ashore facilities Thus, networks "control the machinery that enables a ship to float and move, they ensure safe navigation, they control the weapons systems and maintain the recognized maritime and air picture for timely command and control."[3] It is important to note that networks apply not just to the fleet but also to naval facilities ashore. The RCN consists of the fleet (crews and vessels) and the land-based facilities/supporting infrastructure ashore.[4] Both those entities are highly computerized.

---

[1] DND/CAF Joint Doctrine Note (JDN 2017-02) Cyber Operations.

[2] Canadian Centre for Cyber Security, An Introduction to the Cyber Threat Environment, CSE Canada, no date, file:///C:/Users/Anuta/Downloads/Intro%20to%20cyber%20threat%20environment%20CSEC.pdf

[3] Lieutenant-Commander J.M. Lanouette, "Naval Cyber Warfare: Are Cyber Operators Needed on Warships to Defend Against Platform Cyber Attacks?" Cdn Forces College, MA thesis, 2016.

[4] The land-based fleet supporting units include, for example: Maritime Forces Atlantic (MARLANT), the Naval Intelligence (Trinity), the Fleet Maintenance Facility (FMF), Canadian Forces Supply System (CFSS) and Naval

There are advantages to utilizing computers in the military. Computers never get tired or distracted or bored. They can continuously monitor position/location, surroundings, air quality and equipment, among many other things. More technology can mean less physically demanding work for personnel and, indeed, less personnel. Aside from allowing technology to do the dull, dirty and dangerous work, it also increases efficiency and productivity. Monitoring and surveillance can be conducted more effectively, data processing is quicker and easier, and information is exchanged more efficiently.

The demands of modern warfare also make it necessary to have computers to enhance human personnel. The dynamics of a modern combat, the speed and variety of weapon systems and the volume of tactical information far exceed the ability of a human operator to process and react. Shipboard computers enable decision-making by acquiring and processing information from sensors (radars, sonar, unmanned vessels, tactical data networks) and aid in employing weapons. As well, computers enhance communication, and Canada operates with allies so the RCN needs access to coalition intelligence and sensors.

But for every strength there can be a weakness. Naval systems are all connected to computers, and computers can be breached. Cyber-attacks could "disable military networks that control the movement of troops, the path of jet fighters, the command and control of warships."[5] Could the computers connected to military equipment (ships, helicopters, missiles, etc.) be hacked and with what implications?

Until recently, most cyber-breaches were related to user mistakes or accidents – i.e., a crew member inserted a USB stick that had a virus, or fell victim to a phishing attempt on a military computer. Breaches were a result of personnel who were careless or incompetent enough to inadvertently allow access. These are categorized as accidental and/or natural threats (eg., user's error or a power outage). But more recently, breaches are becoming associated with conscious acts by malicious actors. Potential adversaries – states (state proxies), criminal organizations, hacktivists, terrorists, thrill seekers and insiders[6] – are rapidly developing the means to exploit the vulnerabilities inherent in the systems.

States (i.e., their intelligence and military services) are the most sophisticated actors because they often have dedicated resources and motivated personnel. Although sometimes well-financed, cyber-criminals are usually less sophisticated and unlikely to target military forces because their motive is profit. But they could be utilized by state actors for their specialized technical capabilities. Hacktivists, terrorist groups and thrill-seekers often rely on available tools that don't require significant technical skill. Their actions usually have no lasting effect on their targets beyond reputation. Insider threats are individuals working within a military organization who are disgruntled or in need of money and allow access to a system, network, or device. They are dangerous because they are inside the security perimeter and have access to internal networks.

A cyber-attack targeting technology infrastructure or a denial-of-service attack on a weapon system could endanger the crew and the ship itself. As such, a cyber-attack should be considered in the same way as battle damage from conventional attacks. For example, a number of warships have had their GPS/navigation or their communications tampered with ('spoofed') and if you rely on computers to tell you where your ship is, then this could lead to collisions or grounding.

Ammo Depot.

[5] Mark Clayton, "The New Cyber Arms Race," *Science Monitor*, March 2011.

[6] Canadian Centre for Cyber Security, "An Introduction to the Cyber Threat Environment," CSE Canada, no date, file:///C:/Users/Anuta/Downloads/Intro%20to%20cyber%20threat%20environment%20CSEC.pdf

If a ship runs aground because of this, the ship is just as damaged as it would have been had it been hit by a torpedo.[7] As well, the inability to utilize shipboard computers will degrade warfighting capability, endanger the crew and ultimately may cause the mission to fail.

But to be considered damaging, a cyber-attack does not need to be as spectacular as ships going astray or missiles launching on their own. A corrupted database or a simple network outage at a Fleet Maintenance Facility may turn out to be just as bad. For example, a warship may not be able to sail to an operation because the engine did not receive a critical replacement part.

Even if there is no malicious breaching of computers, they can still break down. If your warship is high-tech and network-centric and the computer system crashes on a mission, that's a problem. A certain network resource could become unavailable when needed. Or a system may be intentionally shut down if an infection is suspected. Rebooting a system makes it temporarily unavailable, and the system does not satisfy operational requirements if it keeps rebooting continuously or even sporadically in the middle of a mission. As well, if a malfunction is detected, operators may lose confidence in the system and have to resort to manual control, thus reducing operational efficiency particularly if personnel are not trained in manual control. As well, we've all had our computers interrupt us with updates. What if the warship's computer system does an update in the midst of a battle?

Another relevant factor is the commercial origin of military technology. In the past, militaries often did their own research and development, and many of today's common items had origins in the military. But this is no longer the case. Now militaries rely on technology developed by private corporations and many elements of military computer equipment are purchased commercial-off-the-shelf (COTS). As the RCN began purchasing COTS computer systems, the cyber-security flaws inherent within them migrated into the naval vessels. This could include something as simple as the operating system for a ship's computers – i.e., Canadian warships rely on Microsoft Office, as does everyone else. That raises questions about security, particularly if software and/or hardware is made outside the country, and/or by unfriendly entities. There may be "weaknesses or flaws in the design, implementation, operation, or management of an information technology system, device, or service that provides access to cyber threat actors."[8] These actors may try to take advantage of flaws to install malware, or exploit the system. As new ships are built, it is important to ensure supply chain integrity.

RCN Response

The RCN recognizes the problem and has made cyber-security a priority. In addition to physical security, personnel clearance and security of communications, cyber-security has become an operational necessity. Cyber-security requirements are included in every design contract for new equipment for the navy. Cyber-security controls implemented in the fleet may include firewalls, domain separation, data encryption, enforcing strong passwords, multi-factor authentication, network monitoring, security awareness and education, anti-virus toolsets, software and firmware updates, data back-ups, comprehensive disaster recovery plan, and so on.

Like other navies, the RCN conducts threat risk assessments and attempts to manage the risk in the cyber-domain. As well as considering the policies of other states and best industry

[7] Tzvi Joffre, "U.S. warns of GPS interference, communications spoofing in Persian Gulf," *Jerusalem Post*, 8 August 2019.

[8] CSEC, "ITSG-33 Security Risk Management: A Lifecycle Approach," Ottawa: CSEC, 2012.

practices, the RCN has adopted ITSG-33 as its guidance for the authorization of systems for operation in the fleet.[9] ITSG-33 Annex A "Cyber Security Framework (CSF)" describes five core functions – Identify, Protect, Detect, Respond and Recover. As new threats regularly emerge, the risk cannot be completely eliminated but it can be reduced to an acceptable level through mitigation strategies. In order to reduce risk, the RCN incorporates cyber-security architecture into a ship's system design. Shipboard mission critical systems must feature strict access control, multi-layer encryption, regular data back-up, continuous network monitoring for any suspicious anomalies and robust respond and recovery procedures. Like individual Canadians buying security protection for their personal devices, the government buys and implements the cyber-security controls as required. And like Canadians, the navy has to continuously apply security updates and patches to stay on guard against new cyber -threats.

What happens after a problem has been detected? Then the navy must respond – on two levels, to the actor responsible and to the damage. A problem related to cyber-attacks is that attribution is extremely difficult and usually time consuming. As a military force, you want to be able to react but in the case of a cyber-attack you need to determine who did it before reacting, and that may take time and expertise. At the practical level, the response involves identifying the issue, containing the damage, deciding if secondary modes of operation should be initiated, and ensuring the system is brought back into service as quickly as possible. The response strategy includes isolating the system from external interfaces, rebooting in a safe mode, restarting applications, activating secondary modes of operation, and so on.

Conclusion

Modern naval equipment and sensitive data on government networks are being controlled via computers that, while increasing efficiency, introduce new vulnerabilities. The systems and platforms of the RCN, as well as the shore infrastructure, are subject to cyber-threats, which can include deliberate attacks, environmental disruptions, or human errors that can result in harm to the operations and/or the national interests of Canada. Cyber-defence has been adopted to protect naval personnel and RCN assets, to minimize risk and to achieve mission success. Without adequate protective measures, the RCN is vulnerable to cyber-espionage and disruptive cyber-operations.

As ships get more complex, they also get more expensive to build and to update. But navies/governments cannot ignore the technological elements, which are often a significant portion of the cost of a new ship. Cyber-warfare is not science fiction any more – it is today's reality. Cyber-security of the RCN cyber-space is an operational requirement.

[9] CSEC, "ITSG-33 Security Risk Management: A Lifecycle Approach." Management of Information Technology Security (MITS) is a policy put out by the Treasury Board Secretariat (TBS) which describes a high-level model for approaching security in Canadian government environments, including CAF/DND. MITS describes a Prevention, Detection, Response and Recovery model. This is similar to the US National Institute of Standards and Technology (NIST), "Cybersecurity Framework (CSF)," 2018, available at https://www.nist.gov/cyberframework/online-learning/five-functions.