Maritime Cyber Situational Awareness Elaboration for Unmanned Vehicles

Olivier Jacq[a], Pedro Merino Laso[b], David Brosset[a,c], Jacques Simonin[a,d], Yvon Kermarrec[a,d] and Marie-Annick Giraud[e]

[a]Chair of Naval Cyber Defense
Funded and supported by École navale, ENSTA Bretagne, IMT Atlantique, Thales and Naval Group, CC 600 F-29240 Brest Cedex 9, France
[b]French Maritime Academy (ENSM) - 38 Rue Gabriel Péri BP 90303 F-44103 Nantes Cedex 04, France
[c]Naval Academy Research Institute, Ecole navale - CC 600 F29240 Brest Cedex 9, France
École navale - CC 600 F-29240 Brest Cedex 9, France
[d]IMT Atlantique - Lab-STICC, F-29238 Brest Cedex 3;
[e]SOFRESUD, 777 Avenue de Bruxelles F-83500 La Seyne sur Mer, France

ABSTRACT

In history, concurrence for dominance at sea has always been a major concern for most sea-facing countries. As the vast majority of worldwide goods exchanges are made by sea, an answer to the growth of the worldwide commerce over the last twenty years has been to increase the size and on board value of ships sailing between eastern and western countries. Digitalization has also been an answer to ease the routing, management, conning and overall return on investment of such ships. But as the cyber surface attacks consequently widened, the maritime sector became a real interest for state-sponsored and criminal hackers. The concern of a major cyber-attack targeting ships at sea or naval shore infrastructures is no more science fiction, and late incidents do confirm the urgency to act. "Safety is paramount" is a known motto on board ships, the crew being drilled for fire and water floods. However, the awareness of the sector on cyber remains low and if modern ships have a reduced crew, autonomous ships are arriving with just nobody on board. This is the reason why, on top of the usual cyber-security measures, the implementation of intrusion detection systems on unmanned vehicles is essential to detect, react and stop any incoming threat. In this paper, we outline the main challenges for the years to come on Maritime Cyber Situational Awareness (MCSA) for autonomous and remotely controlled vehicles.

Keywords: Cybersecurity, maritime, situational awareness, autonomous, unmanned vehicles

1. INTRODUCTION

The use of digital systems is now essential for any civilian or military maritime activity. As a consequence, the availability, integrity and confidentiality of those systems are of the uttermost importance. Newest generations of ships as well as Unmanned Surface Vehicles (USVs), Unmanned Air Vehicles (UAVs) and Unmanned Underwater Vehicles (UUVs) are built around computers and digital sensors to ensure all their missions, from communications, positioning and conning to situation awareness, combat systems, intelligence and, of course, engine and platform management. Another characteristic of the digitalization of ships is a high use of network interconnection to help automation and ease the overall situation awareness, giving the commanding officer and crew a better understanding of what's going on in their own ship and in surrounding maritime activities. The number of sensors available over the network is increasing and heterogeneous systems historically isolated are now interconnected, widening the surface attack of a ship and underlining the urgency to protect them properly.

Further author information: (Send correspondence to O.J.)
O.J.: E-mail: olivier.jacq@ecole-navale.fr
P.M.L.: E-mail: pedro.merino-laso@supmaritime.fr
D.B.: E-mail: david.brosset@ecole-navale.fr

Advanced research, testing and operational deployments are under way on autonomous and unmanned vehicles for surface, aerial and underwater use. As embarked crew is replaced by automation and remote control operations, cyber-security is no option but an important challenge. Research works address this problem from multiple axes such as risk assessment,[1] secured architectures[2] and novel role-based access definition.[3] Adding autonomous features on already vulnerable protocols and systems like Industrial Control Technologies (ICT) draws new attack vectors and an underlined incapacity of facing cyber-attack from within an unmanned vehicle. Detecting and hunting cyber-threats will become a more complex task of that equipment. Specifically, their reaction in case of an emergency such as a cyber-attack has to be anticipated and formalised, down to the software and the hardware, to avoid any physical damage to self, to peers, or to the environment. But, before being able to properly react to a cyber-attack, those vehicles first have to be designed with a very high level of security and safety to be protected from most advanced threats all over their life cycle. Proper detection and reaction schemes must then be designed to detect, alert, and safely react, as one but also as a whole when a coordinated attack against an autonomous vehicles fleet is concerned. As an answer, the Sea4M project[2] aims to define a dedicated security architecture for managing and controlling USV fleets. This project has proposed a novel Human-Computer Interaction (HCI) development that adapts itself to particular roles to address Maritime Situational Awareness (MSA) for specific user's needs. This work is a first step to include MCSA in Sea4M's architecture to provide a full overview of the system state for each particular user.

2. RELATED WORK

In this section, we will underline that Situational Awareness (SA) is a challenging goal for tele-operated systems and that MCSA should be seen a subset of it. The elaboration of MCSA depends on three prerequisites: an efficient knowledge of digital assets, a dedicated maritime CSA and performing visualisation schemes.

2.1 Maritime digital assets cartography

The "knowledge of us" is an essential knowledge both to SA and cyber-security. To correctly assess risk and protect systems, one needs to understand the way systems are designed, set up and run. However, applied to maritime, the commanding officer (CO) of a ship has not designed the boat he's commanding. If he has an excellent overview of her reaction at sea, facing winds and waves, the usual knowledge he has of his onboard Information Technology (IT) and Operational Technology (OT) is usually the multiple function displays set at the bridge. This fact can be explained because the design of a ship is based on the integration of multiple Commercial Off-The-Shelf (COTS) systems, for instance Electronic Chart Display Information System (ECDIS), Automatic Identification System (AIS), Global Navigation Satellite System (GNSS) as well as Programmable Logical Controller (PLC) and Industrial Control Systems (ICS) for platform management. Each of those systems is designed by subcontractors. The shipbuilder usually only has an integration role to make the systems communicate together. If alarms are, however, frequently generated in a logging window per system, there is usually no central or global awareness on how the ship systems are performing.

2.2 Cyber Situational Awareness

Situational Awareness has been described by Mica Endlsey as a "state of knowledge".[4] Her work, based on situation perception, comprehension and projection, has been applied to meet the Air Force needs. One can think of the wide use of Head Up Displays (HUD) in aviation as a very good example of help for the pilot to achieve SA. Applied to maritime, MSA can be seen as a fusion of the "knowledge of them" (the maritime environment such as weather conditions, position of other ships, situation intelligence) and the "knowledge of us" (own situation concerning security, safety, conning, weapons and ship's status) in perspective with mission assignment[5] to help decision makers. Therefore, MSA depends on internal and external-facing sensors, intelligence, and mission planning and knowledge.[6] MSA can have different levels of abstraction, at a ship's, fleet and HQ or shipowners' levels. However, sensors and computers are, most of the case, domain-focused (engine situation, platform management, ECDIS, etc.). The existence of interconnection protocols such as National Marine Electronics Association's NMEA0183 and following greatly helps data sharing, mostly within the bridge. However, other domains from engine and platform management still use dedicated visualisation, platforms and protocols. As a consequence, most commanding officers still have to switch from a display to another to achieve situational awareness.

Franke and Brynielsson[7] remind us that Cyber Situational Awareness (CSA) should not be seen as a goal by itself, but as a subset of global SA, underlining an important effort still has to be drawn for the fusion of CSA to SA, and therefore for the fusion of Maritime CSA (MCSA) to MSA. Current efforts on the MCSA research cover the intrusion detection and architecture[8] as well as an overview of MCSA to help decision makers for the maritime sector.[9] Challenges for elaboration of the MCSA remain multiple. Maritime systems encounter a number of physical constraints which complexify MCSA elaboration, this complexity getting just higher when it comes to unmanned and autonomous vehicles. A first difficulty is isolation at sea, which sets a high level of dependency on satellite links. IT and OT support at sea also remains complicated due to the usual lack of IT/OT experts on board. Satellite coverage and environmental conditions may also lead to temporary link failures and limited bandwidth. The very long life-cycle and design of the ship imply the onboard integration of heterogeneous COTS systems coming from various builders. Their onboard integration is often minimal, mostly just set to enable communication, without much - if any - security features such as content control and filtering or network isolation. Subcontractors, as well as ship integrators, are reluctant to authorize patch management on board to mitigate vulnerabilities. Most software, such as ECDIS, have to undergo new tests to get fully requalified and avoid regression. The same also applies to drones and autonomous vehicles: for instance an UAV would have to be re-qualified after patching and follow intense sea trials to give a high assurance on the absence of any regression due to the patch. When intrusion detection systems are deployed on board, their ability to detect attacks remains low. This is due to their limited possibility to process maritime and industrial specific protocols: even if correctly set up and maintained with up-to-date signatures, such sensors also have to be monitored on a permanent basis by experienced shore-based cyber-security engineers to detect threats. Finally, while MCSA should just be a subset of MSA, cyber-security experts usually lack maritime experience and therefore often fail to measure the impact on the ship's mission. On the contrary, commanding and watch officers' awareness on cyber remains low and lack knowledge, time and procedures to search for causality assessment and precisely measure the possible impact and spread of an attack on the ships' IT and OT systems.

2.3 Visualisation

The fusion and visualisation of all available information for the crew are important challenges. While the amount of data coming from sensors is increasing, the risk that crucial information is not taken into account or that only partial information is given is real. Several studies are working on augmented reality and HUDs for the maritime sector[10] and draw the design for the bridges of the future. But, due to the lack of connexion and common protocols between cyber Intrusion Detection Systems (IDS) and common bridge tools, MCSA and cyber alarms are not part of it. Finally, when talking of a task force commander or headquarters staff, MCSA, when achieved, has to be displayed using a proper abstraction level. For instance, the usual high level of false positives encountered on traditional IDS sensors underlines that only qualified incidents have to be shared with mission commanders. Causality and impact assessments are also key values commanders are looking for, to confirm or modify their action course.

3. CYBER SITUATION AWARENESS FOR SURFACE UNMANNED VEHICLES

The progress in digitalization and autonomy will cross another step forward with unmanned vehicles. In a few years (if not now), a modern fleet will combine such vehicles, either as a whole or as a subset of traditional maritime assets. Remote surveillance of a vehicle's fleet will be paramount to accomplish the mission safely. SA for those assets has to take into parameter the cyber state of the vehicles. However, their small form factor, limited capacities in energy and communication as well as environmental constraints will challenge intrusion detection. Unmanned vehicles add complexity, heterogeneity and widen the attack surface of traditional maritime assets.[1] Their "autonomous" way of acting should not lessen the attention on the fact that they add new and strong dependencies on satellite communications, position systems and external facing sensors (radars, cameras). Whether acting alone or as a coordinated fleet, those unmanned digital systems of systems could be lured, locally or remotely, just by flawing the sensors or by reverse engineering their software to exploit design flaws.

3.1 Situation Perception

On an intrusion detection point of view, unmanned vehicles will embark a high number of new sensors, flowing real time or differed-time data to shore or ashore back-end platforms. This volume of data also means a possibility to corrupt data being sensed and transmitted to change the way back-end platforms behave. Detecting such intrusions on a high volume of data is a hard task. While the programmed reaction to an unknown behavioral or value on a sensor is highly critical and has to be formally approved and tested, the real behaviour, which can be hard-coded in the software, is usually only known by the vehicle designer.

On a whole fleet of unmanned vehicles, the multiplicity of intrusion detection system agents (whether network or host oriented) on multiple sources adds complexity: detecting a coordinated cyber-attack gets even more complicated. Finally, perception relies on detection schemes: anomaly-based detection for those vehicles is a solution, using techniques such as machine learning to learn of the normal behaviour in various conditions. However, this approach needs training datasets, implying a very high level of training of the model, meaning a test in every possible condition is necessary to later flag any deviation. If this condition is not met, the false positive rate can be very high. On the other hand, a behaviour-based detection also seems complex: looking for Indicators of Compromise (IoC) on such systems requires having a very high level of knowledge on its way of working (operating systems, network communications, processes). On specific chipsets, real-time operating systems and proprietary networking protocols, using such sensors might reveal not to be pertinent.

Finally, this multiple-agent and multiple-source detection scheme on unmanned vehicles will need data to be sent to a dedicated Security Operations Center (SOC) for analysis. Choosing between real-time and past-mission analysis is a crucial choice. Real-time means a permanent, dedicated and secure link will have to be set between vehicles and the SOC, which is nearly impossible to achieve - or at a very high price on discretion and bandwidth for UUVs, and which would have an important impact on available bandwidth for maritime UAVs too. Long haul USVs and autonomous commercial ships are probably best targets to meet this requirement. The quality features for situation perception (freshness, truthfulness, completeness) and hence the overall quality of MCSA will highly depend on the choices made at this step.

3.2 Situation Comprehension

Situation comprehension is met when causality assessment, impact assessment and attacker perception are met. Assessing causality means the data gathered during the recognition phase is complete enough to determine where the attack came from. However, forensic experts need a lot of time and data to qualify a complex attack. For instance, snapshots of memory, full low-level copies of hard drives and live captures of network traffic and processes usually needed. This amount of data is impossible to send over a network on a live unmanned system and has to be done afterwards (if the vehicle is not lost). This causality assessment also means all passwords, architecture information and software are accessible, understandable and known by forensic experts. The lower price of storage can give hope to the fact that a lot of logging and debugging data will be held on board such vehicles.

Understanding the attacker's perception is based on causality assessment but has to be cross-checked with generic (such as MITRE's) or dedicated[11] attack frameworks, but also with impact assessment. However, assessing the impact once again implies the overall architecture and working of the vehicle are known, which is rarely the case. This is due to the fact that such vehicles are often COTS by themselves, and that manufacturers set a high level of intellectual property on both software and hardware, making it a ”black box” to the final client. Analyzing data to separate the good from the evil will need the manufacturer to work with forensics experts.

A dedicated maritime SOC including autonomous vehicles is not always available and the operators of the system will always be the first line of defence. Unmanned fleet remote operation is realised by a particular role hierarchy that defines, for each user, specific duties and responsibilities. MCSA would gain in being abstracted for these roles with adapted pertinent information and take into account crisis management times.

3.3 Situation Projection

In such conditions, predicting the next step of the attacker is also a real challenge. With the low real-time data available to SOC analysts, setting a priority level on an event may lead to advanced attacks not being detected due to the lack of data and knowledge. On the contrary, a basic detection or a saturation of low-level detections may trigger unwanted reaction from the vehicle or from the SOC and decision makers, which could mainly be caused by stress or fear of a major impact on the fleet and act in prevention to avoid any further impact.

4. CONCLUSION

Digitalisation of ships and shore infrastructures has widened the attack surface of the maritime domain. While the current awareness of the maritime domain on cyber remains low, and as important incidents are unveiled, the fore-coming and increasing development and use of unmanned surface, aerial and underwater vehicles have to trigger a new way of thinking, designing and using digital assets in the maritime world. The evolution and correction of long-term processes for regulation authorities, subcontractors and ship builders such as *secure by design* and dynamic patching to cope with new threats will take a very long time. In this article, we have shown that intrusion detection for maritime assets, and specifically the integration of MCSA as a part of SA was an efficient way to go, to detect and react accordingly in case of a cyber-attack. Now is the time to embark highly efficient prevention, intrusion detection and resiliency features in unmanned vehicles. If this challenge is not properly taken into account, in case of targeted cyber-attack, it could lead to major cyber-physical issues once the vehicles are at sea.

ACKNOWLEDGMENTS

The project Sea4M, coordinated by SOFRESUD, is supported by the French Environment & Energy Management Agency (ADEME) in the frame of the Future Investments Program.

REFERENCES

[1] Tam, K. and Jones, K., "Cyber-risk assessment for autonomous ships," in [*2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*], 1–8, IEEE (2018).

[2] Merino Laso, P., Brosset, D., and Giraud, M.-A., "Secured architecture for unmanned surface vehicle fleets management and control," in [*2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech)*], 373–375, IEEE (2018).

[3] Merino Laso, P., Brosset, D., and Giraud, M.-A., "Defining role-based access control for a secure platform of unmanned surface vehicle fleets," in [*IEEE 2019 Oceans Conference*], IEEE (2019).

[4] Endsley, M. R., "Toward a theory of situation awareness in dynamic systems," *Human factors* **37**(1), 32–64 (1995).

[5] Riveiro, M., Falkman, G., and Ziemke, T., "Improving maritime anomaly detection and situation awareness through interactive visualization," in [*2008 11th International Conference on Information Fusion*], 1–8, IEEE (2008).

[6] Gad, A. and Farooq, M., "Data fusion architecture for maritime surveillance," in [*Proceedings of the Fifth International Conference on Information Fusion. FUSION 2002.(IEEE Cat. No. 02EX5997)*], **1**, 448–455, IEEE (2002).

[7] Franke, U. and Brynielsson, J., "Cyber situational awareness–a systematic review of the literature," *Computers & Security* **46**, 18–31 (2014).

[8] Jacq, O., Boudvin, X., Brosset, D., Kermarrec, Y., and Simonin, J., "Detecting and hunting cyberthreats in a maritime environment: Specification and experimentation of a maritime cybersecurity operations centre," in [*2018 2nd Cyber Security in Networking Conference (CSNet)*], 1–8, IEEE (2018).

[9] Jacq, O., Brosset, D., Kermarrec, Y., and Simonin, J., "Cyber attacks real time detection: towards a cyber situational awareness for naval systems," in [*2019 CyberScience*], 1–2, IEEE (2019).

[10] Wahlström, M., Karvonen, H., Kaasinen, E., and Mannonen, P., "Designing user-oriented future ship bridges–an approach for radical concept design," *Ergonomics in design: Methods and techniques* **1**, 217–231 (2016).

[11] Jones, K. D., Tam, K., and Papadaki, M., "Threats and impacts in maritime cyber security," *Engineering and Technology Reference* **1**, 1–12 (2016).