National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

NAVIGATION BY THE (NAV)STAR – A STORY OF TECHNOLOGY RELIANCE

Lieutenant-Commander Maude Ouellet-Savard

JCSP 45

Exercise *Solo Flight*

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

PCEMI 45

Exercice *Solo Flight*

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES

JCSP 45 – PCEMI 45
MAY 2019 – MAI 2019

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

NAVIGATION BY THE (NAV)STAR – A STORY OF TECHNOLOGY RELIANCE

Lieutenant-Commander Maude Ouellet-Savard

"This paper was written by a candidate attending the Canadian Forces College in fulfilment of one of the requirements of the Course of Studies. The paper is a scholastic document, and thus contains facts and opinions, which the author alone considered appropriate and correct for the subject. It does not necessarily reflect the policy or the opinion of any agency, including the Government of Canada and the Canadian Department of National Defence. This paper may not be released, quoted or copied, except with the express permission of the Canadian Department of National Defence."

« La présente étude a été rédigée par un stagiaire du Collège des Forces canadiennes pour satisfaire à l'une des exigences du cours. L'étude est un document qui se rapporte au cours et contient donc des faits et des opinions que seul l'auteur considère appropriés et convenables au sujet. Elle ne reflète pas nécessairement la politique ou l'opinion d'un organisme quelconque, y compris le gouvernement du Canada et le ministère de la Défense nationale du Canada. Il est défendu de diffuser, de citer ou de reproduire cette étude sans la permission expresse du ministère de la Défense nationale. »

NAVIGATION BY THE (NAV)STAR – A STORY OF TECHNOLOGY RELIANCE

INTRODUCTION

Our world without technology is something that has become impossible, or for many even unimaginable. Access to information now knows no bounds, and the availability of smart phones, televisions, computers and the internet has become ubiquitous in most regions around the globe. Technology in all its forms is present everywhere, and in everything we do. It is widely accessible, interactive, and has altered our daily lives in immeasurable ways through connectivity, increased rapidity to achieve results and automation of processes. For instance, technological evolution has been omnipresent in the maritime and shipping world. From dugout canoes to tall ships, from trans-oceanic steam powered vessels to nuclear powered submarines and modern warships, technological advances through our history have been remarkable in all extents of marine construction, propulsion, power generation, weapons and sensors. The bridge of a ship is but one area that has seen technological progresses change the fundamental ways in which the maritime sector operates, including the navies of the world. This evolution has resulted in a reliance on modern digital or electronic tools such as global navigation satellite systems (GNSS) and electronic charting.

Nevertheless, no matter how positive the changes have been in the last century, the prevalence of technology has also opened the door for the exploitation and manipulation of systems and network weaknesses by adversaries, ill-intended actors, activists or even simply by folks curious to see where a path can lead. "The interconnectivity that ties all devices and systems to the internet has invited malicious forces into the mix, exposing users and businesses to a wide range of threats."[1] Cyber security is a growing concern for governments, businesses and individuals, and militaries are not exempt from computer-generated dangers. "Maritime companies face significant cyber threats as they adapt their navigational, operational and other equipment to the digital world."[2] The Royal Canadian Navy (RCN) is in essence one of those maritime companies that has adapted its equipment and processes to modern technology and that could face the same dangers as it replaces its traditional skill set. Confronted with this reality, the question of how prepared the RCN is to face the current and emerging challenges of a technology-reliant maritime navigation era poses itself. This paper will argue that training has veered too far off from fundamental concepts in the past, that Her Majesty's Canadian ships (HMCS) bridge teams have grown overly-dependent on the available technology and that they are insufficiently aware of the possible threats they may face in the safe navigation of modern warships. Of note, in order to keep the content at the unclassified level, conceptual examples are used in parts of the paper. Furthermore, as this is a short essay, the scope of the research is limited to navigation systems and processes only, and does not include a study of the Industrial Control Systems (ICS) or the Combat Management Systems (CMS) common to modern warships.

The first section of this essay will review the technological advances that have affected maritime navigation in Canadian warships and discuss the ways the RCN has altered its navigation training and processes to adapt to the new technology, with particular attention placed on fundamental concepts and practices as per the qualification

[1] Trend Micro, "Security Risks in a Technology Driven World," last modified 18 October 2017, https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/security-risks-in-a-technology-driven-world.

[2] Judy Greenwald, "Marine Sector Struggles with Cyber Risks: Navigation Systems Vulnerable to Attack," *Business Insurance* 48, no. 10 (2014): 30.

standard and plan (QSP) for Naval Warfare Officer (NWO) courses. The following section will first study the strengths and weaknesses of three key pieces of equipment part of the integrated navigation system and how they have impacted the proficiency of bridge teams. Finally, the last section will study the broader maritime industry's emerging threats, which foreshadow the challenges HMC ships may by the same token face. The global examination of the RCN's approach to electronic navigation and looming challenges will thereby highlight the organization's inadequacies in preparing for the future operating environment knocking at our doors.

SECTION 1 – ADAPTING TO MODERN TECHNOLOGY

What Isaac Newton intended by saying in a 1676 letter: "[if] I have seen further, it is by standing on the shoulders of giants,"[3] is still as relevant today as it was back then, if not more. Progress and 'seeing further' has been made possible by those who have come before and who have inspired their contemporaries to keep forging ahead in their fields. This cumulative knowledge has resulted in an ever-increasing rate of progress and innovation. In most spheres of research, at a certain point "some new technology is introduced, and a much shorter time span elapses before the next technological development takes place."[4] Thus, it is to be expected that, "in the future, each generation will be more dramatically outpaced than the generation before it, [and that] we will understand even less about the technologies of the day than our parents understand about today's technologies."[5] Similarly, tools and technology that are taken for granted today will be put aside and replaced by new knowledge and equipment as generations follow one another. Such a process is called generational obsolescence and has become a fact of life that also resonates in the maritime environment.

Evolution of Navigation Equipment

Since the Age of Exploration in the fourteenth century to today's globalization setting, the shipping industry has grown to become responsible for approximately ninety

[3] Jordan Tinney, "On the Shoulders of Giants – Celebrating our Past, Building our Future," *Ed – Praxis* (blog), 15 May 2015, https://www.jordantinney.org/on-the-shoulders-of-giants-celebrating-our-past-building-our-future/.

[4] Arlindo Oliveira, *Digital Mind: How Science is Redefining Humanity* (Cambridge: MIT Press, 2017) 19.

[5] *Ibid*., 5-6.

percent of trade around the world.[6] Finding ways to improve safety, security and efficiency in the maritime industry were critical to enabling the rise of trade by sea. Ships are larger, faster and more powerful than ever before, and necessitate the tools allowing them to proceed from a port to another safely and efficiently. As the proverb goes, *necessity is the mother of invention*, or at least a significant driver in it, and the greater needs demanded for the art of navigation to evolve.

Originally, sailors would follow a coastline, staying within sight of land when manoeuvering between destinations in order to avoid getting lost at sea. "Navigation was in many ways a leap of faith."[7] Slowly, seafarers, mathematicians and scientists invented a series of apparatuses to expand the field of sea operations and they opened the door to a world of discovery by enabling ships to sail towards the unknown. These technological advances, such as the compass, the sextant and the chronometer, have since multiplied and can be sorted in one of the four principal methods of navigation that have marked history until the arrival of electronic navigation (e-navigation).

The earliest method used, and most basic, was the dead reckoning (DR), which consists in estimating the ship's future position based on its course, speed and travelling time.[8] It was later supplemented with celestial navigation. The observation of astronomic bodies had long been used at sea, on land and in the air to orient oneself; however it only grew into a widespread practice in the fifteenth century when the calculations and

[6] International Chamber of Shipping, "Shipping and the World Trade," last accessed 20 April 2019, http://www.ics-shipping.org/shipping-facts/shipping-and-world-trade.

[7] Megan Garber, "8 Tools we Used to Navigate the World Around Us Before GPS and Smartphones," last modified 15 April 2013, https://www.citylab.com/life/2013/04/7-examples-how-we-used-navigate-world-around-us/5286/.

[8] National Geographic, "Navigation," last updated 21 January 2011, https://www.nationalgeographic.org/encyclopedia/navigation/.

equipment became more accessible.[9] Similarly, as charts became more common, visual navigation using points of reference on land facilitated navigation in coastal areas. The next most significant method came in the twentieth century with the development of radio navigation where radio wave transmissions are broadcasted and measured to determine an object's position. It includes systems such as DECCA, Loran (long range navigation) and the radar.[10] This method marked an operational shift where for the first time input external to the ship was used to determine its position and identifies the departure point from traditional navigation techniques.

Naturally, the technology continued to evolve quickly and a space element was soon included. Thus, the global navigation satellite systems (GNSS) were launched in the later part of the last century and resulted in precise positioning, navigation and timing (PNT) through the American Global Positioning System (GPS) in 1995. With the exception of the radar, "satellite-based radio navigation"[11] has for the most part supplanted its ground based predecessors and the equipment onboard HMC ships reflects this reality. To complement satellite-based positioning, an inertial navigation system (INS), defined as a "navigation aid that uses a computer, motion sensors, and rotation sensors to continuously calculate the position, orientation, and velocity of a moving object without the need for external references"[12] was developed and fitted onboard HMC ships to provide a continual dead reckoning of the ship's position.

[9] Henry Doyle, "Plotting a Course Through History: A Navigation History Timeline," last modified 22 May 2016, https://slidex.tips/download/plotting-a-course-through-history-a-navigation-history-timeline#.

[10] Michael W. Richey *et al*, "Navigation - Technology," last accessed 20 April 2019, https://www.britannica.com/technology/navigation-technology.

[11] IGI Global, "What is GPS," last accessed 20 April 2019, https://www.igi-global.com/dictionary/using-unmanned-aerial-vehicles-to-solve-some-civil-problems/12406.

[12] Department of National Defence, *Inertial Navigation Systems eHandbook*, (Esquimalt: Royal Canadian Navy, 2018), 8.

These steps in the evolution chain have given rise to today's e-navigation era. E-navigation is defined by the United Nations International Maritime Organization (IMO) as the "harmonized collection, integration, exchange, presentation and analysis of marine information on board and ashore by electronic means to enhance berth to berth navigation […] for safety and security at sea and protection of the marine environment."[13] The role and interaction of the key components of the integrated navigation system at the center of e-navigation will be discussed in more details in the second section of this paper. At any rate, the integrated nature of e-navigation meant a revamping of navigation processes was necessary.

Evolution of Navigation Training and Processes

The digitalization of navigation fixing aids empowered the introduction of the computerized consolidation and display of information, such as with electronic charts and Automated Radar Plotting Aid (ARPA), to enhance decision making and safety at sea. The new equipment and their associated opportunities compelled the RCN to re-evaluate its way of training and operating on the bridge.

According to a former Senior Maritime Instructor at the Naval Officer Training Center and current Command and Leadership Division Commander at the Naval Training Development Centre (Pacific), the training system was initially slow to react to the introduction of e-navigation in the late 1990s and early 2000s. While a conversion course was put in place for the bridge watch keepers (BWKs) of the fleet to familiarize themselves with the electronic chart system itself, the individual training for junior

[13] International Maritime Organization, "E-Navigation," last accessed 19 April 2019, http://www.imo.org/en/OurWork/Safety/Navigation/Pages/eNavigation.aspx.

officers was not comprehensively reviewed in that period. In 2005, in a late knee-jerk reaction, the training centre considerably shifted the focus of NWO courses[14] from paper charts and traditional navigation techniques towards electronic navigation processes.[15] It was a period of limbo where not enough was known yet about electronic navigation to provide wide-ranging training and education to the students, but where fundamental concepts were no longer being taught in depth either. Moreover, those who were the students early in the decade had become the supervisors by the late 2000s. Combined with more limited opportunities to consolidate learning at sea because of the commencement of Halifax Class Modernization project, the navy realized within a few short years that a gap in knowledge and skills had grown in its junior officers. In 2012, an overhaul of the NWO courses was initiated to address training deficiencies and restore a balance between traditional and electronic proficiency.

Confirming how poorly fundamental navigation concepts were understood by NWOs in the fleet, the RCN has recently reintroduced teaching paper navigation basic concepts at the NWO II level, which is the entry course to the navy for all seagoing officers.[16] The familiarization earlier in the career is trusted to help build mental muscle memory that junior officers can fall back on when the environment is sub-optimal. It should assist preventing BWKs from becoming ineffective when their equipment or fixing aids are degraded "by unanticipated changes in the environment and unanticipated changes in how systems perform."[17] Furthermore, it is anticipated that celestial

[14] NWO courses were formerly known under the name MARS until 2018 for the occupation they represented: Maritime Surface and Sub-Surface Officers.

[15] Commander A. Aujla (Retired), telephone conversation with the author, 30 April 2019.

[16] Royal Canadian Navy and Department of National Defence, *Qualification Standard and Plan – Maritime Surface and Sub-Surface 00207* (Ottawa: National Defence, 2016), 4-93.

[17] Jim Garamone, "DOD Must Train for 'Degraded' Environments, Official Says," *American Forces Press Services*, last updated 9 February 2011, https://archive.defense.gov/news/newsarticle.aspx?id=62750.

navigation theory will be included at the NWO IV level in the near future, which will enable ships' navigators to practice the concepts with their team instead of being the sole point of reference onboard. Likewise, thorough information about HMC ship's integrated navigation systems, as well as knowledge about bridge resource management (BRM), was added on the course to become a Fleet Navigating Officer (FNO).[18] These actions contribute to rebuilding resiliency and expertise depth in the fleet for the years to come.

Acknowledging the skill and know-how shortcomings that have affected the latest generation of sailors in a technology dominated environment, the RCN has taken further steps to bridge the gap. As such, a large scale Combat Training Review[19] was initiated in 2016 by the Naval Personnel Training Group in collaboration with Sea Training Group to include all the naval operator trades. Both the training structure and content are being reassessed in order to ensure the navy is "Ready to Help, Ready to Lead, Ready to Fight."[20] While it is an encouraging stride towards improved human-machine integration, the multiple training iterations of the past two decades indicate that significant efforts will be needed to break the cycle and achieve technology enabled, versus technology dependant, bridge teams. The next section of this paper will study the principal navigation equipment used by BWKs, including their possible vulnerabilities and the risks they can pose to navigation.

[18] Latest FNO QSP from 2015 does not yet reflect the addition of INS in the course curriculum; it is however being taught to FNO courses since 2018.

[19] Naval Personnel Training Group Headquarters, *Naval Combat Training Programme Review – NPTG HQ 9982-4500-1* (Esquimalt: NPTG HQ, 17 March 2016), 1.

[20] Royal Canadian Navy and Department of National Defence, *RCN Strategic Plan 2017-2022* (Ottawa: National Defence, 2016), 1.

SECTION 2 – VULNERABILITIES IN NAVIGATION EQUIPMENT

It is undeniable that contemporary warships are highly sophisticated platforms composed of a variety of computerized systems that optimize their three fundamental requirements to float, move and fight. It is however important to realize that most of the technology that has revolutionized navigation in the past thirty years was developed when "bandwidth was very expensive or Internet didn't exist,"[21] especially onboard ships at sea. Apprehension about an adversary's ability to jam, spoof or disrupt new systems was thus much lower than it is in today's context. What is now observed as vulnerabilities in the systems has therefore only been a concern in the recent past. By the same token,

> researchers say they have discovered significant holes in the three technologies sailors use to navigate: GPS, marine Automatic Identification System (AIS) and a system for viewing digital nautical charts called Electronic Chart Display and Information System (ECDIS).[22]

The employment of this equipment in the RCN, connected via the Navigation Data Distribution System (NDDS), as well as their inherent weaknesses affecting safety of navigation, is detailed below.

Modern Equipment in HMC Ships

Global Positioning System

GPS is widely accessible, offers continuous position and speed indication, and achieves an average user range error of "≤0.715 m (2.3 ft.), 95% of the time."[23] This accuracy level is significantly superior to any other system that preceded it. However, its

[21] Jeremy Wagstaff, "All at Sea: Global Shipping Fleet Exposed to Hacking Threat," last modified 23 April 2014, https://www.reuters.com/article/us-cybersecurity-shipping/all-at-sea-global-shipping-fleet-exposed-to-hacking-threat-idUSBREA3M20820140424.

[22] *Ibid.*

[23] GPS.Gov, "GPS Accuracy," last modified 5 December 2017, https://www.gps.gov/systems/gps/performance/accuracy/.

signals are easily disrupted by interference from radio transmitters. They are also extremely weak, making GPS susceptible to jamming[24] and, if not encrypted, they can easily be spoofed with the intention to deny service or deceive the adversary.[25] Deception spoofing[26] was demonstrated in 2013 when

> a research team from the University of Texas at Austin (UT) successfully hijacked an $80 million dollar superyacht using a $2000 device the size of a small briefcase. The experimental attack forced the ship's navigation systems to relay false positioning information [… and the] device had successfully set the vessel off-course by several degrees, all without tripping a single alarm on the ship's navigational alert systems. [27]

In addition, certain natural phenomena like geomagnetic storms and ionospheric scintillations can uncontrollably affect the transmission of signals to the satellite system, degrading GPS accuracy and reliability.[28]

Russia, which like China and Europe has developed its own GNSS, has since 2016 increased its GPS jamming and spoofing activities in its surrounding waters such as the Baltic and Black Sea, both for training purposes and denial-of-service operations.[29] With satellite constellations increasing in numbers, the risk of a state that owns its own GNSS being willing to attack another state's GNSS may also grow and HMCS ships have to be ready for it. Onboard modern ships, GPS provide input into a variety of systems to

[24] C4ADS, Above Us Only Stars: Exposing GPS Spoofing in Russia and Syria (Washington, DC: C4ADS, 2019), 10, https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/5c99488beb39314c45e782da/1553549492554/Above+Us+Only+Stars.pdf. "GNSS Jamming is the deliberate transmission of signals on frequencies used by GNSS in an effort to prevent receivers from locking-on to authentic GNSS Signals."

[25] Orolia, "Resilient Positioning, Navigation and Timing (RPNT)," last accessed 21 April 2019, https://www.orolia.com/our-company/resilient-pnt.

[26] C4ADS, Above Us Only Stars: Exposing GPS Spoofing in Russia and Syria, 10. Deception GNSS spoofing is "when an attacker mimics authentic GNSS Signals in order to hijack target GNSS receiver tracking loops […], feed false positioning or timing information to the target receiver, and covertly misdirect the receiver and its platform to some desired location."

[27] *Ibid.*

[28] NOAA, "Space Weather and GPS," last accessed 24 April 2019, https://www.swpc.noaa.gov/impacts/space-weather-and-gps-systems.

[29] Elisabeth Braw, "The GPS Wars Are Here," last modified 17 December 2018, https://foreignpolicy.com/2018/12/17/the-gps-wars-are-here/.

include ECDIS, AIS, gyros, radars, INS and more.[30] Any degradation of the satellite systems thus has substantial impacts on the integrated bridge system (IBS).

The absence of a robust back-up system to rely upon when a vulnerable GNSS is disrupted is prompting some nations to revisit World War II technology. Countries such as Britain, Russia, South Korea and the United States are exploring updated and electronic versions of the Loran technology. The eLoran would be considerably more difficult to jam as the average signal is an "estimated 1.3 million times stronger than a GPS"[31] or other similar constellation signal, thus providing a reliable alternative if sufficiently developed. Perhaps an even more promising option would be to invest in self-contained quantum compass navigation,[32] which can overcome the fragility of satellite-based radio navigation systems.

Nonetheless, even when no external actors intentionally work to degrade GPS signals, anomalies can occur. The 2014 collision between cargo vessels MV *Francisca* and RMS *Bremen* in the river port of Kiel in Germany is a prime example of this. It was found in the incident investigation that both vessels' AIS and ECDIS had indicated the ships passing clear of each other, despite the damage sustained in the collision. It was later discovered that a GPS anomaly or signal shadowing had offset the input in the navigation equipment.[33] This incident as well as the rise in jamming and spoofing

[30] Martin Bransby, "Innovation: An Alternative to GNSS for Maritime Positioning," last modified 1 November 2018, https://www.gpsworld.com/innovation-an-alternative-to-gnss-for-maritime-positioning/.

[31] Jonathan Saul, "Cyber Threats Prompt Return of Radio for Ship Navigation," last modified 7 August 2017, https://www.reuters.com/article/us-shipping-gps-cyber-idUSKBN1AN0HT.

[32] Hayley Dunning, "Quantum 'Compass' Could Allow Navigation without Relying on Satellites," last modified 9 November 2018, https://phys.org/news/2018-11-quantum-compass-satellites.html.

[33] Federal Bureau of Maritime Casualty Investigation, *Collision in the Kiel Firth at Friedrichsort Between the MV FRANCISCA and MV RMS BREMEN on 5 September 2014* (Hamburg: Ministry of Transport and Digital Infrastructure, 2015), 33.

occurrences both reiterate the necessity for BWKs to continuously validate the integrity of their systems, and more specifically the ship's position, by all available means.

Electronic Chart Display and Information System

ECDIS was first introduced to the Canadian naval fleet in 1997[34] with the installation of the Electronic Chart Precise Integrated Navigation System for Warships (ECPINS-W) still in use today. [35] An ECDIS "offers many advantages over paper charts, such as real-time display of information, easier passage planning, prompt danger alarms and overall enhanced navigational safety."[36] It receives feeds from the ship's positioning systems, such as GPS and INS, in order to provide a continuous indication of the ship's position on the electronic chart. ECPINS-W has the additional capability to overlay a radar image which adds an extra layer of information and redundancy for the bridge team. Despite these advantages, ECDIS also possesses several weaknesses.

In most instances, the software is installed on standardized commercial off the shelf (COTS) components for ease of use and reduced costs. They are then connected to an IBS such as the NDDS, but not linked to external networks or Internet; ECPINS-W runs on Windows 7 onboard HMC ships. As a result of its relative stand aloneness, removable media is routinely used to upload chart updates and navigation plans, which can lead to contamination by malware. When time is limited and changes to the ship's program are frequent, it is easy for a navigator to skip the air gapping process required by the Canadian armed Forces (CAF) information technology (IT) security procedures. Nevertheless, even if scrubbing is performed, some viruses such as badBIOS[37] are immune to the process and can still disrupt a computer's operation without network

[34] Commander A. Aujla (Retired), telephone conversation with the author, 30 April 2019.

[35] OSI Maritime Systems, "About," last accessed 20 April 2019, https://osimaritime.com/about/.

[36] Ship Technology, "ECDIS: Is the Industry Ignoring an Important Update?" last modified 7 March 2018, https://www.ship-technology.com/features/ecdis-is-the-industry-ignoring-an-important-update/.

[37] Dan Goodin, "Meet "badBIOS," the Mysterious MAC and PC Malware that Jumps Airgaps," last updated 31 October 2013, https://arstechnica.com/information-technology/2013/10/meet-badbios-the-mysterious-mac-and-pc-malware-that-jumps-airgaps/.

access. Windows being the "most malware-ridden platform out there"[38] raises concerns for the health of the ECPINS-W in the long run. Software updates are essential to ensuring the most up to date security parameters are present. Of note, the RCN has not yet adopted the ECPINS-W 6.2 upgrade released in 2017.[39]

Furthermore, being an "entirely electronically based system, [ECDIS] can therefore fail outright and can also develop faulty operations."[40] To mitigate the risk, the IMO has mandated that a backup to the primary ECDIS be carried in ships. It is generally complied with by having an identical second ECDIS, which eases the transition when need be, as done in the RCN. Considering that the alternate system requires being loaded with the same information as the primary, the likelihood of both computers being compromised is high and defeats the purpose of having the redundancy.

Lastly, ECDIS uses vector electronic navigation charts, which means that the charts are made of multiple layers that can be interacted with and filtered to show or hide information. Depending of the scale used, the system automatically removes or adds features. For instance, when zooming out, certain symbols will disappear to reduce clutter on the display. BWKs setting their display to the wrong scale can have dire consequences as hazards to shipping can easily be missed, whereas on paper or raster charts the image is fixed. Equally, ECDIS could revert to an abnormal, and non-IMO compliant, mode if the wrong settings or charts are selected. BRM training to avoid such mistakes is indispensable.

[38] Chris Hoffman, "Why Windows Had More Viruses than Mac and Linux," last updated 21 September 2016, https://www.howtogeek.com/141944/htg-explains-why-windows-has-the-most-viruses/.

[39] Navy Recognition, "Navies Upgrade to OSI's ECPINS Warship 6.2 Naval Navigation and Tactical Software," last modified 3 May 2017, https://www.navyrecognition.com/index.php/news/defence-news/2017/may-2017-navy-naval-forces-defense-industry-technology-maritime-security-global-news/5172-navies-upgrade-to-osi-s-ecpins-warship-6-2-naval-navigation-tactical-software.html.

[40] Andy Norris, "The ECDIS Mindset," *Seaways*, (January 2012): 8.

Automatic Identification System

AIS are "designed to be capable of providing information about the ship to other ships and to coastal authorities automatically"[41] by exchanging continuous transmissions in the Very High Frequency mobile marine band. The information is also "shared in a global shipping database via satellite communication."[42] Vessel Traffic Services use this information to monitor and deconflict maritime traffic in their areas of responsibility. AIS, by providing static and dynamic data about ships, are a valuable tool to build situational awareness that can also aid in collision avoidance when used as an additional input for the BWKs.

Nonetheless, an analysis of AIS by cyber security firm Trend Micro identified three macrocategories of threats affecting the system: "spoofing, hijacking and availability disruption."[43] For example, a vessel's data could be technically valid while being false, leading to a misleading representation of that ship's position, direction or speed. Similarly, spoofing of a distress beacon, navigation aid or even a ship via AIS can force vessels into manoeuvering to an adversary's desired location. This could lead vessels into harm's way or result in diplomatic incidents. Likewise, hackers can hijack a system to alter the information transmitted by a vessel, aid to navigation or ground station, without the broadcasting unit being aware of the erroneous data it disseminates. Malicious possibilities are endless with the AIS protocol's lack of verification of content information, only validating format. It is thereby critical to reinforce sound navigation

[41] International Maritime Organization, "AIS Transponders," last accessed 20 April 2019, http://www.imo.org/en/OurWork/Safety/Navigation/Pages/AIS.aspx.

[42] Marc Lanouette, "Naval Cyber Warfare: Are Cyber Operators Needed on Warships to Defend Against Platform Cyber Attacks?" (Joint Command and Staff Programme Master of Defence Studies, Canadian Forces College, 2016), 14.

[43] Marco Balduzzi, Kyle Wilhoit, and Alessandro Pasta, A Security Evaluation of AIS (Irving, Texas: Trend Micro, 2014), 6.

practices that include the correlation of multiple sources of information when making assessments and decisions at sea.

What Does it Mean for the Fleet?

Although there are no statistics available to qualify the competence of BWKs who underwent training since the adoption of e-navigation, some trends were noted. One of the main shortcomings identified was the junior officers' poor ability to understand the principles behind how the information is generated by the electronic systems. For example, ECDIS can automatically provide the turning data when planning a course alteration and plot it on the route.[44] It used to be drawn by hand, ensuring BWKs and navigators were very familiar with the turning rates of their ship. This enabled them to adjust the plan seamlessly to account for the dynamic environment, traffic or other unexpected conditions. By having the software compute the data automatically, junior officers do not recognize or anticipate as well how their ship manoeuvres through the water, unless they are specifically educated on the principles of advance and transfer. Similar data for tidal and current information can be automatically fed to the system, generating recommended courses.[45] The automation of the process removes the demand on the planner to become intimately conversant with all aspects of their passage, as expected of a professional mariner, increasing the risk of unforeseen outcomes during the execution.

Equally, by letting AIS, ARPA and relative velocity functions of modern radars govern their assessment of ships' movement in the vicinity, BWKs struggle in developing

[44] Department of National Defence, CFCD 130, *Canadian Navigation Manual* (Ottawa: National Defence, 2014), 46.

[45] Department of National Defence, CFCD 131, *Bridge Watchkeeping Manual for the Royal Canadian Navy,* chapter 12 (Ottawa: National Defence, 2017), 56.

their ‘seaman’s eye’. Hence, they make decisions based on a system that may not have yet registered a slight change in another vessel’s aspect or speed. As warships are often tasked to operate at high speed in confined waters and in close proximity to other ships, the ability to visually assess the relative movement of contacts and objects is critical. Slower reaction times from watch keepers can therefore be expected when the system fails or does not provide coherent information, increasing risks of collision and accidents.

Another concerning aspect of technology dependence is that by constantly relying on a certain piece of equipment to think for them, instead of using it to validate their own assessment, watch keepers are less likely to identify when a system fault is present. It is a vulnerability that could easily be exploited by an adversary. Ultimately, by constantly depending on bridge equipment and sensors to find a solution to a problem or situation, junior officers fail to develop the capacity to think fast and the aptitude to correlate various pieces of information mentally to make sound decisions in higher stress or degraded environments.

Although it was earlier identified that the training centre was making strides in addressing these deficiencies, it cannot be expected that the requirement stops there. Command teams and navigators are to enforce navigation standards with their teams so the muscle memory built during individual training does not atrophy over time. Despite demanding time and effort, frequent collective training aimed at challenging bridge teams in all aspects of navigation, including traditional techniques, is essential in maintaining the mental agility necessary to prevent risky situations, or react to them efficiently when they do happen. At the moment, there are very limited requirements for ships to practice operating in degraded environments according to CFCD 102(L), the current RCN

Combat Readiness/Training Requirements directive that dictates the activities a ship has to complete in order to be considered ready for its assigned mission.[46] Complacency due to dependency on technology for the sake of convenience is an insidious vice that is difficult to reverse once bad habits are formed. More focus geared towards this issue is recommended for collective training in the fleet.

The positive about the vulnerabilities identified in this section is that the RCN is aware of them and in a position to do something to mitigate them. The next section will look at a wider range of challenges experienced in the broader maritime domain that the RCN could as well soon be confronted with.

[46] Department of National Defence, B-GN-002-000/RQ-001, "CFCD 102(L) Royal Canadian Navy Combat Readiness/Training Requirements" (Ottawa: National Defence, 2016).

SECTION 3 – AWARENESS OF EMERGING THREATS

Whereas GPS denial is often the first thing that comes to mind when discussing degraded operating environments, it is only one of many conditions that can be much more subtle. To date, warships have generally been spared from cyber-attacks or the likes, contrary to the civilian shipping industry, which also plays a critical role in international stability. “Current reliance on digital communication, automation and the interconnectedness of the global economy make cyber security not only an issue of national security but of global security.”[47] In order to better understand what threats lay ahead for the RCN, it is critical to study what has already been experienced in the broader maritime domain.

Takeaways from the Civilian Maritime Industry

As stated by David Patraiko, the Director of Projects at the Nautical Institute in London, “for most companies, the greatest threat comes from the naivety of their own employees, on ship and ashore.”[48] An employee can inadvertently connect an electronic device in an accessible port to charge it, without thinking of what system this port is part of or how it can be affected. Similarly, the improved connectivity in ships increases access to social media, and opens the door to spear phishing. As such, individuals who possess specific knowledge may be targeted with ransomware and forced to divulge protected or sensitive information about the business to a malicious actor. Knowledge being power and information being currency, shipping companies are particularly mindful of the data theft menace posed by hackers. Equally, an individual may be

[47] Oliver Fitton *et al*, *The Future of Maritime Cyber Security* (Lancaster, UK: Lancaster University Faculty of Science and Technology, 2015), 1.

[48] David Patraiko, “Making Sense of Cyber Security,” *The Navigator*, no. 12 (June 2016): 2.

targeted via social media for having expressed negative views about their employer, and then be convinced to commit an attack against them. To mitigate these risks, the Chief Marine Technical Officer at the Baltic and International Maritime Council recommends that training and awareness programs should be implemented at all levels of the hierarchy, both for personnel on the ship and ashore.[49] It is consistent with the Global Maritime Issues Monitor report from 2018 that indicates that cyber-attacks and data theft are the most likely issues to happen within the following ten years, while also being the issues the maritime industry feels the least prepared to face.[50] As there is no code of practice about cyber security internationally established by an organization such as the IMO, each country and each company attempts to navigate the threat landscape as best they can.

On the other hand, in the current environment of budgetary constraints and declining work force levels, an optimization and reduction of crew sizes is unavoidable. “Technology is a logical substitute for personnel due to its availability, continuous improvement, speed of operation, capacity for information exchange, and complete integration with human systems.”[51] An increase in automation and computerized systems to manage sensors and routine machinery operation is to be expected as new platforms are developed and built. While it allows for some savings in human capital, it also increases areas of opportunity for system vulnerabilities to be exploited as there is less human supervision of operations. This reduced interaction demands a rigorous scrutiny of

[49] Aron Frank Sorensen, “The Lowdown on Cyber Security,” *The Navigator*, no. 12 (June 2016): 7.

[50] Global Maritime Forum, “Global Maritime Issues Monitor 2018,” last accessed 2 May 2019, https://www.globalmaritimeforum.org/publications/global-maritime-issues-monitor-2018 .

[51] Bernd Kulmus, “Reduced Crewing: Design Considerations,” in *Human Capital and the National Shipbuilding Procurement Strategy*, ed. Ian Wood (Halifax, NS: Dalhousie University Centre for Foreign Policy Studies, 2015), 80.

the supply chain so faults and malware can be detected early in the procurement process and before the equipment is installed. Prevention is vital in cyber security.

From the RCN Perspective

In an effort to increase sailors' quality of life at sea, HMC ships were recently fitted with nearly ship-wide connectivity. While strict policies were applied at the same time as the implementation of Wi-Fi onboard, the RCN is to remain prudent to avoid complacency in IT handling taking root. In that aspect, being a naval vessel is not different from any other ship at sea and the vulnerabilities are the same. However, the aftermaths of attacks could differ between the two groups. Where the global economy is more likely to be impacted by an attack on the civilian shipping industry, national or international security will more likely be affected with a cyber-attack on a naval vessel.

With regards to automation, the RCN is not immune to the challenges posed by a declining work force as it struggles to recruit and retain members.[52] The organization is continuously trying to optimize the employment of its sailors, and to find alternatives to personnel accomplishing certain tasks. For example, artificial intelligence (AI) is being developed to create a virtual Boatswain's Mate onboard ships. With this system, "the intent is more similar to a private business trying to reduce the need for workers through the use of new technology."[53] Contrasting with the civilian maritime industry, a balance between automation and human-machine integration is even more important in a warship.

[52] Lee Berthiaume, "Shortage of Sailors a Cause for Concern for the Royal Canadian Navy," last modified 14 February 2019, https://globalnews.ca/news/4960812/shortage-of-sailors-navy/.

[53] James McLeod, "Canada's Navy Is Developing an AI Voice Assistant for Warships, but Don't Worry: It Won't Control the Weapons," last modified 1 May 2019, https://business.financialpost.com/technology/canadas-navy-is-developing-an-ai-voice-assistant-for-warships-but-dont-worry-it-wont-control-the-weapons.

The ethical liability related to the employment of weapons and the missions naval vessels are assigned require human decision-making that cannot be delegated to computers. The restructuration of the various skills in seagoing positions with the amalgamation of various occupations into the Naval Weapons Technician, Maritime Technician and, eventually, Naval Combat Operator trades is thus a smart initiative. It enables the RCN to remain versatile while being able to scale crews based on the mission given to a ship.

On a different note, the CAF, supported by civilian partners, is equipped with a robust mission assurance team whose role is to dig into the multiple layers of the supply chain for every major procurement projects. Despite not every piece of equipment purchased by the organisation going through the rigorous review process, significant efforts are made to mitigate the risk of obtaining compromised equipment.

To sum up, while some of the challenges faced by the civilian maritime industry may not be directly applicable to the RCN or vice versa, the security mindset and a requirement for awareness programs apply to both. Lessons identified in either sector of the broader maritime domain should therefore be leveraged in order to prevent and mitigate future threats.

CONCLUSION

In the fast pace of today's technological developments, it cannot be forgotten that to be a warship, a ship needs to be able to float, move and fight. Thus, the role of navigation as a key combat enabler allowing the ship to fight and defend itself cannot be understated. Furthermore, with the RCN being a relatively small navy, each ship is likely worth more to Canada on the international stage than its actual dollar value. The organization cannot afford to lose the use of any of its major surface ships by reason of naivety or complacency related to navigation technology or cyber security. As such, failing to heed the warning signs from the larger maritime community will be detrimental to forthcoming naval and joint operations.

Throughout this paper, the review of navigation training in the RCN has confirmed that the organization had dissociated itself from foundational knowledge in an attempt to rapidly adapt to modern technology at the turn of the century. Nevertheless, it has also revealed the navy's acknowledgement of the capability gap that ensued and its efforts to reintegrate traditional skills and concepts to strengthen the next generation of NWOs. Similarly, the research has shown that the balance between teams being enabled by, and not dependent on, technology had not been struck yet and needs to remain a focus for collective training onboard ships. Finally, it became clear that RCN should take advantage of the wisdom and experience gained by the broader maritime industry to raise its members' awareness of the threat landscape and the role they can play to prevent dire outcomes.

Perhaps when considering the future operating environment it would be wiser to leverage technology as a means to teach the fundamental knowledge and concepts that will enable the RCN’s operators to perform in any condition of technological degradation rather than for watch keepers to depend on the technology to accomplish their duty. And as stated by Doctor Norris, a Fellow of the Nautical Institute and the Royal Institute of Navigation, “maintaining good navigational practice significantly lowers the risk of being dangerously mislead by both miscreant equipment and humans.”[54] Therefore, carefully trained and informed sailors will result in the Royal Canadian Navy being rightly prepared to face the challenges of the future, eventually.

[54] Andy Norris, “Spoofing and Hacking – Thwarted by Competent Navigation,” *The Navigator*, no. 12 (June 2016): 10.

BIBLIOGRAPHY

Botunac, Ive and Marijan Gržan. Analysis of Software Threats to the Automatic Identification System. *Shipbuilding* 68, no. 1 (2017), 97-105.

C4ADS, *Above Us Only Stars: Exposing GPS Spoofing in Russia and Syria*. Washington, DC: C4ADS, 26 March 2019. https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/5c99488beb39314c45e782da/1553549492554/Above+Us+Only+Stars.pdf.

Canada. Department of National Defence. *Inertial Navigation Systems eHandbook*. Esquimalt: Royal Canadian Navy, 2018.

Canada. Naval Personnel Training Group Headquarters. *Naval Combat Training Programme Review – NPTG HQ 9982-4500-1*. Esquimalt: NPTG HQ, 17 March 2016.

Canada. Royal Canadian Navy and Department of National Defence. Canadian Forces Classified Document 130, *Canadian Navigation Manual*. Ottawa: National Defence, 2014.

Canada. Royal Canadian Navy and Department of National Defence. Canadian Forces Classified Document 131, *Bridge Watchkeeping Manual for the Royal Canadian Navy,* chapter 12. Ottawa: National Defence, 2017.

Canada. Royal Canadian Navy and Department of National Defence. *Qualification Standard and Plan – Maritime Surface and Sub-Surface 00207*. Ottawa: National Defence, 2016.

Canada. Royal Canadian Navy and Department of National Defence, *RCN Strategic Plan 2017-2022*. Ottawa: National Defence, 2016.

Dombrowski, Peter and Chris C. Demchak. "Cyber War, Cybered Conflict, and the Maritime Domain." *Naval War College Review* 67, no. 2 (2014): 70-96.

Fitton, Oliver, Daniel Prince, Basil Germond, and Mark Lacy. *The Future of Maritime Cyber Security.* Lancaster, UK: Lancaster University Faculty of Science and Technology, 2015.

Germany. Federal Bureau of Maritime Casualty Investigation. *Collision in the Kiel Firth at Friedrichsort Between the MV FRANCISCA and MV RMS BREMEN on 5 September 2014.* Hamburg: Ministry of Transport and Digital Infrastructure, 2015.

Greenwald, Judy. “Marine Sector Struggles with Cyber Risks: Navigation Systems Vulnerable to Attack.” *Business Insurance* 48, no. 10 (2014): 1, 30.

Hareide, Odd Sveinung, Øyvind Jøsok, Mass Soldal Lund, Runar Ostnes, and Kirsi Helkala. “Enhancing Navigator Competence by Demonstrating Maritime Cyber Security.” *Journal of Navigation* 71, no. 5 (2018): 1025-1039.

International Maritime Organization. “International Convention for the Safety of Life at Sea.” 1 November 1974.

Jensen, Lars. "Challenges in Maritime Cyber-Resilience." *Technology Innovation Management Review* 5, no. 4 (2015): 35-39.

Jurdzinski, Miroslaw. “Changing the Model of Maritime Navigation.” *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation* 12, no. 1 (2018): 35-41.

Kulmus, Bernd. “Reduced Crewing: Design Considerations.” In *Human Capital and the National Shipbuilding Procurement Strategy*, edited by Ian Wood, 78-80. Halifax, NS: Dalhousie University Centre for Foreign Policy Studies, 2015.

Lanouette, Marc. “Naval Cyber Warfare: Are Cyber Operators Needed on Warships to Defend Against Platform Cyber Attacks?” Joint Command and Staff Programme Master of Defence Studies, Canadian Forces College, 2016.

Lawson, Lauren. “An Analysis of the Factors Inhibiting ECDIS from Effectually Achieving its Intended Primary Function of Contributing to Safe Navigation.” Master’s Research Dissertation, University of Cape Town, 2018.

Mileski, Joan, Christopher Clott, and Cassia Bomer Galvao. “Cyberattacks on Ships: A Wicked Problem Approach.” Maritime Business Review 3, no. 4 (2018): 414-430. https://doi.org/10.1108/MABR-08-2018-0026.

Norris, Andy. “Spoofing and Hacking – Thwarted by Competent Navigation.” *The Navigator*, no. 12 (June 2016): 8-10.

———. “The ECDIS Mindset.” *Seaways*, (January 2012): 1.

Oliveira, Arlindo. Digital Mind: How Science is Redefining Humanity. Cambridge: MIT Press, 2017.

Patraiko, David. “Making Sense of Cyber Security.” *The Navigator*, no. 12 (June 2016): 2.

Pazouki, Kayvan, Neil Forbes, Rosemary A. Norman, and Michael D. Woodward. "Investigation on the Impact of Human-Automation Interaction in Maritime Operations, *Ocean Engineering* 153, (April 2018): 297-304.

Pietrzykowski, Zbigniew, Piotr Wolejsza, and Piotr Borkowski. "Decision Support in Collision Situations at Sea." *The Journal of Navigation* 70, no. 3 (2017): 447-464.

Sorensen, Aron Frank. "The Lowdown on Cyber Security." *The Navigator*, no. 12 (June 2016): 6-7.

Svilicic, Boris, Junzo Kamahara, Matthew Rooks, and Yoshiji Yano. "Maritime Cyber Risk Management: An Experimental Ship Assessment." *Journal of Navigation* (2019): 1-13.

Thombre, Sarang, M. Zahidul H. Bhuiyan, Patrik Eliardsson, Björn Gabrielsson, Michael Pattinson, Mark Dumville, Dimitrios Fryganiotis, et al. "GNSS Threat Monitoring and Reporting: Past, Present, and a Proposed Future." *The Journal of Navigation* 71, no. 3 (2018): 513-529.

Zăgan, Remus, Gabriel Raicu, Radu Hanzu-Pazara, and Stănică Enache. "Realities in Maritime Domain regarding Cyber Security Concept." *Advanced Engineering Forum* 27, (2018): 221-228.

Websites

Berthiaume, Lee. "Shortage of Sailors a Cause for Concern for the Royal Canadian Navy." Last modified 14 February 2019. https://globalnews.ca/news/4960812/shortage-of-sailors-navy/.

Bransby, Martin. "Innovation: An Alternative to GNSS for Maritime Positioning." Last modified 1 November 2018. https://www.gpsworld.com/innovation-an-alternative-to-gnss-for-maritime-positioning/.

Braw, Elisabeth. "The GPS Wars Are Here." Last modified 17 December 2018. https://foreignpolicy.com/2018/12/17/the-gps-wars-are-here/.

Center for Strategic and International Studies Event on Cyber Warfare in the Maritime Domain. Washington: CQ Roll Call, 2017. https://search.proquest.com/docview/1941427908?pq-origsite=summon.

Doyle, Henry. "Plotting a Course Through History: A Navigation History Timeline." Last modified 22 May 2016. https://slidex.tips/download/plotting-a-course-through-history-a-navigation-history-timeline#.

Dunning, Hayley. "Quantum 'Compass' Could Allow Navigation without Relying on Satellites." Last modified 9 November 2018. https://phys.org/news/2018-11-quantum-compass-satellites.html.

Garamone, Jim. "DOD Must Train for 'Degraded' Environments, Official Says." *American Forces Press Services*. Last updated 9 February 2011. https://archive.defense.gov/news/newsarticle.aspx?id=62750

Garber, Megan. "8 Tools we Used to Navigate the World Around Us Before GPS and Smartphones." Last modified 15 April 2013. https://www.citylab.com/life/2013/04/7-examples-how-we-used-navigate-world-around-us/5286/.

Global Maritime Forum, "Global Maritime Issues Monitor 2018," last accessed 2 May 2019, https://www.globalmaritimeforum.org/publications/global-maritime-issues-monitor-2018 .

Goodin, Dan. "Meet "badBIOS," the Mysterious MAC and PC Malware that Jumps Airgaps." Last updated 31 October 2013, https://arstechnica.com/information-technology/2013/10/meet-badbios-the-mysterious-mac-and-pc-malware-that-jumps-airgaps/.

GPS.Gov. "GPS Accuracy." Last modified 5 December 2017. https://www.gps.gov/systems/gps/performance/accuracy/.

Hoffman, Chris. "Why Windows Had More Viruses than Mac and Linux." Last updated 21 September 2016. https://www.howtogeek.com/141944/htg-explains-why-windows-has-the-most-viruses/.

IGI Global. "What is GPS." Last accessed 20 April 2019. https://www.igi-global.com/dictionary/using-unmanned-aerial-vehicles-to-solve-some-civil-problems/12406.

International Chamber of Shipping. "Shipping and the World Trade." Last accessed 20 April 2019. http://www.ics-shipping.org/shipping-facts/shipping-and-world-trade.

International Maritime Organization. "AIS Transponders." Last accessed 20 April 2019, http://www.imo.org/en/OurWork/Safety/Navigation/Pages/AIS.aspx.

———. "E-Navigation." Last accessed 19 April 2019. http://www.imo.org/en/OurWork/Safety/Navigation/Pages/eNavigation.aspx.

McLeod, James. "Canada's Navy Is Developing an AI Voice Assistant for Warships, but Don't Worry: It Won't Control the Weapons." Last modified 1 May 2019. https://business.financialpost.com/technology/canadas-navy-is-developing-an-ai-voice-assistant-for-warships-but-dont-worry-it-wont-control-the-weapons.

National Geographic. “Navigation.” Last updated 21 January 2011. https://www.nationalgeographic.org/encyclopedia/navigation/.

National Oceanographic and Atmospheric Administration. “Space Weather and GPS.” Last accessed 24 April 2019. https://www.swpc.noaa.gov/impacts/space-weather-and-gps-systems.

Navy Recognition. “Navies Upgrade to OSI’s ECPINS Warship 6.2 Naval Navigation and Tactical Software.” Last modified 3 May 2017. https://www.navyrecognition.com/index.php/news/defence-news/2017/may-2017-navy-naval-forces-defense-industry-technology-maritime-security-global-news/5172-navies-upgrade-to-osi-s-ecpins-warship-6-2-naval-navigation-tactical-software.html.

Orolia. “Resilient Positioning, Navigation and Timing (RPNT).” Last accessed 21 April 2019. https://www.orolia.com/our-company/resilient-pnt.

OSI Maritime Systems, “About,” last accessed 20 April 2019, https://osimaritime.com/about/.

Richey, Michael W., W.E. May, Tom S. Logsdon, John L. Howard, S.S.D. Jones and Edward W. Anderson. “Navigation – Technology.” Last accessed 20 April 2019. https://www.britannica.com/technology/navigation-technology.

Saul, Jonathan. “Cyber Threats Prompt Return of Radio for Ship Navigation.” Last modified 7 August 2017. https://www.reuters.com/article/us-shipping-gps-cyber-idUSKBN1AN0HT.

Ship Technology, “ECDIS: Is the Industry Ignoring an Important Update?” last modified 7 March 2018, https://www.ship-technology.com/features/ecdis-is-the-industry-ignoring-an-important-update/.

Trend Micro. “Security Risks in a Technology Driven World.” Last modified 18 October 2017. https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/security-risks-in-a-technology-driven-world.

———. “Threats at Sea: A Security Evaluation of AIS.” Last modified 16 December 2014. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/a-security-evaluation-of-ais.

Wagstaff, Jeremy. “All at Sea: Global Shipping Fleet Exposed to Hacking Threat.” Last modified 23 April 2014. https://www.reuters.com/article/us-cybersecurity-shipping/all-at-sea-global-shipping-fleet-exposed-to-hacking-threat-idUSBREA3M20820140424.