Cyber Security and the RCN

As technology shifts and evolves, so too do warfare and weaponry. As much as technological developments have enhanced the efficiency of warmaking, they have also exposed it to new vulnerabilities. Specifically, just as the reliance of airlines, hospitals, businesses, and banks on computer systems has exposed such institutions to the risk of being hacked and breached, the ever-increasing computerization of navies means that those forces must confront a new potential avenue of threat and combat. Forces now contend not only with threats from the land, maritime, and air domains but also from the cyber domain.

A handful of definitions are required to inform this discussion. First, cyberspace entails Information Technology (IT) networks that are interdependent and that include, for instance, the internet, computer systems, telecommunication networks, and embedded controllers and microprocessors, in addition to the data and software they contain.[1] The cyber domain is comprised of all activities, users, entities, and infrastructure affecting or related to cyberspace, while 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] Finally, cybersecurity entails protecting data, software, hardware, and other systems connected to the internet from cyber threats. These are all concepts the RCN must consider as it constructs and procures new ships, and with which the Government of Canada must grapple as it seeks to integrate cyber warfare into the nation's defence policy.

The RCN, like the CAF more generally, has become increasingly reliant on the use of cyberspace for and in its operations. For instance, a modern warship has numerous computer networks, with command and control, communication (with other vessels, onshore facilities, aerial assets, and naval allies), propulsion, situational awareness, weapons, navigation, mechanical equipment, surveillance, and emergency response all relying on and utilizing computers. As such, 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] Cyber networks are thus imperative for a naval fleet's operation, as well as its interoperability with allied fleets. They are also critical to onshore naval facilities and supporting naval infrastructure,[4] which similarly have become increasingly computerized.

There are, of course, significant advantages to this computerization of fleets and their onshore supporting units. Computers are not subject to fatigue or boredom, and they are capable of continually monitoring a variety of elements, including a vessel's surroundings, equipment, location, and air quality. By enabling more effective surveillance and monitoring, in addition with faster and easier data processing and the more efficient exchange of information, the integration of technology into warships enhances their productivity and efficiency. Technology can also reduce the physically demanding tasks its personnel must perform and indeed even mean that the vessel requires fewer personnel to function. Given the complexity of contemporary warfare, computers are imperative to supporting and enhancing the operations of human personnel.

Computers acquire and process a wealth of information from radar, unmanned vessel, sonar, and tactical data networks, thus facilitating decision-making. Computers also assist in deploying and employing weapons. A human operator on their own, unassisted by technology, would be unable to process the sheer volume of tactical information or adequately react, given the variety and speed of the available weapons systems.

However, this widespread reliance on technology and computers also exposes militaries to vulnerabilities. Computers can be hacked and breached, and thus a cyberattack could potentially "disable military networks that control the movement of troops, the path of jet fighters, the command and control of warships."[5] Naval fleets are not immune from this susceptibility, given how thoroughly naval systems now rely on computers. Traditionally, most cyber breaches in the naval sector were accidental or natural in character, stemming from, for instance, a power outage or a crewmember who mistakenly allowed access to a military computer by succumbing to a phishing attack or inserting a virus-bearing USB stick. More recently, however, breaches have become predominantly linked to deliberate actions by hostile or malicious actors. There are a variety of actors that may harbour an interest in disrupting naval systems and operations, ranging from states/state proxies to hacktivists, from criminal organizations to terrorists, all of whom are developing methods and means of exploiting system vulnerabilities.

Hostile state actors (for instance, state military and intelligence services) tend to be the most sophisticated, thanks to their possession of motivated personnel and dedicated resources, while cyber criminals tend to be less sophisticated and, given their profit motive, less likely to target military forces.[6] Thrill-seekers, terrorist groups, and hacktivists often deploy available tools that do not need substantial technical skill, with typically little lasting effect on the targets beyond impacting their reputation. Insider threats, stemming from individuals within a military organization who permit access to a device, network, or system due to their desire for profit or on account of their discontentment with the organization, are more dangerous, since those individuals have access to internal networks and are inside the organization's security perimeter.

Given the breadth of naval systems that are now reliant on computers and technologies, a breach of any system could produce severe consequences. For instance, a cyberattack that targets a vessel's IT infrastructure, or a denial-of-service attack (an attack attempting to make a service or system unusable) on a weapons system, could imperil both the vessel and its crew. If a vessel's shipboard computers were taken out of use, the vessel's warfighting capability would be significantly diminished, endangering the crew and hindering the broader operation. Indeed, cyberattacks can be just as damaging as conventional attacks. For instance, recent years have seen hostile actors tampering with or "spoofing" vessels' communications and GPS systems. Given modern vessels' reliance on computers to position and locate themselves, this could result in groundings or collisions, causing significant physical damage.[7] Smaller, less conspicuous cyberattacks can be similarly damaging. For example, a corrupted database or network outage at a Fleet Maintenance Facility, while seemingly minor, could prohibit a vessel from sailing on an operation if it is unable to receive a key replacement part in time. Since computers are now integral to all aspects of naval operations, from the vessels' functioning to the control of their weapons systems and operations of their onshore support infrastructure, there are a variety of avenues a hostile actor could take to disrupt naval operations.

Naval computer systems are perhaps even more susceptible now to cyberattacks given the commercial origins of many military technologies. While, historically, militaries often conducted their own research and development processes, militaries today predominantly rely on technology developed by private corporations, with many elements of their computer equipment being purchased commercial-off-the-shelf (COTS). For instance, Canadian warships utilize a microsoft operating system. As these COTS computer systems are incorporated into naval vessels, so too are those systems' cyber-security flaws. Further security concerns may arise if hardware or software is produced internationally or by unfriendly actors, who may seek to exploit the system or capitalize on flaws to install malware. Ensuring the integrity of the supply chain is thus critical when procuring and constructing new vessels.

Cognizant of these vulnerabilities, the RCN has prioritized cyber security as an operational necessity. The RCN, like other modern navies, performs threat risk assessments and actively seeks to minimize its cyber-domain risks. Incorporating best industry practices and international state practices, the RCN has moreover established its own guidance for authorizing systems for use in its fleet, entailing the five central functions of Identify, Protect, Detect, Respond, and Recover. First and foremost, each design contract for new naval equipment includes cybersecurity considerations and requirements, and the RCN actively integrates cybersecurity architecture into its vessels' system designs to reduce risks. Mission critical systems on vessels are required to have strict access control, regular data backup, strong respond and recovery procedures, multi-layer encryption, and continual network monitoring for any dubious abnormalities or anomalies. Firewalls, data encryption, multi-factor authentication, security education and awareness, firmware and software updates, comprehensive disaster recovery plans, domain separation, network monitoring, anti-virus toolsets, data backups, etc. are all cybersecurity controls that the RCN has implemented in its fleet, with frequent security patches and updates keeping these systems guarded against emerging threats.

If an issue is detected, the RCN must respond to the damage caused as well as the actor that caused it. Oftentimes, identifying the source of a cyberattack is exceptionally difficult and time-intensive, but this attribution is imperative to be able to respond. A practical response to a cyberattack on a naval system thus entails identifying the problem, containing or restricting the damage, determining whether to initiate a secondary mode of operation, and returning the system to service as rapidly as possible. Responding to a cyberattack means segregating the system from external interfaces before rebooting in safe mode, relaunching applications, initiating secondary operation modes, etc. While cyber risks cannot be entirely eliminated, given the frequent and constant emergence of new threats, they can be minimized through such mitigation strategies.

Thus, while the computerization of naval equipment, systems, and networks has elevated their efficiency and productivity, it has also created new vulnerabilities. The naval systems of the RCN's fleet, aerial assets, and shore infrastructure are all susceptible to cyber threats, ranging from environmental disruptions and human error to intentional attacks, all of which can jeopardize naval operations and Canada's national interests. As such, the RCN has been incorporating cyber defence measures to protect its assets and personnel and reduce their risk of succumbing to cyber espionage and hostile cyber operations. Cybersecurity is now a major factor that the RCN must continue to consider to protect a its assets and operational capabilities.

References

[1] DND/CAF Joint Doctrine Note (JDN 2017-02) Cyber Operations.
[2] Canadian Centre for Cyber Security, "An Introduction to the Cyber Threat Environment," Communications Security Establishment Canada, https://open.canada.ca/data/en/dataset/27b59b82-b29b-42f8-8bd5-8ba18456bf31.
[3] Lieutenant-Commander J.M. Lanouette, "Naval Cyber Warfare: Are Cyber Operators Needed on Warships to Defend Against Platform Cyber Attacks?" (Master of Defence Studies thesis, Canadian Forces College, 2016).
[4] Maritime Forces Atlantic (MARLANT), the Fleet Maintenance Facility (FMF), Naval Intelligence (Trinity), the Naval Ammo Depot, and the Canadian Forces Supply System (CFSS) are examples of land-based fleet-supporting units.
[5] Mark Clayton, "The New Cyber Arms Race," *Science Monitor*, March 2011.
[6] Cyber criminals can, of course, be hired by state actors on account of their technical abilities.
[7] See, for instance, David Hambling, "Ships fooled in GPS spoofing attack suggest Russian cyberweapon," *New Scientist*, August 10, 2017, https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/#ixzz6fs3Aim1X; "GPS Spoofing Experiment Knocks Ship off Course," Inside GNSS, July 31, 2013, https://insidegnss.com/gps-spoofing-experiment-knocks-ship-off-course/.