Detecting and Hunting Cyberthreats in a Maritime Environment: Specification and Experimentation of a Maritime Cybersecurity Operations Centre

Olivier Jacq, Xavier Boudvin, David Brosset, Yvon Kermarrec, Jacques Simonin

Detecting and Hunting Cyberthreats in a Maritime Environment: Specification and Experimentation of a Maritime Cybersecurity Operations Centre

Olivier Jacq*, Xavier Boudvin*, David Brosset*, Yvon Kermarrec*†, Jacques Simonin*†
* Chair of Naval Cyber Defense -
Ecole Navale - 29460 Lanvéoc, France
firstname.lastname@ecole-navale.fr
† Lab-STICC - IMT Atlantique - 29238 Brest, France
firstname.lastname@imt-atlantique.fr

***Abstract*—The vast majority of worldwide goods exchanges are made by sea. In some parts of the world, the concurrence for dominance at sea is very high and definitely seen as a main military goal. Meanwhile, new generation ships highly rely on information systems for communication, navigation and platform management. This ever-spreading attack surface and permanent satellite links have grown a concern about the potential impact of cyberattacks on a ship at sea or on naval shore infrastructures. Therefore, on top of the usual cyberprotection measures taken for safety reasons, it is essential to implement an ongoing cyber monitoring of ships in order to detect, react accordingly, and stop any incoming threat.**

In this paper, we explain the specific constraints when trying to assess the cyber situation awareness of maritime information systems. As we will demonstrate, those systems combine physical and logical constraints which complexify their cyber monitoring process and architecture. Gathering valuable data while having a limited and controlled impact on the satellite bandwidth, maintaining a high level of integrity on remote systems in production are, for instance, thriving challenges for both civilian and military ships. We have designed and set up a research platform which fulfils those specifications to streamline the cyber monitoring process. We will then describe the architecture used to detect cyber-threats and collect potential Indices of Compromise from naval systems, as well as the results we have currently achieved.

***Keywords*—ICS - SOC - maritime - cyber situation awareness.**

I. Introduction

COVERING 71 percent of the Earth's surface, oceans have historically been a centre of interest for trade, oil and gas industry as well as passenger traffic. Transferring large amount of goods from one part of the world to another is often cheaper by sea than by any other means. Ensuring a free access to the sea as well as maintaining secured sea lanes are often top priorities for industrial countries which have developed naval military capacities to achieve these objectives.

90 percent of global world trade is operated by the shipping industry[1]. For most of us, the importance of the sea in our daily life cannot be seen. It is even often forgotten. However, an enormous part of the goods we buy and consume has had a link with the sea during its industrial life cycle. Throughout history, the use of the sea for goods exchange has developed and became a priority for local, regional and worldwide trading, growing together with ships capacities and navigation reliability. Ships provide a cost-efficient delivery of goods for most industries as well as for agriculture or human needs. The remarkable progress of the naval industry has given the capacity to build larger and faster ships. Today, the largest container ships, which are 400-metre long, can carry over 21,000 Twenty-foot Equivalent Units (TEU)[2] while being operated by a crew of 20 people only.

The development of civil aviation from 1960s has signed the quick decline of ocean liners for passengers intercontinental travels. However, commuting via ferry boat is still a daily reality for workers and tourists in many parts of the world, on short distances or when competing with aircraft makes no sense economically. The tremendous interest for cruising over the last twenty years has greatly increased the commercial offers - and the size of cruise vessels. Those built nowadays are the largest ever, welcoming nearly 9,000 people on board including passengers and crew[3].

Ever since the start of trading over the ocean, piracy has been an immediate concern. Competition for importing goods, discovery of new sea lanes, protection of national territories and fish resources, safe sailing on sea lanes and straights such as Panama, Suez, Hormuz, Bab el-Mandab or Malacca are of highest concerns for most countries. The will to protect national interests and establish naval leadership has led to the development of navies. Developed and developing economies are today upgrading their naval capacities with last generation surface ships and submarines to respond to modern threats at sea and secure their vital imports of goods. With the ability to operate in most parts of the oceans, a powerful navy multiplies the possibilities to deter, anticipate, protect and take a decisive role in modern conflicts.

The ability to build and operate the so-called 'megaships' for industry or cruising highly relies on their digitalization. The effectiveness and power of our navies depend on accurate and secure information systems. The use of industrial control systems and information systems to drive naval engines, ship-to-shore communications or weapons systems has never been higher, simplifying their operation and leveraging their capacities[4]. Those ships, as well as naval shore infrastruc-

tures, are no more built as they used to be just a decade ago. Things have radically changed, forever. The shift from analogical to digital has been drastic, spreading sensors, computers, networks as a replacement for buttons, meters and analog displays. Even on small fishing or sailing vessels, digital devices such as sounders, radars, Global Positioning System (GPS), Electronic Charts Display and Information System (ECDIS), satellite systems and radios are now interconnected.

While this has dramatically improved ships and shore infrastructures performance and safety, the attack surface has similarly grown over the last few years, drawing new weaknesses and threats to the maritime sector. This growth will become even higher over the next decades, as digitalization will completely transform the way ships, ports and offshore infrastructures will operate[5]. Reflections and projects are also on their way to build fully autonomous and unmanned ships, drawing a new era of maritime evolution. Setting a high priority on cybersecurity is therefore paramount to ensure maximum integrity and resilience of the underlying information systems[6][7].

In this paper, we present an architecture we have designed and built to generate the real time cyber situational awareness for naval systems and the initial results and outcomes we have obtained. In the first section, we present the rationale and the specific characteristics of naval systems. In the second section, we describe the solutions which are currently available through the usual triad: People, Process, Technologies. In the third section, we describe the design constraints and demonstrate that the existing recommendations and architectures do not fully meet the requirements in terms of naval systems. In the fourth section, we highlight all parts of the architecture we have designed to fully meet our objectives. The fifth section describes the results we have currently achieved. In the final section, we conclude with a survey of our current activities and the future plans we have as perspectives to enhance our current implemented platform.

II. Cyber-threats to the maritime sector and characteristics of maritime information systems

Naval systems can be of high interest for both state actors, non-state actors, and cyber-criminals. The high level of onboard digitalization has greatly improved operations but, in the meantime, has dramatically increased the number of vulnerabilities and threat vectors[8].

Large civilian ships and navy vessels usually share a overall common architecture for their digital onboard architecture. All modern ships are linked to the shore via satellite links, providing Internet and phone connexions onboard. The bridge uses computers for ECDIS, navigation and collision avoidance, closed circuit television (CCTV). The bridge also controls and manages Platform Management Systems (PMS), for instance to drive the ship's engine and rudder. If naval IT systems share vulnerabilities and threats with usual Information Technologies (IT) and Operational Technologies (OT) systems, the addition of this common background with the specificities of the maritime world makes it a specific domain to secure. We have found out that the naval sector combines the following unique specifications:

- Industrial Control Systems (ICS) with Programmable Logical Controllers (PLCs), ECDIS, communication systems, collision avoidance, navigation and platform management, entertainment, traditional IT and, for the navies, combat systems are networks which can be found on board. If most systems use proprietary protocols and software, convergence is also growing and those installations are increasingly using Commercial Off The Shelf (COTS) protocols, software and equipment and tend to be interconnected, sometimes using wireless protocols. Securing such networks is a tedious task and security equipments are usually non existent;
- high constraints are set on the satellite link: the bandwidth is costly and often limited to a specific value, ranging from tens of kbit/s for a small vessel to Mb/s for a large or military vessel[9]. Ships can also be isolated from shore, on a short or medium period, due to poor satellite coverage, antenna masks or failures: remote control and administration to mitigate a security issue is therefore complicated;
- the ship has to remain highly resilient even in case of failure of one of her IT systems: human lives, safety at sea, environmental issues are concerned: patching systems in a timely way is usually not possible;
- while autonomy at sea is paramount, if an ashore expertise support is needed, it can only be organized during a port of call, by phone or via a network access;
- no or very few cyber or IT-aware crew members are present aboard on a continuous shift: on the cyber part as well as on the embarked IT/OT systems expertise, the knowledge is usually low to non-existent;
- the maritime company supervises its ships as a whole fleet. This also means an interconnection between ships at sea or ashore: if no isolation is set, this can be an easy vector for a viral spreading;
- the deployment of security patches on those systems when at sea is complex. The various companies involved in developing and integrating embarked systems as well as the lack of pre-production platforms complicate security updates integration: evolutions made on the IT/OT systems traditionally have to go through a full certification process prior to any deployment;
- limited space and physical constraints on board ships spread the use of embedded systems and wireless networks, creating new attacks vectors while the integration of cyber-security assets remains a complicated task;
- finally, when ashore, ships highly rely on shore infrastructures, for instance to disembark their merchandise or for power and cooling supply: the IT and OT managing those infrastructures should not be forgotten in the cybersecurity process.

Most guides and articles cited in this article share the overall concern of the low cyber-security awareness of the maritime sector. They also confirm that maritime information and communication technologies are complex, due to the variety and criticality of most information systems used, combining vulnerabilities of IT and OT systems. Target systems,

whether ashore or aboard, may be of high interest for attackers; impacts could be massive, leading to material or ship loss, pollution, casualties, death. The fact that attackers profiles on the maritime sector could go from a wide prism from cyber-crime to non-state or state attackers is also of high concern. Finally, cyber-attacks targeting the maritime sector[10][11] or causing collateral damage to the maritime sector[12], have already been being reported publicly.

The unique characteristics we exposed, combined with the specific threat vectors lead us to think that the most feared cyber-scenario is probably a network intrusion, enabling a remote takeover of the ship for sabotage or piracy, leading to high damages to the crew, shipping or the environment[13][14]. The ongoing developments on autonomous ships and drones underline the likelihood of this scenario. We can also add to the list the spreading of ransomware ashore and aboard IT/OT naval systems, due to phishing, spear-phishing or viral infection during maintenance operations or via the use of personal devices. Using various Denial of Service (DoS) attacks, the disruption of essential services, such as satellite localisation or telecommunication and collision avoidance systems, Automatic Identification System (AIS)[15], mapping technologies (ECDIS) or bridge and conning is also a main feared issue[16][17]. Onboard cargo management systems[18] and shore infrastructures are also at risk: their digitalization over the last years has been very important and major ports are now using PLCs and interconnecting their information systems to get closer to the *smart port* design and to smooth the complex processes of logistics[19]. Due to the amount of valuable merchandise in transit, container terminals (CT) are especially of interest for attackers[20]. Finally, in some cases, and especially in the navy sector, sabotage and espionage techniques could have critical consequences for naval operations.

Cyber-security of those naval systems to cope with multiple and advanced threat vectors presents challenges of all types.

III. Solutions to maritime cyber-threats

As we know, a proper integration of cyber-risks highly relies on human cyber awareness and efficient cyber-regulation driven processes. So we have investigated the usual triad of People, Process, Technologies (PPT) to find specific issues and solutions for the maritime sector.

A. People for maritime cyber-security

Largest container megaships, such as Maersk's E-Class 400-meter long vessels, operate with only 22 people aboard[21]. IT operations are mostly automated and often assigned to one of the deck officers, usually the Electro Technical Officer (ETO), who has a basic operating and maintenance level on different systems, but is no cyber or IT expert[22]. Some naval training centres now offer continuous education programs on cyber-security (for instance the French Ecole nationale supérieure maritime, ENSM) and shipping companies and crews are increasingly aware of cyber-security risks and trained on crisis management. But at sea, they would probably be unable to detect and react accordingly during an advanced cyber-attack, and also unable to recover the harmed system. Depending on the quality and experience of the company and crew, the level of cyber awareness can also be very different, due to cultural, educational or management and communication issues. To cope with this issue, the International Maritime Organisation (IMO) recently asked maritime companies to integrate cyber risks management within safety management by January 1st, 2021[23].

On military ships, the analysis which can be made from official documents is somehow different. Due to the possible impact on vessels or shore infrastructures, espionage possibilities or other risks, States and Ministries of Defence of most countries have been strengthening their defence systems over the last years. While it is hard to gather public figures on the subject, depending on the type, complexity and mission of the navy ship and its digitalization level, IT people aboard may represent between 2 and 10 percent of the whole crew. Most of the time, they are not cyber experts, but have an internal or external diploma in IT, as well as in telecommunications or messaging systems maintenance. Modern navies educate their officers and crew to cyber-security during their education period. For non-IT staff, this education is mainly on a very short period and tackles their specific responsibilities as end users. This process is sometimes mandatory, as well as a meeting with their cyber-security officer during in-and-out assignment process, called in and out processings. Cyber awareness is a matter of continuing education and procedures, like in and out processings, but also onboard training: once assigned on board a ship or shore units, IT people are regularly trained, together with the whole crew and headquarters to react properly to realistic cyber-attacks, whether on dedicated platforms or during typical red team/blue team exercises [24][25]. Some Ministries or Departments of Defence also organize major cyber-defence exercises, targeting the naval sector amongst others such as, for instance, DEFNET or other exercises in France[26]. This shows that the level of preparation to cope with cyber crisis is now taken seriously and on a formal and regular basis, just like any other kind of navy training.

However, even in that case of maturity, personnel on board ships are not cyber experts, at least on small and medium vessels. In case of a real cyber event, they would have to escalate the event to shore cyber expertise centres for support, analysis or intervention. Due to the lack of cyber experts, and the impossibility to have them onboard on a permanent basis, this situation is unlikely to change soon.

B. Processes for maritime cyber-security

In history, the maritime sector has experienced a number of accidents, leading to casualties, shipwrecks and high impact on environment. This has lead to the regulation of the sector being mainly based on safety, registration and certification, insurance processes and a number of regulations. Two of the most known regulations are the International convention for the safety of life at sea (SOLAS) and the Global Maritime Distress and Safety System (GMDSS).

Concerning cyber, the following guidelines have been issued specifically to the attention of the maritime sector and are usually taken as references in France:

- ANSSI[27], with a best practise guide for cyber security on board ships;
- IMO[28] and its recommendations on maritime cyber security;
- BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, IUMI, OCIMF[29], with the cyber security guidelines they issued for ship owners and operators;
- ENISA[30] and its analysis on specific cyber threats to the maritime sector and the recommendations the agency issued.

However, in those guides, recommendations remain high level and mostly identical to generic best practices for cyber-security issued for most IT or industrial sectors[31]. The maritime sector is wide and global: those many guidelines may also prove to be conflicting with other national regulations or even between each other[32]. As we read them today, they prove to be years behind what they would need to be to cope with the high level of attackers, the wide attack surface and the potential impacts on the sector. If we take the detection process as an example, it is defined as an essential part of the NIST framework (Identify, Protect, Detect, Respond, Recover)[33]. The recommendation also exists for other industrial or critical sectors, where requirements are clearly established to connect remote systems to a central Security Operations Centre (SOC). But specific recommendations or regulations on cyber-detection for the maritime sector are non existant. While, like other critical sectors, the maritime transportation and the navies would certainly have to report incidents to a regulation authority, there is no current precise regulation protecting the maritime sector and requiring a clear monitoring and detection process. This lack could be explained by a low maturity level in this sector to implement this kind of complex architecture. We have also noticed that, if alerting processes exist for the maritime sector, for instance for piracy prevention and alerting, they do not include cyber. Given the time needed to achieve those long-term evolutions and the progressive increase in maritime cyber-awareness, it seemed to us that this work has to be started as a matter of urgency.

C. Technologies for maritime cyber-security

Cyber-security may be seen as an efficient combination of networked and host-based secured technologies from the physical to the application layer. It also relies on external security techniques, from the human security to the avoidance of environmental incidents which could impact IT/OT assets. Most quoted guides and articles do not issue specific technological requirements for the maritime sector and rely on common usual guides, issued as standards or recommendations. Securing a maritime information system should of course rely on common and usual requirements and recommendations as can be seen in traditional IT and OT systems. But we have seen that they have specific characteristics which make it difficult to ensure an up-to-date cyber-security level. For instance, the integration of multiple navigation and management technologies and brands at the bridge level requires interoperability between those systems and therefore relies on exchange protocols which are often unsecured. This is, for instance, the case of many navigation information distribution systems, where the data frame broadcasting the latitude, longitude, course and speed of the ship to several instruments on board the ship is unsecured, allowing for many attack vectors[34]. Even if new and secured protocols are on their way[35], the life cycle is so long that those types of systems will take a very long time to get enhanced and changed aboard.

This life cycle problem and the great difficulty to patch-in-time and secure those systems is common to other OT systems, for instance in the nuclear or oil industry. For the information security officer, this means: the longer those systems live, the higher the number of vulnerabilities exploitable on his systems[36]. This explains why the use of cyber-monitoring infrastructures to support embarked and ashore IT and OT systems is essential to provide a quick and appropriate response: cyber-monitoring has a direct role to play in the assessment of risk exposure. The use of such techniques on maritime systems together with a combined situation awareness can greatly enhance the cyber-security level. This choice has been made for instance by the European SAURON[37] project for port infrastructure monitoring.

However, our goal is to be able to monitor not just one harbour but many harbours as well as ships at sea, with higher constraints. The result will be a proper and wider cyber situational awareness on a whole fleet and port infrastructures which can be used by a navy or a national agency to monitor a complete maritime sector, where cyber also acts as a convergence factor for IT and OT sectors.

IV. Design constraints for a maritime cyber-monitoring platform

Designing a cyber-monitoring architecture and building a Security Operations Centre (SOC) is a long term project with plenty of pitfalls.

Most existing and helpful guides for building a SOC, such as MITRE's[38] focus on the organizational processes of a SOC to make it reliable and perform as expected. The French Agency for Information Security (Agence Nationale de Sécurité des Systèmes d'Information, ANSSI) issued a complete guide of requirements for cyber-detection specialized Managed Security Service Providers (MSSP). This guide [39] proposes an overall cyber-detection architecture we have been following, enabling the data to be shipped to a central site (SOC) to be processed, normalized and analysed, while enabling the distant site to have an overview of the possible incidents detected in its IT premises. While describing network requirements, this middle-level guide does not suggest a precise architecture for cyber detection pipelines or sensors.

Collecting event logs, network/host detections and traditional useful metadata for cyber-detection is not a real problem for traditional SOCs, because of the large bandwidth capacities which are available in modern data centres or offered over WAN by Internet Service Providers. The traffic is heavy, but the capacity to absorb it is mainly there, both on the network side and during the ingestion process, thanks to the use of big data software suites for log processing, analysis and storage. The case we have studied may also be encountered in

industries using remote production sites, such as oil industry, electricity or drinkable water production sectors.

However, those sectors do not reach the complexity of naval systems architecture and constraints. The characteristics we are talking about, combined on naval systems, complexify the cyber-monitoring architectures which could be set up. We have synthesized those constraints as follows. They fix the network and software requirements for the remote side of cyber-monitoring infrastructure. First of all, cyber-monitoring system must prove to be isolated from supervised systems: it should not impact them and we should be able to observe without interrupting them (Safety is paramount). Cyber-sensors, one for each network/information system, must keep isolated networks safe and cope with high integration constraints and specific features of each system. The bandwidth used by the cyber-surveillance process must be controlled and monitored at all time to ensure that it is limited to a value coherent with the operational bandwidth and costs. Satellite link up and down times must also be automatically managed to avoid data loss while still allowing a local monitoring. Finally, even if the network flow analysis is run on board by sensors, alerts and metadata flows have to be carefully selected to avoid useless data being sent to shore.

Researchers at ANSSI issued an article[40] which describes the system and network levels of a safe Network Intrusion Detection Sensor (NIDS). The architecture describes a local sensor capable of monitoring several networks, without interconnecting them physically, and with the possibility to have specific sets of detection signatures and protocol processors (such as specific processors for industrial systems[41]) for each of them. The collected data can then be shipped to be ingested in a central SOC. This article was useful to set up the needed custom NIDS systems in our naval detection architecture. However, once again, the complete data pipeline is not described in the given article and the naval characteristics we have summed up in the previous sections are not fully met by the architecture description.

The five constraints aforementioned, taken one by one, seem to be quite easy to cope with, but their combination highly complexifies the final architecture.

V. Our architecture for a fully capable maritime cyber-monitoring operational capacity

As we have presented earlier in this paper, no off-the-shelf solution meets the high requirements of a cyber-monitoring architecture for naval systems. In this section, we describe the functional blocks which were chained to achieve our goals. The architecture, shown in figure 1, could also be useful for other industrial cases with similar requirements.

A. The remote site

The shore infrastructure can be on a remote site from the central SOC, linked to it via a reliable WAN or satellite connexion. The medium to large size merchant, passenger, oil or gas production platform or military ship is linked to the shore via a standard satellite link. We have designed six functional blocks to fully meet our requirements.

The first block is Network Connexion Safety (NCS), which ensures a high level of harmlessness on the supervised system. As we have seen, the monitoring sensors must be safely connected to the supervised systems. When dealing with network sensors, the solution provided enables to have one to many capture ports on the network. On board, this block is achieved by using usual capture technologies, such as port mirroring on traditional or industrial network switches and the use of dedicated Test Access Ports (TAP).

The second block is Network Probe Isolation (NPI). Each sensor is isolated from the others, so each sensor, while being hosted on the same server, can have its own engine, preprocessor and detection schemes and signatures. It also enables the possibility to configure the probe to fetch specific metadata and metrics depending on the kind of system supervised. Those features are essential for a proper hunting of cyber-attacks.

The third block is a Local Preprocessor (LP). The LP synchronizes timestamps between all metadata, normalizes the inputs, adds filters or transforms the data if necessary, and correlates events and alarms to limit the impact on the satellite uplink.

The fourth block it the Local Engine (LE). The LE stores events on premises, allowing for long term read-only retention for legal purposes and local alerting.

The fifth block is the Ship Shore Manager (SSM): it acts both as a cache and processor to ensure data is properly sent to shore. It can also prioritize data being sent depending on tags, for instance to send alerts first and metadata/logs afterwards to take into account the latency of satellite links. In case the satellite link is not available, data is cached in memory or disk to provide a backlog which is automatically and timely sent when the link is back on duty. This engine also manages the bandwidth, allowing to set up a precise throughput to use only the allowed portion of the satellite link. The available throughput can be manually set up to a limit or depend on the real activity of the link. While called Ship Shore, this item can also be set up on remote shore sites, mainly depending on the quality and bandwidth of the link between the remote site and the central SOC.

Finally, the sixth block is the Cyber Situational Awareness Console (CSAC). Using this console, the crew of the ship has a simplified yet complete overview of the onboard cyber situation, giving operational and technical knowledge about the impacted systems and the details associated, together with immediate tasks to achieve. Apart from operational dashboards, this console gives an impact assessment of the cyber event on the ship's capabilities, which we call Cyber Battle Damage Assessment (CBDA). This console also propagates a common cyber situational awareness between the crew and the SOC. Sharing the same information is essential to gain time and help the ship's captain to take the good decisions.

The link between the remote sites and the SOC has to be secured as it carries critical information and should not be corrupted nor captured. Depending on the company or national information security policies, it can be encrypted to avoid interception and also provide a logical isolation from the other ship/shore network flows with the use of specific virtual links

and crypto material. This feature, which seemed essential to us, can be mitigated due to the additional cost on bandwidth when using layer 3 or lower network encryption protocols.

While cyber-monitoring of remote sites highly relies on satellite link quality, which means that the central site can be blind in case of failure, the quality of those links, the presence of efficient resilient satellite links or installations on board ships reduce the risk of link loss. The design of our architecture also allows for a local alarming capacity even in case of satellite link loss.

The only drawback of the architecture is its security level. Having a full isolation from the monitored systems means the SOC cannot react on the remote systems after a detection. While this can be mandatory due to national regulations, this is also safer. The immediate intervention can easily be handled either to the remote site to take proper measures, or to the network operations centre or IT/OT operations managers.

B. The maritime SOC

On the shore side, the network flows usually either exit at the fleet management centre or at the SOC, either hosted or at the sub contractor premises. After the possible crypto equipment used for deciphering, the first block is the Ship Shore Manager (SSM). It completes the specific channel between SSMs, ensuring all collected data on board properly exits on the shore side as expected, in a timely and ordered manner, and within the specified bandwidth limits. Then, the second block is the Central Processor (CP). All metadata, logs and alerts flowing from remote sites are centralized on the CP where they are pipelined, filtered, normalized or transformed as needed by the SOC. The third block is the Data Store (DS). Traditionally, this can be a big data engine, enabling the secured storage of data and its indexing for efficient queries. Finally, the fourth block is the Bandwidth Manager (BM), used to set up and monitor the bandwidth configuration for distant sites.

The other assets of the maritime SOC are quite common with what can be found in modern SOCs for analysis, display and common services. The Cyber Awareness Toolchain (CAT) is primarily used by SOC level 1 and 2 maritime experts for cyber detection engines and signature tuning, big data analytics, automated searches and graphs, as well as alerting and displaying. We also use this tool chain to link the maritime SOC with Threat Intelligence sources, Digital Forensics and Incident Response (DFIR) as well as Security Incident Response Platform (SIRP) platforms to boost its efficiency on threats, analyse malwares or phishing, and follow the incident response process and reports to the management level. Maritime Cyber Situational Awareness (CSA), short and long term, is processed this way. We also hope one day, that with such tools, specific naval or generic Threat Intelligence (TI) and IoCs sharing between fleet managers will become a reality. The fleet / maritime RCP Recognized Cyber Picture (RCP) is used to ensure a proper display of the individual ship and fleet cyber overview, which is needed to help the SOC engineers and managers giving directions to their cyber-related decisions or to help for crisis management and risk assessment. Finally,

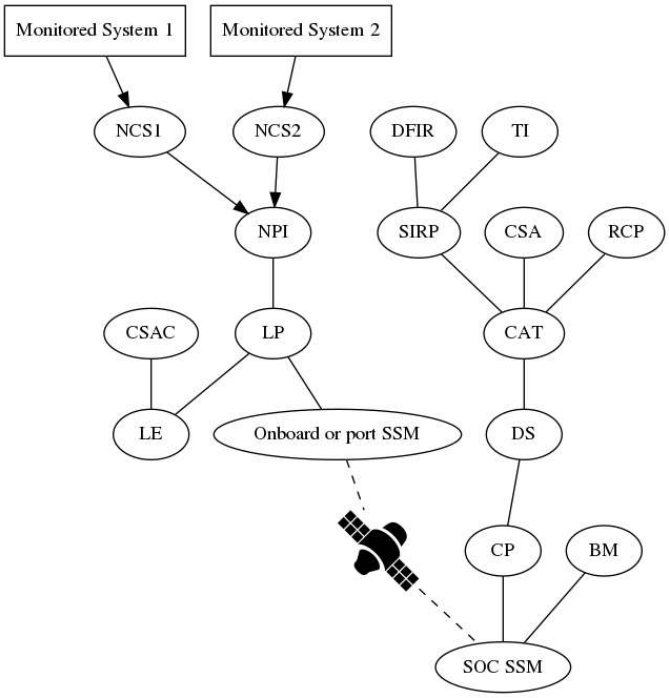

Fig. 1. Overall architecture of the maritime cyber-monitoring capacity with the distant site (left) and the maritime SOC ashore (right).

the Common Services (CS) tool set consists of services like Domain Name Service, Network Time Protocol and other tools essential for the proper work of a cyber-detection tool chain.

VI. Results of the proposal for a Maritime Security Operations Centre

The design and tuning of each functional block has been a real challenge, especially when working on networks where data flows or even assets are sometimes unknown. One of the biggest issues when writing signatures was to cope with specific proprietary data formats, which we had to capture, analyse, understand, formalize, test, and retest, to make sure our detection scheme and signatures, up to the application level, were precise and good enough to avoid false positives as much as possible.

As shown in Figure 2, data flows on the distant networks are monitored by the sensors in the NPI (2) through the corresponding NCS (1). The NPI extracts valuable data from the network flows, called metadata. Depending on the signature rule sets, when a malicious flow is detected, the NPI also sends an alert, together with the relevant metadata. The flows from the NPI are sent to the LP (3) to be synchronized and normalized, before being stored on the LE (4). In case of an alert, the CSAC on board the ship will display the corresponding data (5). When there is no alert, usual graphing tools are used to give the crew a cyber situational awareness of the network activity for both OT and IT. The LP pipelines the data to be sent to shore to the onboard SSM (6), acting as a memory buffer and flow control asset. Alerts are passed first, followed by metadata. When the link between the SSMs is not effective, the whole data is stored on the distant SSM

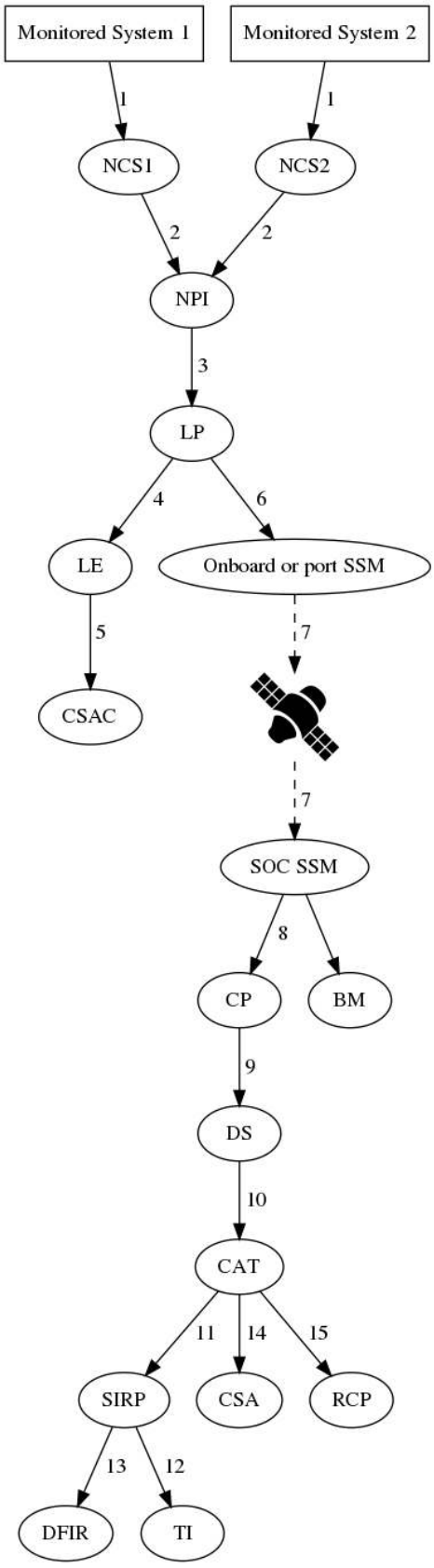

Fig. 2. Metadata and alerts processing in the maritime cyber-monitoring capacity with the distant site (top) and the maritime SOC ashore (down).

and the link failure is displayed on the CSAC and shore CSA. If the link is functional, alerts and metadata from all sites go through the SSM (7) and are gathered by the CP (8). The CP treats the flowing documents, merging, filtering, formatting or enhancing their fields so the data stored on the DS if of highest quality (9). The alerting tools on the CAT (10) are permanently querying the DS with generic or specific requests on the indexed metadata. For instance, the alerting framework periodically searches the DS for specific values in fields, to detect cyber events in logs, such as repetitive failed Secure Shell (SSH) connexion attempts as *root*. In such case, the alerting tool automatically creates an incident in the SIRP, enriched with the relevant metadata it gathered (11). When a new threat is known trough the use of TI feeds (12). SOC experts following the feeds can also task the DFIR tools for specific analysis of the data stored in the DS (13). Finally, CSA and RCP are used to display the present cyber situational awareness, the trends and the impact of cyber on global operational naval activities for risk assessment (14, 15).

The quality of each functional block as well as the overall performance of the architecture has been thoroughly tested. First of all, with the help of professional red team experts to ensure a high level of confidentiality, integrity and availability of the cyber-monitoring platform. This process has also been used to confirm the total harmlessness of the cyber-monitoring process on the monitored systems as well as between them. The tests also confirmed the high quality of cyber-detection by the design of specific preprocessors on proprietary systems, as well as of the quality of the detection signatures written for the maritime systems.

Large simulated interruptions or limitations on the satellite bandwidth have also been tested to check that no data is lost and that, when the satellite is back, data is properly ordered, prioritized, collected and sent to its destination; those tests also confirmed the good working of the CSAC on board the ship, even in case of loss of the link to the SOC.

Finally, we have confronted the system with cyber-attacks simulations to ensure a highly beneficial balance between the metadata and logs being sent ashore with the detection quality and with the bandwidth clipping. The bandwidth is now optimized and fullfils our requirements.

VII. Future work

Three and related steps have yet to be developed on a deeper basis to finalize an overall excellent cyber-situational awareness. First of all, the creation of time-related graphs on the data lake would assist SOC analysts understanding and ”fighting” against cyber events over a large amount of data. This is essential, but difficult, due to the amount of data collected, the potential high number of sensors and the risks of mis-interpretation of graphs (for instance, some local networks share common IP address plans). Another plan is to study and implement proper graphing and displaying methods for metadata depending on their type and features to create rich, dynamic and still efficient dashboards for ship commanders, SOC, and headquarters/fleet managers. Finally, we plan to integrate the Cyber Situational Awareness with

other situational awareness tools to ensure a better overall risk management and to provide more complete and richer information to build the situation awareness. For instance: intrusion detection, CCTVs, fire detection and cyber events could be efficiently linked and displayed together to ensure a high level efficient common picture of the situation.

VIII. Conclusion

In this paper, we have presented the context of maritime information systems, whether ashore or onboard, with the various types and characteristics they share. Whether civilian or military, we have described their unique characteristics.

We have demonstrated that those unique characteristics require a dedicated detection and data pipeline architecture that common SOC and cyber-detection architectures do no provide.

In addition, we have described the remote and central functional blocks we have designed and integrated to meet our requirements.

The overall is a summary of the characteristics of a maritime cyber Security Operations Centre compared to a traditional one, and why a proper cyber-detection architecture has to be taken into account during the engineering process of modern ships, naval infrastructure, and fleet management centres.

Our current platform is still heavily and daily tested to check its performance on huge data sets, as well as to verify that its cyber detection is at the highest expected level and reacts properly even in a "crisis situation". The results currently achieved are highly positive. Our platform has been presented to officials and experts, raising enthusiasm amongst cyber experts and maritime commanders and executives, both civilian and military. The exchanges with those experts were extremely valuable, enabling us to add new features or updating the platform characteristics to meet new or updated requirements and address the feedback. We are now challenging the platform with real-life and real-time situations at sea and ashore on complex systems to collect more results and achieve success.

References

[1] Internal Chamber of Shipping. Ics - key facts. Accessed: 2018-05-20.

[2] Marine Insight. 10 world's biggest container ships in 2017. Accessed: 2018-05-20.

[3] Royal Caribbean Press Center. Symphony of the seas fact sheet. Accessed: 2018-05-20.

[4] Peter Dombrowski and Chris C Demchak. Cyber war, cybered conflict, and the maritime domain. Naval War College Review, 67(2):70, 2014.

[5] Oliver Fitton, Daniel Prince, Basil Germond, and Mark Lacy. The future of maritime cyber security, 2015.

[6] Ørnulf Jan Rødseth and Kwangil Lee. Secure communication for e-navigation and remote control of unmanned ships. In Proc. of the 14th Conference on Computer and IT Applications in the Maritime Industries-COMPIT, volume 15, 2015.

[7] Kimberly Tam and Kevin Jones. Cyber-risk assessment for autonomous ships. 2018.

[8] Ryan Burton. Cybersécurité et marétique, un enjeu européen ? Centre d'études stratégiques de la marine. Accessed: 2018-05-20.

[9] Satellite Markets & Research. Executive summaries of market trends and opportunities in key market segments and regions worldwide, the maritime satellite market. Accessed: 2018-05-20.

[10] Bullguard blog. Cyber-attacks and underground activites in port of antwerp. Accessed: 2018-10-20.

[11] Joseph DiRenzo, Dana A Goward, and Fred S Roberts. The little-known challenge of maritime cyber security. In Information, Intelligence, Systems and Applications (IISA), 2015 6th International Conference on, pages 1–5. IEEE, 2015.

[12] MAERSK. Cyber-attack update. Accessed: 2018-05-20.

[13] Michael G Frodl. Pirates exploiting cybersecurity weaknesses in maritime industry. National Defense-Journal of the American Defense Preparedness Association, 96(702):22, 2012.

[14] Observatoire du monde cybernétique, 1er trimestre 2014. pages 17–25. Accessed: 2018-05-20.

[15] Erwan Alincourt and Cyril Ray. Méthodologie d'extraction de signatures issues des signaux ais. Symposium sur la sécurité des technologies de l'information et des communications, 2016.

[16] MARSH. The risk of cyber-attack to the maritime sector. Accessed: 2018-05-20.

[17] NCC Group. Ncc group - preparing for cyber battle ship. Accessed: 2018-05-20.

[18] Kevin D Jones, Kimberly Tam, and Maria Papadaki. Threats and impacts in maritime cyber security. Engineering & Technology Reference, 2016.

[19] Joseph O. Eichenhofer, Elisa Heymann, and Barton P. Miller. In-depth software vulnerability assessment of container terminal systems. 2017.

[20] Peter Beaumont. Cyber-risks in maritime container ports: An analysis of threats and simulation of impacts. 2017.

[21] MAERSK. The world's largest ship. Accessed: 2018-05-20.

[22] Zoran Škrlec, Zlatimir Bićanić, and Joško Tadić. Maritime cyber defense. In 6th International Maritime Science Conference, page 19, 2014.

[23] International Maritime Organisation. Maritime cyber risk management in safety management systems. In US Coast Guard; The Maritime Safety Committee, 2017.

[24] US Navy. Fleetwide cyber awareness challenge training update. Accessed: 2018-05-20.

[25] David Brosset Gaël Héno Thibaud Merien Olivier Jacq Yvon Kermarrec Thomas Becmeur, Xavier Boudvin and Bastien Sultan. A platform for raising awareness on cyber security in a maritime context. International Conference on Computational Science and Computational Intelligence, 2017.

[26] Centre d'études stratégiques de la marine. The french navy and maritime cyberdefense, September 2015. Accessed: 2018-05-20.

[27] Agence nationale de la sécurité des systèmes d'information. Best practices for cyber security on board ships. Accessed: 2018-05-20.

[28] International Maritime Organisation. Guidelines on maritime cyber risk management. Accessed: 2018-05-20.

[29] BIMCO. Guidelines on cyber-security onboard ships. Accessed: 2018-05-20.

[30] Dan Cimpean, Johan Meire, Vincent Bouckaert, Stijn Vande Casteele, Aurore Pelle, and Luc Hellebooge. Analysis of cyber security aspects in the maritime sector. Technical report, ENISA, 2011.

[31] Christopher R Hayes. Maritime cybersecurity: the future of national security. PhD thesis, Monterey, California: Naval Postgraduate School, 2016.

[32] Lars Jensen. Challenges in maritime cyber-resilience. Technology Innovation Management Review, 5(4):35, 2015.

[33] National Institute of Standards and Technology. Framework for improving critical infrastructure cybersecurity. Accessed: 2018-05-20.

[34] Pen Test Partners. Crashing ships by hacking nmea sentences. Accessed: 2018-05-20.

[35] International Maritime Electronics Alliance. An ip/ethernet interface standard for marine electronic devices. Accessed: 2018-05-20.

[36] Andrew E Tucci. Cyber risks in the marine transportation system. In Cyber-Physical Security, pages 113–131. Springer, 2017.

[37] Scalable multidimensionAl sitUation awaReness sOlution for protect-iNg european ports. Sauron project, the concept. Accessed: 2018-05-20.

[38] Carson Zimmerman. Ten strategies of a world-class cybersecurity operations center. MITRE corporate communications and public affairs. Appendices, 2014.

[39] Agence nationale de la sécurité des systèmes d'information. Security incident detection service providers - requirements reference document. Accessed: 2018-05-20.

[40] Pierre Chifflier and Arnaud Fontaine. Architecture système sécurisée de sonde de détection d'intrusion réseau. In C&ESAR; France, 24-26 November 2014, 2014.

[41] D Diallo and M Feuillet. Détection d'intrusion dans les systèmes industriels: Suricata et le cas de modbus. In C&ESAR; France, 24-26 November 2014, 2014.