THE JOURNAL OF NAVIGATION, Page 1 of 15.
doi:10.1017/S0373463318000164

Enhancing Navigator Competence by Demonstrating Maritime Cyber Security

Odd Sveinung Hareide[1,2], Øyvind Jøsok[3,4], Mass Soldal Lund[3], Runar Ostnes[5] and Kirsi Helkala[3]

[1](*Norwegian Defence University College, Royal Norwegian Naval Academy, Navigation Competence Center, Bergen, Norway*)
[2](*Norwegian University of Science and Technology, Joint Research Program in Nautical Operations, Norway*)
[3](*Norwegian Defence University College, Cyber Academy, Lillehammer, Norway*)
[4](*Child and Youth Participation and Competence Development Research Program, Inland Norway University of Applied Sciences, Lillehammer, Norway*)
[5](*Norwegian University of Science and Technology, Department of Ocean Operations and Civil Engineering, Aalesund, Norway*)
(E-mail: oddsveinung.hareide@sksk.mil.no)

As technology continues to develop, information and communication technology and operational technology on board ships are increasingly being networked, and more frequently connected to the Internet. The introduction of cyber systems changes the work environment with the aim of decreasing the workload for the navigator, but at the same time introduces more complexity and vulnerabilities that in turn may alter the competencies needed to perform safe and efficient navigation. Contemporary examples of how cyber-attacks can distort situational awareness and interfere with operations are needed to enhance the navigator's competence through increased system awareness. This paper demonstrates some of the possible attack vectors that a cyber-attack can present to a ship, as well as discussing the plausibility and consequences of such attacks. In this study we provide a practical example to better understand how one can demystify cyber threats in order to enhance the navigators' competence.

KEYWORDS

1. Maritime. 2. Cyber Security. 3. Human Factor. 4. Navigation.

Submitted: 27 October 2017. Accepted: 4 March 2018.

1. INTRODUCTION. *"For the first time in maritime history the positive correlation between capital spent and power is undermined, cyber-attacks are low cost alternatives to physical attacks which have the ability to cripple maritime operations."* (Fitton et al., 2015, p. 14). This statement summarises the current dilemma for the maritime domain, as it is beginning to experience the vulnerable side of reliance on Information and

Communications Technology (ICT). The craftsmanship of maritime operations has always been the ability to safely and efficiently navigate the oceans, traditionally performed more or less in isolation from the rest of the world (Fitton et al., 2015). With increased digitisation and advances in electronically aided navigation where systems are increasingly being networked and integrated, such as Electronic Chart Display and Information System (ECDIS), radar, Automatic Identification System (AIS) and the Autopilot (AP), the maritime domain is increasingly dependent on cyber systems for safe and efficient navigation. However, digitisation and convergence of ICT and Operations Technology (OT) (BIMCO et al., 2017), creates potential attack vectors for an adversary with intent, persistence and resources to interfere with maritime operations.

The current drive towards even more integration of sensors together with increased use of automation to enable, for example, remote monitored or remote-controlled operations, will potentially bolster the significance of such successful attacks in the near future. Overreliance in some parts of the integrated navigation system can result in dangerous situations (Norris, 2010; MAIB, 2014), and not being prepared for a cyber-incident against navigation systems might lead to significant consequences (Gard, 2016). Scholars and industry have jointly called for more cyber security testing of maritime cyber systems, in order to raise awareness and identify the need to conduct appropriate training and education for personnel operating such systems (Fitton et al., 2015; Dyryavyy, 2014). Simultaneously suggesting that to mitigate both the threat of, and potential negative effects of successful cyber-attacks requires investment in both technology and people (Fitton et al., 2015). Despite recent headlines in the media regarding the effects of cyber-attacks in the maritime domain (Baraniuk, 2017; Demchak et al., 2017), there seems to be a lack of relevant examples demonstrating attack vectors and effects of cyber incidents on maritime navigation systems. We argue that more examples of cyber-attack possibilities are needed to aid the conceptual development and understanding of Maritime Cyber Security (MCS).

This article will first explore the contemporary understanding of the emerging concept of MCS. We argue that the current awareness and understanding of cyber security in the maritime domain is insufficient. By using the concept of Situational Awareness (SA) as a measure of safe and efficient navigation, Sections 2 and 3 discuss how cyber systems make SA more complex for the modern navigator. Section 4 introduces a demonstration of MCS carried out for learning purposes at the Royal Norwegian Naval Academy. The main body of the experiment is demonstrating how a cyber-attack can be performed against a modern maritime navigation system. This section also includes the design of the study and data collection, both utilising the cyber kill chain model (Hutchins et al., 2011). Section 5 presents the findings from the experiment. Sections 6 and 7 discuss impacts and conclude the article.

2. MARITIME CYBER SECURITY.

2.1. *The emerging concept of MCS.* MCS is a combination of the two terms 'maritime security' and 'cyber security'. The first term; maritime security, has been argued to have no definite meaning, and subsequently relates to different concepts depending on the individuals attempting to make sense of it, or practice it (Bueger, 2015). Only relatively recently has the North Atlantic Treaty Organisation (NATO) included maritime security as an objective in its Alliance Maritime Strategy (NATO, 2011). Bueger (2015) further argues that: "*Maritime security can first be understood in a matrix of its relation to other concepts,* *such as marine safety, sea power, blue economy and resilience*." (Bueger, 2015, p. 1), where each of these concepts points to different dimensions of maritime security. However, these concepts described in the Maritime Security Matrix (Bueger, 2015) emphasise mostly the physical domain characteristics of maritime security. As the maritime domain is utilising advancements in ICT, new vulnerabilities are introduced as the cyber domain[1] is emerging in importance (MoD, 2013). Further, as assets in the maritime domain are becoming more integrated with increased sharing of information between ICT systems, maritime security relies also on a mature understanding of cyber security to operate and navigate safely and securely.

The second term; cyber security, has its origin in information security. Information security is mainly concerned with securing the integrity, confidentiality and availability of information (Whitman and Mattord, 2011), while cyber security is mainly concerned with the availability and integrity of the cyber systems (Von Solms and Van Niekerk, 2013). A consequence is that cyber security, in addition to protecting information transmitted or stored using ICT, also includes securing networks, Hardware (HW) and Software (SW) from unauthorised or malicious use. When ICT and OT are merging in the maritime domain, cyber security transcends into the operational domain of the navigator. Recent examples highlight that cyber-attacks have the potential to impact in the maritime domain by crossing the borders of cyber-physical interaction, resulting in loss of revenue (Maersk, 2017), or even have the power to provoke collisions by manipulating navigation information (Humphreys et al., 2008; Bhatti and Humphreys, 2014). While catastrophic events as a result of cyber-attacks such as explosions or fire are unlikely, errors introduced in a critical system such as the ECDIS are more likely. Such incidents have already been reported, with one of the latest examples known as the Black Sea incident (Goward, 2017).

To summarise, MCS can be understood as a part of maritime security concerned with the protection from cyber threats of all aspects of maritime cyber systems, particularly concerning integrity and availability. In addition, MCS is concerned with the reduction of the consequences of cyber-attacks on maritime operations. Thus, the means of MCS are not merely technological, but also consist of information and people.

2.2. *Understanding MCS.* According to Fitton et al. (2015), three elements of maritime cyber security should be taken into consideration to understand and mitigate cyber-attacks: Information, People and Technology.

These three elements are intertwined in forming the contemporary maritime cyber domain and are further outlined in Section 3. Technology is important in navigation and the conduct of all types of maritime operations, but also renders possible the exchange of information between agents in the maritime socio-technical system. In addition to the three elements of MCS, introduction of cyber systems in the maritime environment extends the reach of the maritime domain itself (Fitton et al., 2015). ICT creates connections between different locations in real time, with the result that the maritime domain is now, to a greater extent, converging with other domains like air, space and land. Hence, one important feature of the cyber domain is the ability to decouple location and presence (Floridi, 2017), creating the possibility of influencing both people and information in and through the cyber domain from distant locations. Therefore, when considering the concept of maritime

[1] Cyber domain means an electronic information (data) processing domain comprising of one or several information technology infrastructures (MoD, 2013).

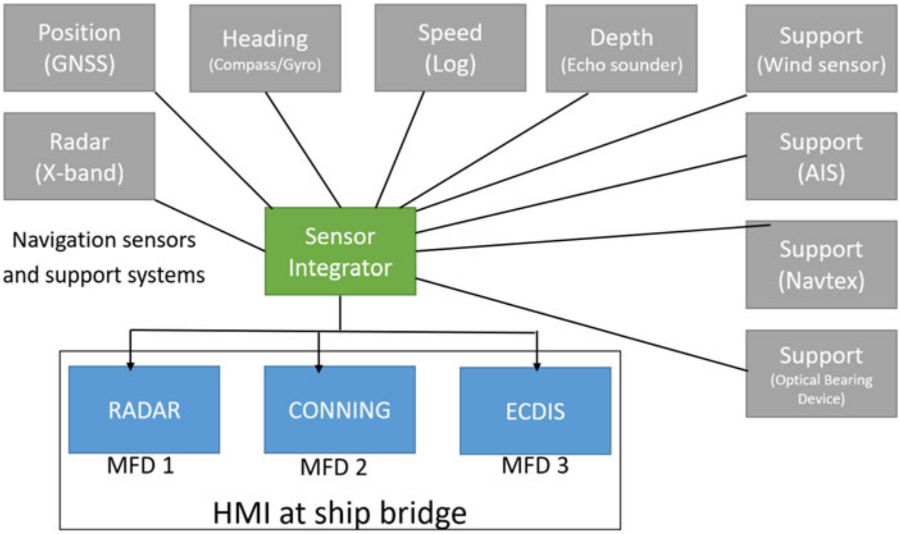

Figure 1. Example schematic of an integrated maritime navigation system.

security in the future, it will be vital to consider how the cyber domain is extending the maritime operating environment beyond a standard littoral boundary (Fitton et al., 2015).

By briefly exploring the features that cyber adds to the maritime domain, it is apparent that both the extended reach of the maritime domain and the mutual dependability between technology, people and information adds to the domain of interest for a navigator. This results in an extension of the SA requirements beyond the physically observable domain to conduct safe navigation.

3. SITUATIONAL AWARENESS FOR THE MODERN NAVIGATOR. With the modern ship bridge, the maritime navigator has gone through a paradigm shift concerning the number and use of displays and sensors when conducting a passage. Historically, the main task for the navigator was to find and fix the position of the vessel, while today's navigator monitors the vessel's presented position on the ECDIS.

3.1. *Technology.* The displays and sensors on board ships are connected using computer networks, known as Sensor Integrators (SINT). An example of how a maritime navigation system used by a navigator to conduct a passage could be integrated is shown in Figure 1.

The navigation system aims to provide information to increase the SA of the navigator in a timely manner. By providing an increased SA, the modern maritime navigation system enhances the safety of navigation by integrating information from sensors and provides augmented functions to avoid navigation accidents (Hareide and Ostnes, 2017a).

Navigation systems and sensors on board ships have been networked, and information increasingly integrated, for many years. The International Maritime Organization (IMO) has released a voluntary-fitted performance standard for Integrated Navigation Systems (INS), to set the minimum requirements for the equipment in use. IMO Resolution MSC.252(83) (IMO, 2007) describes the revised performance standards for INS, and the IMO recommends governments assure that an INS should be installed on ships built after

2011. There are several functions within the INS, and the aim is to utilise and combine these functions to provide “added value” for the operator to plan, monitor and control the safety of the ship during its passage (IMO, 2007).

The sensors and systems within an INS include, but are not limited by (IMO, 2007):

- The Electronic Position Fixing System (EPFS), providing the absolute position of the vessel (for example Global Positioning System (GPS)).
- Heading Control System (HCS), which enables the ship to keep a pre-set heading, known as an autopilot.
- Speed and Distance Measurement Equipment (SDME), providing the speed of the vessel (and thus distance).
- The ECDIS, used for chart presentation and presentation of relevant information for the navigator.
- Radar system, used as a mean for terrestrial positioning.
- AIS, automatic tracking system used on ships and by vessel traffic services (VTS).
- Echo Sounding System (ESS), providing the depth measurements for the vessel.
- Conning application providing information about the engine and manoeuvring status.
- Information distribution on Local Area Networks (LAN) and presentation of information on Multi-Function Displays (MFDs).
- Use of Communication channels such as Global Maritime Distress Safety System (GMDSS), which uses, for example, the NAVTEX receiver to receive navigational messages, or other communication channels for distributing data such as Satellite Communication (SATCOM) or mobile broadband.

The Maritime Cyber Security demonstrator presented in this paper shows an attack against an INS, but the attack would also be relevant against a networked and integrated maritime navigation system, even though not compliant with IMO Resolution MSC.252(83) (IMO, 2007).

3.2. *Information.* Concern has been raised about the modern navigators’ ability to conduct proper monitoring of the systems in front of them. As an example, the term “play-station mode” (Hareide et al., 2016) has been introduced to visualise the concern about the navigator focussing more on the displays than the surroundings of the ship.

The e-Navigation concept was introduced to enhance safety of navigation and efficiency of shipping (Hagen, 2017). e-Navigation is intended to promote safety, security and efficiency in global shipping, and a Strategic Implementation Plan (e-Nav SIP) has been introduced with a vision for e-Navigation (IMO, 2015). e-Navigation intends to meet users’ needs through harmonisation of on board navigation and information systems, communication and supporting shore services. It is also expected that the level of automation will increase, and the number of displays will be reduced with implementation of e-Navigation. An example is the SMART e-Navigation project for integrating chart and navigation information for coastal ships in Korea (Kim and Park, 2016).

Today, the navigators’ ability to determine and fix position is mainly conducted through EPFS, such as Global Navigation Satellite Systems (GNSS) and the most commonly used is GPS. GNSSs provide the absolute position of the vessel in more or less real time and have been a revolution for navigators. However, a navigator needs to be aware of several vulnerabilities such as signal interference and level of accuracy when using a GNSS. This has led some to argue that the craftsmanship of navigation has decayed, because of an over-reliance on GNSS (Glomsvoll and Bonenberg, 2017; Norris, 2010). The craftsmanship of navigation for the modern navigator and the traditional navigator still shares at least one important factor of safe and secure navigation. The safe and secure navigation of a vessel relies on a navigator with a high level of Situational Awareness (SA). The purpose of e-Navigation and the INS is to provide the navigator with enhanced SA through timely and accurate information. However, with technological vulnerabilities introduced, we argue that the SA requirements also change.

3.3. *People.* A high degree of SA supports the handling of unexpected incidents (Wickens, 2002). According to Endsley (1995), SA has three constituent parts; perception, comprehension and prediction. The ability to develop and maintain a high level of SA varies significantly between people and tasks (Endsley and Garland, 2000) and when the cyber domain has entered the playground, Endsley's model of SA has been criticised for being too physical-domain oriented, missing vital features that the cyber domain brings (Alcaraz and Lopez, 2013). In the same vein, cyber-oriented SA papers have been criticised for being concerned with aspects related to SA that in fact are only sub-components, that is, sensors, recognised cyber picture, strategic picture, physical operations, etc., leaving the overall SA unmentioned (Franke and Brynielsson, 2014). According to Franke and Brynielsson (2014) the technical and cognitive sides of SA are closely related and somewhat intertwined, meaning that cyber information needs to be combined with other information to make sense and to obtain full understanding of the situation.

Wickens (2002) argues that in the context of aviation, the three components of SA are spatial awareness, task awareness and system awareness. The importance of awareness of the system has been mentioned by Adams et al. (1995) in relation to a growing concern of complex systems taking the operator partly "out of the loop". The maritime domain has similarities with aviation, and several of the conditions and restraints are coincident (Hareide and Ostnes, 2017a). Spatial awareness consists of the environment to which the navigator must adhere, and incorporates all the variables that the navigator must address to conduct a safe and efficient passage. The maritime environment is dynamic, and variables will alter during the passage. A navigator must take into account the vessel's current task (mission), which consists of navigation, seamanship, communication with other internal and external agents to conduct the task and system management (for example fuel management). System awareness for a navigator consists of the ability to understand and be aware of the state of the systems on the bridge. In aviation, the pilot usually needs not to be aware of the system status, unless an unexpected situation arises (Wickens, 2002, p. 131). With the introduction of e-Navigation and cyber systems on board, a high degree of system awareness is increasingly important in order to maintain SA. Both the vessel and the maritime environment are complex and dynamic, as are the systems within the vessel. One of these systems is the INS (Figure 1), which a navigator operates continuously. The complexity of the system, often coupled with poor design, makes system awareness difficult to maintain (Sarter and Woods, 1995; Hareide and Ostnes, 2017b). When understanding the system, and in this specific context the INS, it is important to relate it to the integrity, confidentiality and availability of relevant and time-crucial information flowing on the network of the INS. Thus, MCS is related to a navigator's SA through system awareness, illustrated in Figure 2.

According to Endsley's theory, level three SA gives a person the ability to project future states and events (Endsley, 1995). In a cyber-security context this will be the ability to;

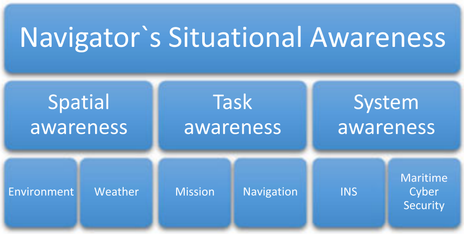

Figure 2. The relation between SA and system awareness. Note that the bottom line is meant as examples, and is not comprehensive as other examples could have been used.

"anticipate, detect and respond to unforeseen situations (failures or attacks) before they can cause disruptions" (Alcaraz and Lopez, 2013, p. 31). While this might seem too much to expect of a navigator, we think that simple efforts focussing on understanding and comprehension of the cyber threat could help mitigate large portions of contemporary cyber-attacks against an INS. With approximately 70% of breaches exploiting non-technical vulnerabilities (Deutscher et al., 2017), a navigator cannot afford to disengage in gaining cyber competence and leaving it to be the sole responsibility of the ICT department. Hence, there is currently a need to make the intangible cyber threat tangible, in order to add to the competence of the navigator instead of creating more confusion and uncertainty. *"Preventing, identifying and defending against cyber-attacks requires educating, training and drilling staff, so they can efficiently respond to attacks, spot errors and continue to operate under cyber-attack conditions"* (Fitton et al., 2015).

4. USING THE CYBER KILL CHAIN TO DEMONSTRATE A CYBER-ATTACK AGAINST AN INS. This project was conducted as a cooperation between state-actors and industry. In order to facilitate and conduct the MCS demonstrator, the composition of the working group was important, and a need for different types of Subject Matter Expert (SMEs) was identified. The working group in this project consists of one engineer from an ECDIS developer, two cyber specialists, one navigation specialist and three students. Two of the participants have served as sailors with the Norwegian Royal Navy. The project started in February 2017, data gathering was conducted in August 2017 and findings were analysed and discussed in the Autumn of 2017 with the project ending in late 2017. It may be possible to reduce the timeframe of a similar project by applying the initial findings from this paper.

4.1. *Data Collection.* An important resource is a vessel on which to conduct the cyber-attack. The vessel presented in this paper is equipped with Commercial Of The Shelf (COTS) computers with the Windows 7 operating system, and a commercially available INS delivered by a contractor as the target system. Data was collected in a real-time environment on board a ship fitted with an INS as shown in Figure 1. Figure 1 outlines the complexity and shows how several sensors are interconnected through a Sensor Integrator (SINT). The navigation data is provided to the INS via a redundant LAN, providing all the MFDs with the information from the sensors interconnected through the SINT.

The passage was carried out during three days in late August, in Norwegian littoral waters in the vicinity of Bergen. The data collection was done around Bergen which had 87,156 port calls in 2015 according to Port of Bergen (POB) (POB, 2015).

The area is characterised by confined waters that are challenging for navigation, due to a high number of islands, skerries and underwater rocks. For the purpose of the experiment the procedure was documented by means of video recording and pictures. This documentation will not be presented in this article in order to anonymise the vessel and the manufacturers.

The first step was to gather the participants for an initial workshop where the overall concept for the study was discussed. In order to make swift progress the workgroup decided to separate the technical and operational part of the project, leaving one part working on how to spoof the ship's position presented in the INS from a technical point of view, and the other part working on the plausibility of gaining access and discussing operational consequences.

The exploration of the competencies needed to navigate in the twenty-first century, with regard to implications caused by the cyber threat, can be performed by thinking as if you are the potential attacker. This can be achieved by using the Cyber Kill Chain from Lockheed Martin (Hutchins et al., 2011) as the conceptual framework which consists of seven phases:

1. *Reconnaissance* such as harvesting email addresses, conference information, etc.
2. *Weaponisation* such as exploiting a backdoor in a system to achieve a deliverable payload.
3. *Delivering* a weaponised bundle to the victim via email, web, Universal Serial Bus (USB), etc.
4. *Exploiting* a vulnerability to execute code on a victim's system.
5. *Installing* malware on the asset.
6. *Command and Control* channel for remote manipulation of victim.
7. *Actions on objectives* conducted with "hand on keyboard" access, intruders accomplish their original goals.

4.2. *Reconnaissance.* The first part of the Cyber Kill Chain is reconnaissance. This was conducted in a workshop where the participants brainstormed potential attack vectors of the system. The participants in the workshop had in-depth knowledge of the technical and operational aspects of the system, navigational practice and routines regarding updates of HW and SW on board the specific vessel. In this initial phase we decided that spoofing the position provided by the EPFS by a small amount would be one plausible goal of an adversary with intent and capacity. The effect could be bolstered by triggering the offset at a predefined point or by means of a remote command utilising the INS's merging of auxiliary systems such as AIS or NAVTEX (Figure 1). By drawing off knowledge about the updating routines and SME's system knowledge, an array of different cyber-attack vectors was identified. These vectors can be roughly be divided into two: firstly, if one has direct access to the system and secondly, if one can gain indirect access to the system. For the purpose of this project we decided to analyse what could be possible if we had direct access to the system and discuss the plausibility of gaining indirect access. The discussion was conducted by analysing the routines performed by developers, technicians and operators with access to the on board computers used in the INS (known as Operator Stations – OS). From an operational perspective, both an indirect access and direct access are plausible vectors of attack. The identified attack vectors are illustrated in Figure 3.

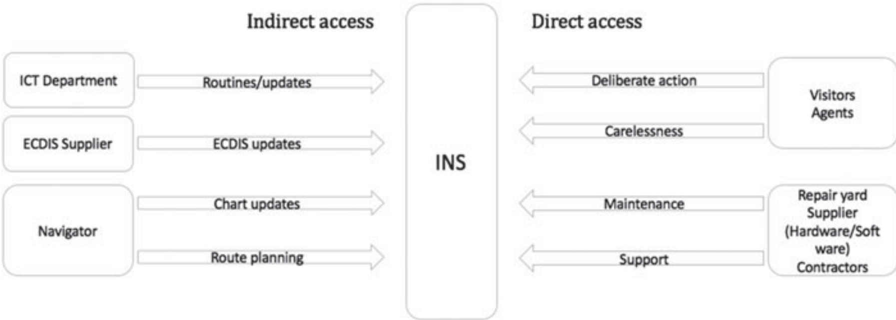

Figure 3. Potential attack vectors towards the INS.

The attack vectors are in general the same for all vessels, but there will be some differences when it comes to the age and maintenance routines of different types of vessels. Figure 3 provides an example of how one could map the different possible threat vectors within the MCS domain for a vessel. These attack vectors assume the INS does not have any outbound connections. However, reports (Dyryavyy, 2014; Baranuik, 2017) indicate that connecting the INS to the internet is becoming increasingly common, providing even more attack vectors.

4.3. *Weaponisation.* The weaponisation phase was performed by the cyber specialist by utilising open source information on how to develop the attack (Lund et al., 2018, in review). The cyber specialist used a laptop with the current windows version and the ECDIS application installed in order to test the attack during development. The rest of the participants engaged in conceptualising the notion of maritime cyber security and conducting focus groups with navigators to disclose cyber security awareness and current routines, and understanding of routines to mitigate cyber threats.

4.4. *Delivery, exploitation and installation.* Ways of gaining access to the system were identified in the initial workshop and the potential access points are shown in Figure 3. Once the attack was properly developed it was delivered through a USB port using a specially built USB device. First the USB device acted as a mouse and keyboard to log out of ECDIS and enter the operating system. The malware was installed on the Windows operating system and the computer was restarted. Once installed, the malware acted as "a man in the middle" between the sensory data input and the ECDIS application. The duration of this procedure was 5 minutes and 17 seconds, however improving the delivery could reduce the time needed to infect the system (Lund et al., 2018, in review). The end state is an ECDIS that seemingly has no faults and works as normal. Using the VirusTotal site (www.virustotal.com), the malware was tested against 60 of the most common anti-virus programs available for purchase. Only two of these detected any suspicious code in the malware, while the remaining 58 categorised the malware as "clean". An anti-virus program installed would therefore not be sufficient protection against a tailored cyber-attack like this.

4.5. *Command & control and action on objectives.* The INS is usually considered as an offline system. Therefore, command and control communication between malware and attacker through an Internet connection is not possible. In order to solve this problem, the malware was programmed to trigger at a specific position, so that when the ship crosses this predefined line, the malware starts to inject faulty values. In this case, the result is the ECDIS showing an increasingly faulty position.

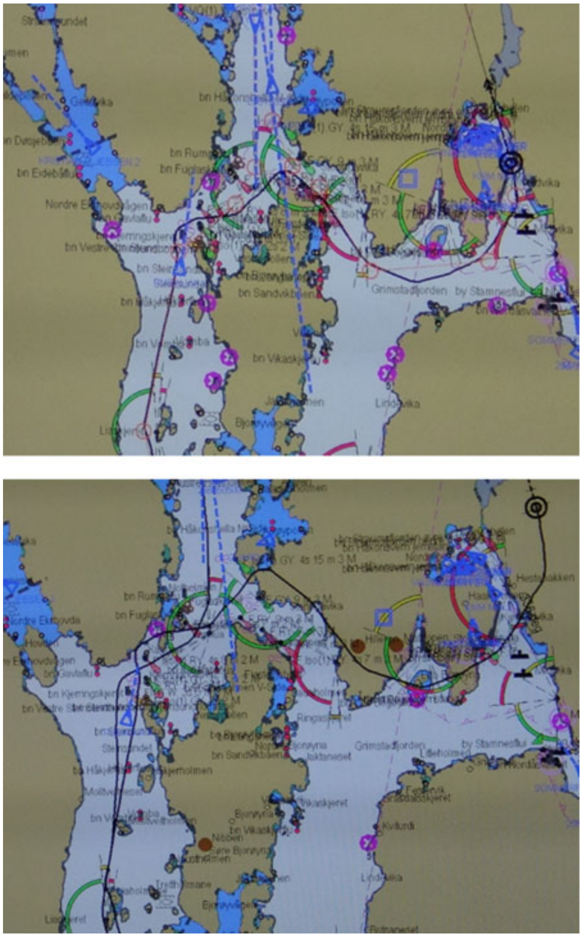

Figure 4. Upper print screen picture shows the ships actual track, lower screen picture shows the infected operator stations ship track.

5. FINDINGS. The malware was successfully installed on the computer by putting the USB device into an open and available USB slot. The full technical procedure is explained in Lund et al. (2018, in review). The malware was installed on the computer running the ECDIS SW, and successfully manipulated the GPS input causing the ECDIS to present a faulty position during the passage.

The malware was triggered when the ship crossed a predefined and pre-programmed position in latitude (lat) and longitude (long). The displayed position during this experiment was offset with at a rate of 0·0004 minutes (approximately 0·8 metres) per second towards the northeast (045°). This can be viewed in Figure 4, which shows the ECDIS, where the lower picture is spoofed, and the real position can be viewed in the upper picture.

A shutdown of the navigation computer was performed by triggering the malware at a second predefined position (lat/long), leaving the navigator unable to restore the proper ECDIS function during the passage. When restarting the computer, the malware hampered the SW's ability to operate, implied by a "blue screen".

The attack was also conducted when the vessel operated in "track mode", which means that the autopilot is following the pre-planned route. When the position was spoofed, the autopilot corrected the spoofing by turning the vessel, thus taking the vessel away from the actual pre-planned route, which would eventually result in a "controlled" grounding of the vessel.

6. DISCUSSION. The introduction of ICT in the maritime domain expands the notion of maritime security by introducing cyber domain challenges. Therefore, it is fair to say that MCS has to be included as a part of maritime security measures. However, the cyber domain is crossing cyber-physical borders and hence cannot be treated as a technological issue alone. The implication of this insight is that maritime cyber security has to be considered as something more than an ICT department issue; it also includes people and information. As proven in our demonstration, the most crucial phase of a cyber-attack is the reconnaissance phase where an attacker utilises whatever means are available to gain critical information about the target system. This can include information available online, information gained through social engineering or even by gaining physical access to the target system. Hence, being off-line does not exclude the possibility of being exposed to targeted attacks. From a MCS perspective this means that if one can deny a threat actor information in the reconnaissance phase, this will reduce the risk of eventually experiencing an attack. However, this seems to be reliant on a combination of measures including enhancing competence of personnel operating the systems; in this case the navigator.

Introducing the cyber domain in the maritime context changes something; it adds something. It adds complexity and dependency on technology (for example, the removal of paper charts), and the operator's competence requirement is changing from traditional navigation with analogue tools to also requiring digital competence and system awareness. This leads us to evaluate if introducing INS and e-Navigation also changes the competence requirements for the navigator. The demands for spatial and task awareness may be similar, while demands for system awareness change. This can be exemplified by comparing the "use of ECDIS" and the "understanding of ECDIS". Today one could argue that the first is the focus, to use and harnessing of the advantages of the INS. However, from a competence perspective; to use and to understand the system is two different approaches to education and training. The need for a high degree of situational awareness is essential to be able to make good informed navigation decisions. When introducing INS and enabling the cyber domain we add the need to be situationally aware of the status of the system and the limitations and possibilities it presents. If one lacks system awareness, one would lack a vital part of the overall situational awareness and potentially present a risk factor rather than a risk reduction factor. So, in order to utilise the human capacity to be the strongest link in the MCS chain, MCS has to become a part of education and training in order to enhance the navigator's competence by increasing system awareness. Using the cyber kill chain to conceptualise and demonstrate MSC can be a cost efficient and beneficial way to expose navigators to the threat and thus offer an easy solution to a growing challenge.

Our experiment demonstrates that cyber-attacks against an INS are relatively easily achievable. The security of the INS relies heavily on physical protection, while the INS itself is quite open once access has been established. Initially, the reconnaissance phase is the most resource-consuming for a potential attacker. This is where the attacker has to gain knowledge about the system and the routines of the crew in order to obtain information such as passwords for login to higher maintenance levels, etc. However, ECDIS systems are available for purchase on the open market and technical documentation is relatively easily available, and sometimes even passwords can be available online (US-CERT, 2013). The discussion of whether this is possible is more a discussion about the attacker's intent, motivation, resources and persistence, than a discussion about whether this information is obtainable or not. Once the required technical documentation is obtained, an attacker would benefit from the ability to test the malware before installation. In this project our cyber specialist used less than two months' worth of man hours to achieve familiarisation with the system and to develop the attack. Even if the cyber specialist was given the ECDIS SW and had technical support from the supplier, this would also be within reach for a state actor or a large criminal organisation. The discussion then becomes if this would be plausible if the cyber specialist did not have the above-mentioned resources. It is quite clear that a teenager in his bedroom or a computer specialist in isolation would not have been able to perform such an attack.

Once the initial two phases are completed, the next critical phase is getting the malware installed. An ECDIS requires updates to sustain integrity over time, and in addition the ECDIS SW we used runs on a Microsoft Windows-based operating system that also requires regular updates and patching. The updating of charts and routes sometimes requires weekly or even daily updating and interaction between other computers through USB drives. Most vessels use ECDIS as an offline system, and all updates are done by USB sticks. This results in a lot of interaction between the INS and auxiliary systems. Taking into account that the systems seldom have anti-virus and protective measures (Baraniuk, 2017), this leaves the operation of getting into the system with malware less demanding for an attacker. If direct access cannot be gained, an unknowing navigator or maintenance technician could potentially be used as the messenger, (see Figure 3). Once installed, the malware can trigger at a predefined position and therefore requires no more interaction with the attacker. The threat remains dormant until the activation criteria have been met.

The end state of this attack is to create uncertainty for the navigator when the position in the INS/ECDIS, and the observed position is not correlating. This may in turn reduce the navigators trust in the ECDIS and heighten workload if the position deviation is noticed (Hareide, 2013). This will reduce the quality of the navigator's SA, and it could contribute to a dangerous and undesirable event in relation to the navigation of the vessel. In a worst-case scenario the position deviation could be tailored to the ship and the waters in such a way that the deviation is difficult to detect and fast enough to run the ship aground.

For the navigator to better understand MCS, the conduct of the process as described in the cyber kill chain will establish a better system awareness, which in turn increases SA for the navigator and can contribute to the navigators' resilience in case of a cyber-attack. This will have implications for education and training of navigators, and we argue that an increased focus on system knowledge and understanding is needed with the changing working environment as more technology for the navigator is introduced. With an increased system awareness, the navigator will understand the importance of integrity monitoring and system awareness in the conduct of a passage.

7. CONCLUSION.

This study explains and gives a working definition of Maritime Cyber Security and identifies the relationships between MCS and safe and efficient navigation through system awareness as a part of the navigator's overall SA. The importance of high system awareness for a navigator operating the INS is laid down, as a contribution to increase the SA of the navigator. Further, the MCS demonstrator is explained and put into context.

Our demonstrator utilises the cyber kill chain to address the need to close the gap between the emerging threat of cyber-attacks and the competence needed at operator level. By utilising the cyber kill chain, the awareness of the emerging cyber threat to the maritime environment can be identified. When the threat is identified, measures can be taken to mitigate these threats. The demonstrator is a relevant example of how an actor with resources and motivation can spoof an INS.

By understanding the possibilities and limitations within the system in use, in this case an INS, an increased system awareness is developed and thus an increased SA and ultimately a safer and more efficient passage.

8. FURTHER WORK. The Original Equipment Manufacturer (OEM) of the equipment used in this study will patch the current SW by implementing our current findings in the existing SW, and the crew of the vessel will provide physical adjustments to on board equipment (for example lock-down procedures and use of anti-tampering tape) to prevent access to the system by outsiders (attackers). The findings from this study will be implemented in the current curriculum for maritime navigators at the Royal Norwegian Naval Academy to improve system knowledge and thus contribute to a higher level of SA. In future development of the demonstrated cyber-attack, we will investigate other vectors of delivery, as well as using the Automatic Identification System to exercise remote command and control of the malware.

ACKNOWLEDGMENTS

A special thanks to the Royal Norwegian Naval Academy and the Norwegian Defence University College, Cyber Academy, for support in conducting the work. We would also like to thank the crew of the vessel for facilitating the demonstrator and the OEM for contributing with system engineers.

FINANCIAL SUPPORT

The work was sponsored by the Norwegian Armed Forces CD&E grant EP1710 Concepts for CND in joint operation and the Royal Norwegian Naval Academy R&D grant.

ETHICAL STANDARDS

The authors assert that all procedures contributing to this work comply with the ethical standards of the relevant national and institutional committees on human experimentation and with the Helsinki Declaration of 1975, as revised in 2008. All details of the cyber-attack have been disclosed to the manufacturer of the INS.

REFERENCES

Adams, M.J., Tenney, Y.J. and Pew, R.W. (1995). Situation Awareness and the Cognitive Management of Complex Systems. *Human Factors*, **37**, 85–104.

Alcaraz, C. and Lopez, J. (2013). Wide-area situational awareness for critical infrastructure protection. *Computer*, **46**, 30–37.

Baraniuk, C. (2017). *How hackers are targeting the shipping industry*. Available: http://www.bbc.com/news/technology-40685821 [Accessed 22.08.2017].
Bhatti, J. and Humphreys, T.E. (2014). *Covert control of surface vessels via counterfeit civil GPS signals*. University of Texas, unpublished.
BIMCO, CLIA, ICS, Intercargo, Intertanko, OCIMF and IUMI. (2017). *Guidelines on Cyber Security onboard Ships*. *In:* BIMCO (ed.) Version 2.0 ed. Bagsvaerd.
Bueger, C. (2015). What is maritime security? *Marine Policy*, **53**, 159–164.
Demchak, C., Patton, K. and Tangredi, S.J. (2017). *Why Are Our Ships Crashing? Competence, Overload, and Cyber Considerations*. Available: http://cimsec.org/ships-crashing-competence-overload-cyber-considerations/33865 [Accessed 12.09.2017].
Deutscher, S., Bohmayr, W. and Asen, A. (2017). *Building a Cyber resilient Organization.* Available: https://www.bcgperspectives.com/content/articles/technology-digital-building-a-cyberresilient-organization/.
Dyryavyy, Y. (2014). Preparing for Cyber Battleships - Electronic Chart Display and Information System Security. NCC Group.
Endsley, M.R. (1995). Toward a theory of situation awareness in dynamic systems. *Human factors*, **37**, 32–64.
Endsley, M.R. and Garland, D.J. (2000). *Situation awareness analysis and measurement.* CRC Press.
Fitton, O., Prince, D., Germond, B. and Lacy, M. (2015). *The future of maritime cyber security*. Lancaster University.
Floridi, L. (2017). Digital's Cleaving Power and Its Consequences. *Philosophy & Technology*, Vol 30, 1–7.
Franke, U. and Brynielsson, J. (2014). Cyber situational awareness–a systematic review of the literature. *Computers & Security*, **46**, 18–31.
Gard. (2016). Cyber Security – managing the threat. Available: http://www.gard.no/Content/21112216/Cyber Security [Accessed September 2016].
Glomsvoll, O. and Bonenberg, L.K. (2017). GNSS jamming resilience for close to shore navigation in the Northern Sea. *The Journal of Navigation*, **70**, 33–48.
Goward, D. (2017). *Mass GPS Spoofing Attack in Black Sea?* Available: http://maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea [Accessed 10.08.17].
Hagen, J.E. (2017). *Implementing e-Navigation*, Norwood, Artech House.
Hareide, O.S. (2013). *Control of ECDIS (electronic charts and display information system) on high speed crafts in littoral waters.* MSc, University of Nottingham.
Hareide, O.S. and Ostnes, R. (2017b). Maritime usability study by analysing Eye Tracking data. *Journal of Navigation*, **70**(5), 927–943.
Hareide, O.S. and Ostnes, R. (2017a). Scan Pattern for the Maritime Navigator. *TransNav 2017*, 10.
Hareide, O.S., Ostnes, R. and Mjelde, F.V. (2016). Understanding the Eye of the Navigator. *In:* NAVIGATION, N. I. O., ed. *European Navigation Conference, 2016 Helsinki. Confedent International*.
Humphreys, T.E., Ledvina, B.M., Psiaki, M.L., O'Hanlon, B.W. and Kintner Jr, P.M. (2008). Assessing the spoofing threat: Development of a portable GPS civilian spoofer. *Proceedings of the ION GNSS international technical meeting of the satellite division*, 56.
Hutchins, E.M., Cloppert, M.J. and Amin, R.M. (2011). Intelligence-driven computer network defence informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research,* **1**, 80.
IMO. (2007). Resolution MSC.252(83): Adoption of the Revised Performance Standard for Integrated Navigation Systems. London. Available: http://www.imo.org/en/KnowledgeCentre/IndexofIMOResolutions/Maritime-Safety-Committee-(MSC)/Documents/MSC.252(83).pdf
IMO. (2015). Draft e-Navigation Strategy Implementation Plan (SIP). *In:* 1/28, N. (ed.). Available: http://www.imo.org/en/ourwork/safety/navigation/documents/enavigation/sip.pdf
Kim, J. and Park, Y.-Y. (2016). An Integrated Approach to Korea's e-Navigation Communication Infrastructure. *International Information Institute (Tokyo). Information*, **19**, 643.
Lockheed Martin (LM). (2015). *Gaining the advantage*. Available: http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/Gaining_the_Advantage_Cyber_Kill_Chain.pdf [Accessed 05.06.2017].
Lund, M.S., Hareide, O.S., Jøsok, Ø. & Skare, K.E. (2018). An attack on an integrated navigation system. USENIX Security Symposium, submitted, 2018.
Maersk. (2017). *Press release Interim Report Q2* 2017. Copenhagen. Available: http://investor.maersk.com/releasedetail.cfm?releaseid=1037421.

Marine Accident Investigation Branch (MAIB). (2014). *Report on the investigation of the grounding of Ovit in the Dover Strait*. Southampton. Available: https://assets.publishing.service.gov.uk/media/547c6f2640f0b60244000007/OvitReport.pdf

MoD, Finland. (2013). Finland's Cyber security Strategy. *In:* COMMITTEE, S. O. T. S. (ed.). Helsinki: MoD.

NATO. (2011). Alliance Maritime Strategy. Available: http://www.nato.int/cps/en/natohq/official_texts_75615.htm

Norris, A. 2010. *Integrated Bridge Systems vol 2 ECDIS and Positioning,* London, Nautical Institute.

Port of Bergen (POB). (2015). Annual Report. Available: https://bergenhavn.no/om-bergen-havn/arsrapporter/.

Sarter, N.B. and Woods, D.D. (1995). How in the World Did We Ever Get into That Mode? Mode Error and Awareness in Supervisory Control. *Human Factors*, **37**, 5–19.

US-Cert. (2013). Risks of Default Passwords on the Internet. *In:* SECURITY, D. O. H. (ed.). Available: https://www.us-cert.gov/ncas/alerts/TA13-175A.

Von Solms, R. and Van Niekerk, J. (2013). From information security to cyber security. C*omputers & Security*, **38**, 97–102.

Whitman, M.E. and Mattord, H.J. (2011). *Principles of information security*, Cengage Learning.

Wickens, C.D. (2002). Situation awareness and workload in aviation. *Current Directions in Psychological Science*, **11**, 128–133.