WHITE PAPER

CYBERSECURITY OF MARITIME DRONES AND AUTONOMOUS SHIPS

07/11/2023

SUPPORTED BY

FRANCE RELANCE

PREMIER MINISTRE
Liberté Égalité Fraternité

Secrétariat général de la mer

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

ANSSI

Région BRETAGNE

Brest MÉTROPOLE

FOREWORD

France Cyber Maritime is a non-profit organisation whose mission is to contribute to the strengthening of cybersecurity in the French maritime and port sector. The issue of cybersecurity for maritime drones and autonomous ships is a topic on which we were quickly approached. This question is the subject of frequent discussions with our members and partners, as well as with the Administration, and during conferences and roundtables, both in France and abroad, France Cyber Maritime is frequently asked for advice.

The topic of drones and autonomous ships, both civilian or military, is no longer just a "future" case study. The first designs, realizations, and operational uses are taking place today. Implementing these devices raises specific regulatory, human, technological, and organizational challenges that require an appropriate response. Highly digitized, these vehicles, whose autonomy is ensured by complex algorithms, are filled with sensors and actuators and rely on telecommunication and navigation systems to fulfill their missions. Given their current and future strategic use in our "blue economy" and for our security, they and the companies that design them are of genuine interest to state, criminal, or terrorist cyber attackers. In addition to the cyber threat to these vehicles, whose sovereign production is a real issue, the risk of failures related to their information systems cannot be overlooked. Maritime drones and autonomous ships will play an essential role in understanding, exploring, and mastering the oceans, which are strategic challenges for our future[1]. Therefore, their entire digital ecosystem must be protected against cyberattacks, from design to operation.

In this White Paper, we aim to provide the reader with a comprehensive overview of this topic and identify the main points of attention and regulatory, human, technological, and organisational recommendations for the cybersecurity design and operation of drones and autonomous ships. Our goal is to shed light, which we hope is objective and complete, on these challenges for the maritime and port world.

We hope to demonstrate that implementing suitable cybersecurity mechanisms for these types of vehicles is possible, provided this topic is addressed from the design phases. For this, the commitment of the State and the action of designers, equipment manufacturers, shipowners, operators, and sailors, companies, and personnel responsible for their maintenance, insurers, and classification societies are crucial.

As a stakeholder in the maritime and port world or in cybersecurity, and without necessarily becoming an expert, we hope that reading this White Paper will enable you to have an informed opinion to contribute effectively to the cybersecurity of maritime drones and autonomous ships.

FRÉDÉRIC MONCANY DE SAINT-AIGNAN
President of France Cyber Maritime

[1] The French Ministry of the Armed Focess established a strategy for mastering the seabed in February 2022 (in French) : https://www.defense.gouv.fr/sites/default/files/ministere-armees/20220211_GT%20MAITRISE%20FONDS%20MARINS_dossier%20de%20presse.pdf

CONTRIBUTORS

We would like to thank all individuals and organizations, both public and private, who contributed to the creation of this White Paper. Their expertise and experience on the subject have been particularly valuable in achieving a collaborative and high-quality work.

France Cyber Maritime would like to thank the following organizations, in alphabetical order:

- Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)
- Armateurs de France
- Bureau Veritas
- Cluster Maritime Français
- Direction Générale des Affaires Maritime, de la Pêche et de l'Aquaculture, (DGAMPA)
- École Nationale Supérieure Maritime (ENSM)
- Groupement des Industries de Construction et Activités Navales (GICAN)
- NAVAL GROUP
- Secrétariat Général de la Mer

Web illustrations by Storyset*

*https://storyset.com/web

TABLE OF CONTENT

FOREWORD 3

CONTRIBUTORS 4

INTRODUCTION 7

WHY SHOULD YOU READ THIS WHITE PAPER? 7
INFORMATION SYSTEM AND CYBER DOMAIN 9
CYBERSECURITY 9
CYBER RISK MANAGEMENT 10

MARITIMES DRONES AND AUTONOMOUS SHIPS: CHARACTERISTICS AND USE CASES 11

MARITIME DRONES 12
- Unmanned Aerial Vehicles evolving in a maritime context 12
- Unmanned Surface Vehicles (USVs) 14
- Unmanned Underwater Vehicles (UUVs) 14
- Operational context 16
- Constraints 16

AUTONOMOUS SHIPS 17
- Operational context 17
- Constraints 18

OVERALL AND FUNCTIONAL ARCHITECTURE OF AUTONOMOUS DRONES AND SHIPS 18

MARITIMES DRONES AND AUTONOMOUS VESSELS: VULNERABILITIES AND THREAT SCENARIOS 20

REGULATIONS AND APPLICABLE BEST PRACTICES 20
SECURITY NEEDS 23
RISK ANALYSIS 23
- Risk analysis scope 24
- Strategic scenarios 24

MARITIMES DRONES AND AUTONOMOUS SHIPS: CYBERSECURITY RECOMMANDATIONS 26
ORGANIZATIONAL RECOMMENDATIONS (R. ORG) 28
HUMAN RECOMMENDATIONS (R. HUM) 30
TECHNOLOGICAL RECOMMENDATIONS (R. TEC) 30
REGULATORY RECOMMENDATIONS (R. REG) 32

ANNEX 1 – DETAILS OF THE RISK ANALYSIS 34
MISSIONS, BUSINESS VALUES AND SUPPORTING ASSETS 34
STAKEHOLDERS 35
SOURCES OF RISK 36
FEARED EVENTS 36

ANNEX 2 - REDUCING RISKS ASSOCIATED WITH STRATEGIC SCENARIOS 38

ANNEX 3 – COMPLIANCE WITH THE REQUIREMENTS OF THE EUROPEAN NIS DIRECTIVE 39

GLOSSARY 41

INTRODUCTION

Why should you read this White Paper?

Like all industrial sectors, the maritime sector has undergone significant digital transformation since the 2000s. Moving from predominantly analog and mechanical systems, both on the bridge and in the engine room of ships, critical onboard installations now heavily rely on digital technologies. This includes communication with the shore, vessel navigation, situational awareness and weather information, as well as the execution of missions. This holds true for both civilian and military vessels. Today, it's inconceivable to set sail without information systems, industrial control systems, or telecommunication systems.

In parallel, more recently, maritime drones and autonomous vessels are gradually becoming a reality. Their purposes are diverse: enhancing the endurance of sea presence, undertaking tasks that are unappealing or hazardous for humans or shipowners, thus improving sailor safety, addressing personnel shortages, performing surveillance or transportation missions, and more.

Digitization and automation reduce the need for tasks that were once repetitive or dangerous for humans, making them a vector for enhancing the safety, security, and productivity of our maritime world. This transition also brings speed, flexibility, and security benefits to the entire maritime and port sector. In a highly competitive industry, tight logistics flows requires more efficiency. Digital technology becomes a differentiating factor for shipowners or ports in some cases and can also lead to cost reductions.

However, digital technology does not come without weaknesses: the use of insecure protocols, obsolete software and hardware, or systems designed without considering cybersecurity, difficulties in patch management processes, and the implementation of unsecured architectures are regularly exploited by state actors, criminals, or activists to carry out cyberattacks.

Cyberattacks, with diverse objectives (espionage, ransom demands, sabotage, etc.) and far-reaching consequences (damage to reputation, financial loss, cyber-physical impact, etc.), have been severely affecting the sector for several years.[2] The well-oiled machinery of the sector can suddenly grind to a halt, sometimes with significant short-term operational impacts.

It is based on this observation and applying it specifically to maritime drones and autonomous vessels that we wanted to address topics that we consider essential to understand their operation, strengths and weaknesses, associated risks, and means of protection. While the cyber risks related to maritime drones and autonomous vessels are generally common with other systems of the same type, the responses provided by the sector will be unique to each, as they will depend closely on the organization's strategy, its perception of cyber risks, the context of equipment use, and its budget.

This work was carried out by France Cyber Maritime during a working group organized within the framework of the French Cyber Council for the Maritime World (Conseil Cyber du Monde Maritime, C2M2), led by the French General Secretariat of the Sea.

[2] The « ADMIRAL » dataset of disclosed maritime cybersecurity incidents, maintained by the M-CERT operated by France Cyber Maritime can be browsed for awareness and reseach purposes: https://www.m-cert/admiral

This White Paper is divided into three main sections:

Firstly, we will provide an overview of the physical, technical, and design characteristics of drones and autonomous vessels, as well as their operational contexts, to ease the use of common vocabulary and concepts.

Next, we will explore vulnerabilities and potential threat scenarios for this type of equipment. Finally, we will offer specific cybersecurity recommendations to enhance their cybersecurity, from design to retirement from service.

Of course, a complex and technological subject like the cybersecurity of maritime drones and autonomous vessels cannot be comprehensively covered in a few pages, and the support of a high-quality cyber ecosystem, such as that represented within our association, France Cyber Maritime, will be essential for shipowners, ports, equipment manufacturers, and integrators.

We hope that this White Paper will provide you with initial insights, stimulate further developments, and contribute to strengthening the cybersecurity of maritime drones and autonomous vessels.

Web illustrations by Storyset*

*https://storyset.com/web

Information system and cyber domain

The term 'information system' is subject to numerous definitions and interpretations depending on countries, individuals, and organizations. In general terms, it can be defined as a 'manual or automated system, such as an automatic data processing system, a computer system, or a computer network, relying on technical infrastructure and composed of people, machines, and methods organized to perform functions of data collection, processing, transmission, and dissemination, representing information.[3]

By extension, the cyber domain, a new 'full-fledged field of confrontation,' according to NATO, encompasses 'the information itself, the individuals, organizations, and systems that receive, process, and transmit it, and the cognitive, virtual, and physical space in which this occurs.[4]

The cyber domain is thus interdependent with the domains of air, land, sea, and space, although it is cross-cutting as it can be found within each of them.

Cybersecurity

According to a commonly accepted definition, 'cybersecurity is a desired state for an information system, enabling it to withstand events originating from the cyber domain that may compromise the availability, integrity, or confidentiality of the data stored, processed, or transmitted, as well as the related services that these systems provide or make accessible.' [5]

One will also often hear about:

- **cyberprotection** (or information systems security), as a desired state for information systems to be safe and high-performing in terms of availability, integrity, and confidentiality from their design phase throughout their lifecycle;
- **cyberdefense**, which encompasses 'technical and non-technical measures allowing a state to defend essential information systems in the cyber domain.' [5];
- **cyber resilience**, representing the 'ability of an information system to withstand a failure and return to its initial state after an incident.' [5],

the word 'cybersecurity' encompassing all of these aspects.

The following security properties will also be discussed, the pursuit of which ensures cybersecurity and reduces risks:

- **availability**, which ensures continuous and resilient access to information system resources;
- **integrity**, which guarantees the absence of unauthorized or unintentional modification of the information system;
- **confidentiality**, which ensures that information is only accessible and disclosed to individuals, organizations, or processes authorized to have knowledge of it;

[3] Olivier Jacq. Real-time detection, contextual analysis and visualisation of cyberattacks: elaboration of the Maritime Cyber Situational Awareness. Cryptographie et sécurité [cs.CR]. École nationale supérieure Mines-Télécom Atlantique, 2021. English. NNT : 2021IMTA0228. tel-03145173 (https://theses.hal.science/tel-03145173v1/file/2021IMTA0228_Jacq-Olivier_Annexe.pdf)

[4] *North Atlantic Military Commitee*. Mc 0422/4 *NATO military policy on information operations*, July 2012.

[5] CICDE. Glossaire interarmées de terminologie opérationnelle (GIATO)

- **traceability**, which ensures that any manual or automatic action on an information system is subject to appropriate continuous monitoring;
- **non-repudiation**, which guarantees that the author of any manual or automatic action cannot later deny having taken that action.

Finally, it should be noted that, while cybersecurity often focuses on external and intentional attacks, internal threats (both unintentional and malicious) on one hand, and accidental risks (such as failures, malfunctions, errors) on the other, should never be underestimated.

Cyber risk management

The attack surface, the complexity of certain systems, and the inability to address certain specific or systemic vulnerabilities often make it impossible to secure a system entirely. Therefore, cyber risk management aims to identify the risks that need to be taken into account for the system and to ensure their optimal and rational mitigation in order to reduce the occurrence of the scenario to an acceptable threshold..

Two approaches are essential to this cyber risk management:

- Risk treatment through compliance, in order to meet general, sector-specific, normative, legal, or regulatory constraints, as well as those related to an existing cybersecurity policy or status of the organization;
- Risk treatment after the analysis and formalization of strategic and operational risk scenarios for the considered system, taking into account its characteristics and usage context, with the aim of achieving the most rational analysis possible.

Cyber risk assessment and mitigation are truly effective and more cost-efficient when conducted during the design phase of the system in question. Risk treatment downstream, often more time-consuming and complex to implement, generally does not allow for a consistent, relevant, and 'in-depth' treatment of risks. During the design phase, and depending on the considered risks and the digital scope, it is widely recognized that the implementation of cybersecurity measures represents a necessary investment of approximately 5 to 10% of the total project cost. This investment can transform into an additional cost of around 10 to 15% of the project if it has not been carried out upstream.

The risk analysis method currently recommended by the French National Cybersecurity Agency (Agence Nationale de la Sécurité des Systèmes d'Information, ANSSI) is EBIOS Risk Manager[6].

[6] https://cyber.gouv.fr/en/publications/ebios-risk-manager-method

MARITIMES DRONES AND AUTONOMOUS SHIPS: CHARACTERISTICS AND USE CASES

The International Maritime Organization (IMO) is working on a project to develop a code linked to the Safety Of Life At Sea (SOLAS) convention[7], aiming to clarify the applicability of international conventions to autonomous ships.

Maritime drones are not covered by these international efforts, as the distinction between drones and autonomous ships is specific to the framework currently established in France. Indeed, France has created a specific regime for the experimental operation of these devices, established by the decree of May 20, 2020, relating to the conditions of experimentation of navigation for autonomous or remotely operated maritime floating devices[8]. The new regime, applicable during the experimental phases, introduced by Ordinance No. 2021-1330 of October 13, 2021, relating to the navigation conditions of maritime ships and drones[9], will only come into effect once the implementing texts are published (decree amending decree 84-810 and technical operation orders). This ordinance defines the terminology of maritime drones and autonomous ships:

- A maritime drone is a floating surface or underwater device operated remotely or by its own operating systems, without personnel, passengers, or cargo on board, and whose technical characteristics, including size, power, and speed limits, are defined by regulation, without its gross tonnage being equal to or greater than 100 Universal Measurement System (UMS) units;
- An autonomous ship is a ship operated remotely or by its own operating systems, with or without crew members on board.

However, the concept of a maritime drone is not solely based on the physical characteristics of the device but also on the specific conditions of its operation (see, in particular, Article L.5000-2-2 of the Transport Code)[10].

[7] https://www.imo.org/fr/about/Conventions/Pages/International-Convention-for-the-Safety-of-Life-at-Sea-(SOLAS),-1974.aspx
[8] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000041938890
[9] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000044202140
[10] https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000044202953

Maritime drones

Maritime drones typically take on a specific designation based on the environment in which they operate[11]:

- *Unmanned Aerial Vehicles* (UAVs) ;
- *Unmanned Surface Vehicles* (USVs);
- *Unmanned Underwater Vehicles* (UUVs).

It is worth noting that some drones can change their operating environment depending on their missions (e.g., UAV to USV, USV to UUV), carry other types of drones (e.g., USV carrying UUV or USV), or be carried by autonomous ships.

Furthermore, maritime drones can operate individually or as part of a fleet of multiple vehicles, coordinated by a mothership drone or synchronized with each other.

Figure 1: Example of a USV carrying a UUV. Source: Thales

• Unmanned Aerial Vehicles evolving in a maritime context

Unmanned Aerial Vehicles (UAVs) operating in a maritime environment carry out various missions, including maritime surveillance, search and rescue at sea, coastal mapping, fisheries monitoring, and marine pollution surveillance.

They are not considered maritime drones and fall under the regulations developed by the French General Directorate of Civil Aviation (Direction Générale de l'Aviation Civile, DGAC) to govern the use of aerial drones in France. They can be remotely piloted from a ground control center or a carrier vessel, or programmed to fly autonomously along a specific route.

[11] GICAN « Drones and Autonomous Maritime Systems 2022 » brochure : https://gican.asso.fr/wp-content/uploads/2023/06/2022.10-GICAN-BROCHURE-MARITIME-DRONES-AUTONOMOUS-SOLUTIONS.pdf

These drones can be categorized depending on their size:

- *Very Small UAVs: Micro or Nano UAVs*
- *Small UAVs: Mini UAVs*
- *Medium UAVs*
- *Large UAVs*

Or their endurance, which is their ability to operate at a distance from their base:

- *Very close range UAVs*
- *Close-range UAVs*
- *Short-range UAVs*
- *Mid-range UAVs*
- *Endurance UAVs*

The terms MALE (Medium Altitude, Long Endurance) or HALE (High Altitude, Long Endurance) can also be found in the literature.

Category	***Size***	***Maximum Gross Takeoff Weight*** (MGTW) (lbs)	***Normal Operating Altitude*** (ft)	***Airspeed*** (knots)
Group 1	Small	0-20	<1,200 AGL*	<100
Group 2	Medium	21-55	<3,500	<250
Group 3	Large	<1320	<18,000 MSL**	<250
Group 4	Larger	>1320	<18,000 MSL	Any airspeed
Group 5	Largest	>1320	>18,000 MSL	Any airspeed

Table 1: Classification of UAVs, from the US Department of Defense. Source: psu.edu[12]

[12] https://www.e-education.psu.edu/geog892/node/5

• Unmanned Surface Vehicles (USVs)

Unmanned Surface Vehicles are designed to operate on water and be remotely piloted for various applications. These drones can be used for a variety of tasks, such as maritime surveillance, collecting oceanographic data, conducting search and rescue operations (detection and locating, support for rescuers), seabed mapping, marine environmental protection, pollution control, or naval combat actions.

Surface maritime drones are often equipped with sensors to collect data about the underwater environment, such as temperature, salinity, depth, and water turbidity sensors, as well as cameras to capture photos and videos of the water surface and marine life.

They can be remotely controlled from a carrier vessel, a Shore Control Center (SCC), or another drone, and can be programmed to carry out specific missions autonomously.

USVs also provide an efficient and cost-effective means to monitor and collect data in remote and hard-to-access maritime areas.

• Unmanned Underwater Vehicles (UUVs)

Unmanned Underwater Vehicles (USVs) are designed to move beneath the water and perform various tasks such as oceanographic research, seabed mapping, inspection of underwater structures, or marine environmental monitoring. Equipped with sonars, cameras, depth sensors, and effectors (e.g., robotic arms), they provide an efficient and cost-effective means to operate in remote and hard-to-access underwater areas.

It's worth noting that remotely operated underwater drones connected by a tether (Remotely Operated Vehicles, ROVs) are considered extensions of their carrier vessels and fall under the regulations applicable to robotics.

Figure 2: Example of a USV: Exail's DriX.[13]

[13] https://www.exail.com/

Underwater drones can be classified based on their mode of propulsion and their operating depth (ranging from a few meters to thousands of meters deep):

Surface vehicles: drones designed to operate on the water's surface.	
Free-diving vehicles: drones that use the free-diving technique to move, meaning they dive or surface by using their buoyancy systems and altering their density. However, they do not have a motor or propeller and cannot move laterally underwater. These drones are suitable for autonomous exploration missions at relatively shallow depths.	
Swimming vehicles: drones that use motors and propellers to move underwater. They are capable of moving in all directions. These drones are suitable for operations that require rapid and precise movement underwater.	**Gliders**: drones that use wings to perform horizontal glides and density variations to dive and surface. These drones are suitable for long-duration explorations.[14].
Bottom crawlers: drones equipped with wheels or tracks that move on underwater surfaces (seafloor or pipeline walls).	

Table 2: Classification of UUVs.

Figure 3: Bottom crawler example : the work class ROV HECTOR 7, operated by Orange Marine. Source: L. MIQUEL, Armateurs de France.[15]

[14] The current work related to the implementing decree excludes gliders from the category of maritime drones.
[15] https://www.armateursdefrance.org/actualite/chapitre-2-journal-linfirmiere-bord-du-pierre-fermat-sonia-meriaux-avril-mai-2020

• Operational context

The operational context for maritime and naval drones is particularly diverse:

- Naval context: mine countermeasures, surface, aerial, or underwater patrol, intelligence, state action at sea, search and rescue at sea, offensive actions, seabed control and surveillance.
- Environmental context: environmental parameter measurements, pollution control, marine environmental pollution measurements, maritime surveillance, and combatting illegal fishing.
- Scientific context: hydrographic and oceanographic measurements, archaeological research, biodiversity monitoring.
- Underwater diving: the use of drones extends the temporal and spatial autonomy of dives and avoids risks for humans.
- Construction and maintenance: surveys, work (Marine Renewable Energy (MRE), offshore), laying and maintenance of underwater cables (telecommunications, energy), inspection and maintenance of ship hulls and port facilities, site or area surveillance..

• Constraints

Due to their operational context, drones are subject to particularly significant physical and environmental needs and constraints in their design and use:

- Precise 2D/3D positioning, especially underwater and in degraded environments.
- Collision prevention (with other users at sea, the seafloor, obstacles, the carrier vessel, or other drones).
- Precise maneuvering in an environment where physical constraints are significant and variable (current, temperature, wind, waves).
- Detection of the aerial, surface, and underwater environment at short, medium, and long ranges depending on the cases and propagation conditions.
- Secure collection and onboard storage of data or elements captured during the mission.
- High-speed secure telecommunications by radiofrequency, satellite, or acoustic signal with the carrier vessel, shore, or other vehicles, to ensure remote control, bilateral transmission of mission-related information, in quasi-real-time or deferred, maintenance operations, etc., with particular difficulty in underwater operations.
- Autonomy and control of energy expenses.
- Survivability on board in the event of onboard crew (for Level 1 and Level 2 autonomous ships).
- Operation under strong environmental physical constraints: pressure, corrosion.
- Resilience in the event of a breakdown.

Autonomous or semi-autonomous maritime vehicles are already used in operational maritime or naval contexts.

Autonomous ships

The IMO has proposed a categorization of autonomous ships, Maritime Autonomous Surface Ships (MASS), based on their degree of autonomy[16]. These four degrees of autonomy proposed by the IMO are the result of a regulatory scoping exercise conducted in 2021.

Degree	Description
1	Seafarers are on board to operate and control shipboard systems and functions. Some operations may be automated and at times be unsupervised but with seafarers on board ready to take control.
2	The ship is controlled and operated from another location. Seafarers are available on board to take control and to operate the shipboard systems and functions.
3	The ship is controlled and operated from another location. There are no seafarers on board.
4	Fully autonomous ship: the operating system of the ship is able to make decisions and determine actions by itself.

Table 3: Grouping of autonomous ships according to their degree of autonomy. Source: IMO.

The degrees of autonomy are not intended to play a structuring role in the MASS Code project, mainly because the operating conditions of autonomous ships can vary, leading a vehicle to operate at multiple levels of autonomy. Thus, during the MSC.107 committee meeting in June 2023, it was proposed to replace the concept of 'degree of autonomy' with that of 'operational mode,' which appears to be more consistent with the reality of autonomous ship use.[17]

• Operational context

The employment contexts for autonomous ships are also particularly diverse:

- Freight transportation: containers or bulk (solid or liquid), currently primarily in coastal, port, or river contexts;
- Passenger and vehicle transportation, currently over short distances;
- Port operations: tugboats, pusher boats;
- Naval operations: combat ships.

Taking the example of the SOLAS Convention[18] or the Convention on the International Regulations for Preventing Collisions at Sea (COLREG)[19], it appears difficult, if not impossible in the current state, to operate an autonomous ship for international navigation.

[16] http://www.imo.org/en/MediaCentre/HotTopics/Pages/Autonomous-shipping.aspx: it should be noted that this definition is expected to be revised in the summer of 2023.
[17] https://www.imo.org/en/MediaCentre/MeetingSummaries/Pages/MSC-107th-session.aspx
[18] https://www.imo.org/en/About/Conventions/Pages/International-Convention-for-the-Safety-of-Life-at-Sea-(SOLAS),-1974.aspx
[19] https://www.imo.org/en/about/Conventions/Pages/COLREG.aspx

Indeed, Chapter V of the SOLAS Convention requires that every ship has sufficient crew on board to ensure her own safety or to assist a vessel in distress; autonomous ships of degrees 3 and 4 will not be able to comply with this requirement. Similarly, with regard to COLREG, its Rule 5 states that "every vessel shall at all times maintain a proper look-out by sight and hearing as well as by all available means appropriate in the prevailing circumstances and conditions so as to make a full appraisal of the situation and of the risk of collision".

Autonomous ships are still largely in the experimental phase: although no major technological barriers remain, as demonstrated by various experiments and implementations (such as Yara Birkeland[20], ROSS[21], SVAN[22]), regulatory, economic, and even social constraints can weigh on a more systematic operation.

• Constraints

The constraints associated with autonomous ships are diverse:

- Precise 2D/3D positioning, especially in degraded environments;
- Collision prevention (with the seabed, obstacles, other ships, autonomous or not);
- Precise navigation in an environment with significant and variable physical constraints (currents, temperature, wind, waves, etc.);
- Detection of the environnement on the surface at short, medium and long ranges;
- Secure collection and storage of mission data on board;
- High-speed secure communication with the land or other drones, for remote control, two-way transmission of mission-related information in quasi-real time or delayed, maintenance operations, etc.;
- Autonomy and control of energy expenses;
- On-board survivability in case of personnel embarkation;
- Resilience in case of breakdown.

Overall and functional architecture of autonomous drones and ships

The overall architecture of autonomous maritime drones and ships can be generically divided into several modules:

- Ground stations (possibly onboard), which may be responsible for controlling the equipment (ROV, MASS degrees 2 or 3) or preparing and monitoring their mission;
- Télécommunication systems (satellite or radio) for communication with the carrier vessel or the shore control station;
- Sensor sets (positioning, RADAR, LIDAR, caméras, laser, sonars, etc.);
- Actuator sets (propulsion, navigation, flotation, energy management, etc.);
- The digital system to manage the entire setup.

[20] https://www.yara.com/news-and-media/press-kits/yara-birkeland-press-kit/
[21] https://seaowlgroup.com/wp-content/uploads/2020/09/poc-ross.pdf
[22] https://breakingwaves.fi/wp-content/uploads/2019/06/SVAN-presentation.pdf

More specifically, depending on its level of autonomy and the type of mission:

- The maritime drone or autonomous ship is assigned a mission that it carries out either by following a predefined route or by navigating partially or entirely autonomously;
- To navigate, it obtains geographical references from Position, Navigation and Time (PNT) sensors and also adjusts its navigation attitude based on environmental parameters such as available power and sea conditions, as well as surface situation (e.g., the presence of other vessels);
- It takes action to adjust its navigation using its actuators (propulsion, steering), adapting their effectiveness according to environmental conditions;
- In parallel, it performs any specific missions that are not directly related to the carrier's behavior;
- The coordination and execution of the mission are generally managed by one or more redundant and specific coordinating computers (e.g., one computer for the carrier and one for the mission).

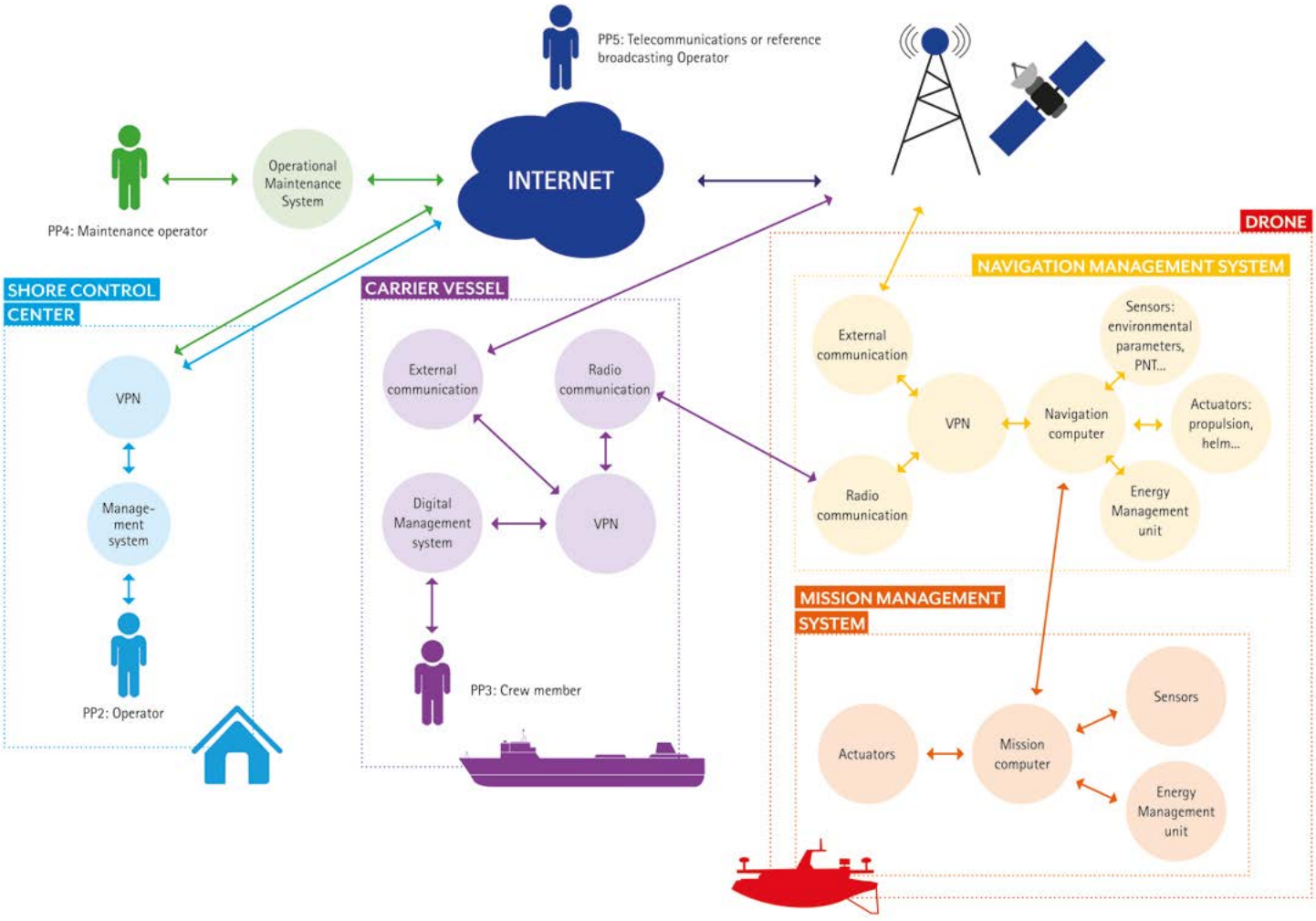

Figure 4: Overall and functional architecture of maritime drones and autonomous vessels.

MARITIMES DRONES AND AUTONOMOUS VESSELS: VULNERABILITIES AND THREAT SCENARIOS

Regulations and applicable best practices

Before discussing vulnerabilities and threat scenarios, it is important to mention the regulations that could apply to maritime drones and autonomous ships in termes of cybersecurity.

At the international level, the objectives of the International Safety Management Code (ISM)[23] aim to define operating practices for working in a safe environment, assess all identified risks to ships, their personnel and the environment, establish appropriate precautionary measures, and continuously improve the skills of shore-based and onboard personnel. In addition to this, the IMO Resolution MSC.428(98)[24] on Maritime Cyber Risk Management in Safety Management Systems was adopted in 2017.

This code could apply to autonomous vessels depending on their size and operational context. However, the absence of personnel on board highly autonomous ships would require adaptation of the practical application of the resolution. The future IMO MASS Code (Maritime Autonomous Surface Ship), expected to be promulgated in 2025 and becoming binding by 2028 or at the latest by 2029, could include specific and adapted cybersecurity measures for autonomous ships.

At the European and French levels, the Military Programming Law (Loi de Programmation Militaire, LPM) and the status of Operator of Vital Importance (Opérateur d'Importance Vitale, OIV) operating Vital Information Systems (Système d'Information d'Importance Vitale, SIIV) could apply to shipowners and operators implementing maritime drone and autonomous vessel systems, depending on the specific application and declaration criteria of the Military Programming Law according to the relevant sector. [25]

The European Parliament and the Council of the European Union adopted the directive on measures to ensure a high common level of cybersecurity across the Union in July 2016, also known as the Network and Information Security (NIS) Directive. [26] Transposed into French law in 2018, this directive aimed to increase the level of cybersecurity for major players in ten sectors, including maritime transport. With this initial framework, large players in these sectors, recognized as Operators of Essential Services (OES), were required to report their security incidents to ANSSI, implement necessary preventive security measures to significantly reduce the exposure of their most critical systems to cyber risks, and be capable of responding adequately in the event of an incident).

[23] https://www.imo.org/en/OurWork/HumanElement/Pages/SafetyManagement-Default.aspx
[24] Resolution MSC.428(98), adopted on June, 16th, 2017, Maritime Cyber Risk Management in Safety Management Systems: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf
[25] See https://cyber.gouv.fr/en/french-ciip-framework
[26] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148

In 2022, the NIS 2 was adopted[27] by the European Parliament and Council, expanding the objectives and scope of applicability to provide increased protection compared to the first version of the directive.

The second version of this Directive could enable new actors of the maritime sector to be included, particularly operators or designers of maritime drones and autonomous vessels, as well as, more explicitly for its transposition into French law, teleoperation centers. None of the versions of the Directive, however, include ships, as they are explicitly excluded. Therefore, this Directive would also not be applicable to maritime drones and autonomous vessels for the status of Essential Entity (EE), except for shore control centers.[28]

The French Directorate-General for Maritime Affairs, Fisheries, and Aquaculture (Direction Générale des Affaires Maritimes, de la Pêche et de l'Aquaculture, DGAMPA) is developing implementing texts for Ordinance No. 2021-1330, including the draft decree amending Decree No. 84-810 of August 30, 1983, on the regime applicable to autonomous vessels and maritime drones.[29] This decree will be supplemented by technical orders specifying provisions related to cybersecurity, particularly concerning security equipment.

At the French sectoral level, the French Maritime Cluster issued a "Guide to Best Practices for Maritime Drones" in June 2020, which addresses the topic of cybersecurity.[30] This guide makes the following recommendations, notably based on the cybersecurity framework proposed by the American National Institute of Standards and Technology (NIST)[31]:

13.7.1	The protection of information systems involved in the safety functions of a maritime drone must be ensured as much as possible in order to preserve the confidentiality, integrity, and availability of information. In particular, it is recommended to conduct a risk analysis concerning data modification (either by mistake by an authorized person or maliciously by an unauthorized person), their misuse, or the unintentional denial of their accessibility.
13.7.2	Even if the provisions of the NIS Directive do not apply to vessels, manufacturers, operators and/or managers must conduct audits and implement the necessary corrective measures to ensure safe operation. Particularly, based on the risk assessment, cyber, it involves: Identifying: specifying the roles of personnel and responsibilities for the management of information systems and identifying the risks that weigh on the different elements of the systems and can compromise safety or operations; for example, the risk that a third party mistakenly accesses the drone's industriel control system; • Protecting: implementing protection and contingency measures between the identified risks and enabling the continuity of operations; for example, having passwords for controlled access to the system; • Detecting: developing and implementing means to detect a cyber event in a timely manner; for example, identifying a new connection to the information system; • Responding: implementing measures to react to the event and maintain the essential functions of the systems; for example, blocking access; • Recovering: implementing backup and system restoration measures; for example, having a reference version of the software that can be reinstalled.

Table 4: Cybersecurity recommendations for maritime drones. Source: Cluster Maritime Français.

[27] See https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555&qid=1689168337809
[28] See https://cyber.gouv.fr/en/actualites/revision-nis-directive-opportunity-strengthen-cybersecurity-level-eu
[29] https://www.mer.gouv.fr/sites/default/files/2022-10/PV%20CCS%20971%20INF.03%20-%20D%C3%A9cret%2084-810%20navires%20autonomes.pdf
[30] https://www.cluster-maritime.fr/wp-content/uploads/2022/09/CMF_guide_drones_juin2020.pdf
[31] https://www.nist.gov/cyberframework

Classification societies have issued several guides and recommendations for autonomous vessels. One notable example is:

- BUREAU VERITAS's NI 641 DT R01 E note, "Guidelines for autonomous shipping". This note references cybersecurity and provides for the application of NR659 requirements for the additional class notation, CYBER SECURE, for units covered by this note.[32]

2.11 Cybersecurity

2.11.1 The usage of information and communication technologies makes possible virtual unauthorized or malicious actions to ships (e.g. virus infection). Data communication between ship and control centre or GPS signal could be intentionally disturbed or changed in order to hijack the ship or cause severe damages.

2.11.2 Amongst the best practices for the usage of information and communication technologies, measures should be adopted to provide the highest level of confidence for data (e.g. protection, encryption) and for user access (e.g. password authentication).

2.11.3 For cybersecurity reference is made to Sec 4, [7].

7 Cyber security

7.1 References

7.1.1 The computer based systems and networks should be compliant with the applicable requirements related to the assignment of the additional class notation **CYBER SECURE** from Society Rule Note NR659, Cyber Security for the Classification of Marine Units.

7.1.2 The applicable requirements related to the assignment of these additional class notation may be adjusted to the satisfaction of the Society according to the results of the risk and technology assessment, the degree of automation, the degree of direct control and remote control, the navigation notation, the operational limitations, the possibility of external rescue, etc.

Figure 5: Recommendations from note NI 641 DR R01E. Source: BUREAU VERITAS.

- Note NR 659 DT R02 from BUREAU VERITAS, dated January 2023[33], although it does not directly reference maritime drones or autonomous vessels, il largely applicable and adapted to address the specific challenges and constraints of these devices.
- The International Association of Classificaiton Societies (IACS) UR E26 and E27[34], set to enter into service on January 1st, 2024, for new constructions.

In December 2017, Lloyd's Register issued a document « *Cyber-enabled ships: ShipRight procedure assignment for cyber descriptive notes for autonomous & remote access ships* »[35].

Furthermore, numerous research articles, both in France and abroad, discuss the topic of cybersecurity for maritime drones and autonomous vessels, covering aspects of risk analysis and potential technical solutions. Notable examples include research conducted by the French Maritime Acadamy (École nationale supérieure maritime, ENSM) as part of the Sea4M research project[36], and a research article[37] from the NATO erative Cyber Defence Centre of Excellence, (CCDCOE).

[32] https://erules.veristar.com/dy/data/bv/pdf/641-NI_2019-10.pdf
[33] https://erules.veristar.com/dy/data/bv/pdf/659-NR_2023-01.pdf
[34] https://iacs.org.uk/resolutions/unified-requirements/ur-e/ur-e26-new and https://iacs.org.uk/resolutions/unified-requirements/ur-e/ur-e27-new
[35] https://fr.scribd.com/document/449320742/MO-Cyber-Enabled-Ships-ShipRight-Procedure-V2-0-201712
[36] https://www.supmaritime.fr/en/sea4m/
[37] https://ccdcoe.org/uploads/2022/09/Cybersecurity_Considerations_in_Autonomous_Ships.pdf

Security needs

Maritime drones and autonomous ships combine the security needs of more traditional vessels[38], often implementing many of their protocols and various equipement (sensors, actuators, communication systems, PNT systems, etc.).

In addition to these, there are new requirements related to the specific characteristics of autonomous equipment, including:

- increased dependence on communication systems, especially satellite-based, where availability, integrity and confidentiality often become critical, especially when autonomy levels are low or when the mission requires frequent communication with the shore;
- the importance of trust in electronic, visual and auditory sensors, which must be highly reliable and available;
- a heavy reliance on algorithms in decision-making and, more broadly, in the operation of the vessel and its systems.

It's also worth noting the physical risks. While historically, hijacking a manned vessel has been a major concern and remains so in certain navigational zones, it can be a hazardous and dangerous endeavor. The risk of capturing a maritime drone or autonomous vessel also poses security concerns regarding the confidentiality of information systems (reverse engineering, vulnerability assessment, sensitive data capture, compromise of uplink connections, etc.). In addition to the safety of maritime drones, autonomous vessels, and Shore Control Centers, their security is a significant concern.

Risk analysis

First, it's interesting to note that the maritime and naval sector is not the only one concerned with the cybersecurity of autonomous vehicles. There are interesting parallels and potential collaborative studies and projects that could be undertaken with sectors like road transportation or aviation, even though the maritime context and its unique constraints need to be considered.

The objective of this paragraph is not to conduct an exhaustive risk analysis for drones and autonomous vessels but to present the key principles to follow when conducting such an analysis, as well as the main high-level attack scenarios to consider, known as strategic scenarios.

While cyber risk management should be part of broader risk management efforts, such as those related to registration, established cybersecurity methodologies should be applied.

A few important points should be noted before conducting a cybersecurity risk analysis on these systems:

1. Maritime drones and autonomous vessels can be inherently autonomous by design. They can also be existing vessels to which an autonomy component is added, either for experimentation or production purposes, although this scenario seems less likely. Autonomous vessels "gain" in efficiency and profitability when systems, accommodations, and onboard infrastructure are eliminated, leading to significant benefits, particularly in terms of weight and energy consumption.

[38] Vulnerabilities of more traditional vessels were identified in the following guidelines published by BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and WORLD SHIPPING COUNCIL on cybersecurity onboard ships: https://www.bimco.org/-/media/bimco/about-us-and-our-members/publications/ebooks/guidelines-on-cyber-security-onboard-ships-v4.ashx

2. The cyber treatment to be undertaken in both cases differs significantly. In the first case, cybersecurity needs to be integrated by design, while in the second case, existing onboard systems, potentially old and not very secure, need to be interconnected with autonomous control and navigation systems. In this scenario, risk analysis is particularly crucial because the extension of these systems or their accessibility from the shore poses a significant risk.

• Risk analysis scope

It is essential that the risk analysis conducted encompasses not only the navigation system itself but also the Shore Control Center(s) (SCC), the carrier vessels - or those from which the drones are operated - as well as satellite communication links, for example. Likewise, maintenance operations pose a significant risk of compromise for this type of equipment: people, processes, and associated tools should receive special attention to reduce the risk of attacks related to the supply chain, also known as Supply Chain Attacks. **Therefore, the complete ecosystem of maritime drones/autonomous vessels must be taken into account.**

The business and technical scope of the risk analysis is detailed in Annex 1, through the definition of the missions of drones and autonomous vessels, their business values (i.e., important information and processes to protect), associated support assets (technical elements on which business values rely), and feared events.

• Strategic scenarios

The following strategic scenarios (SS) could be selected based on the risk analysis conducted:

- **SS1 – A cybercriminal threat actor conducts a ransomware attack on the ground control center's management system.**

  This scenario involves a ransomware attack on the shore control center's management system, leading to a loss of communication with the maritime drone or autonomous ship and a mission interruption in order to extort a ransom. This scenario corresponds to the feared events ER7 and ER11 (see Annex 1). To achieve their goal, the cybercriminal group may use several attack paths:

  - Direct attack on the management system, by exploiting a software vulnerability accessible from the internet or by connecting with legitimate credentials to a remote access service (e.g., Virtual Private Network);

  - Spear-phishing email attack targeting an operational operator and the retrieval of legitimate credentials.

- **SS2 – A state or pseudo-state actor sabotages the maritime drone or autonomous ship during a mission.**

  This scenario corresponds to the sabotage by a state or pseudo-state group of the management systems of a maritime drone or autonomous ship (navigation and mission) in order to disrupt or even prevent the mission carried out by the maritime drone or autonomous ship. This scenario corresponds to the feared events ER8, ER9, ER10, ER11, ER12, and ER13 (see Annex 1). To achieve its goal, the actor might employ several attack vectors:

  - Disruption through deception, jamming of information received by the drone's or autonomous ship's sensors (GNSS, AIS, RADAR, satellite links, etc.), or logical or physical destruction of associated equipment.

  - Direct attack on the management systems of the maritime drone or autonomous ship by exploiting a vulnerability accessible from the internet or by connecting with legitimate credentials to a remote access service (operations, maintenance, etc.).

- **SS3 – A state actor pre-positions themselves on the maritime drone or autonomous ship during the maintenance phase**

  This scenario corresponds to the pre-positioning of a state actor on the management systems of a maritime drone or autonomous ship (navigation and mission) during maintenance phases, with the aim of compromising the maritime drone or autonomous ship and its mission or conducting economic and strategic espionage (stealing data captured during the mission or data related to the architecture or programming of the maritime drone or autonomous ship). This scenario corresponds to the feared events ER1, ER3, ER4, ER6, ER7, ER8, ER9, ER10, ER11, ER12, and ER13 (see Annex 1). To achieve its goal, the state actor might use several attack vectors:

  - Attacking the IT systems of the external maintainer or the IT systems of the shore control center (if maintenance is done internally) by exploiting a vulnerability present on an Internet-exposed device or by connecting with legitimate login credentials to a remote access service, before bouncing towards the management systems of the maritime drone or autonomous ship.

  - Spearphishing email attack on a maintenance operator (internal or external).

  - Attacking the supply chain to compromise updates and then bouncing towards the management systems of the maritime drone or autonomous ship.

- **SS4 – Terrorist – Sabotage of the maritime drone or autonomous ship during the design phase**

  This scenario corresponds to the sabotage by a competitor or a third party acting on behalf of a competitor of the calculation and decision-making algorithms of the maritime drone or autonomous ship during the design phase, with the aim of creating a serious incident during its commissioning in order to discredit it. This scenario corresponds to the feared events ER3, ER7, ER8, and ER10 (see Annex 1). To achieve its goal, the competitor could use several attack paths:

  - Direct attack on the designer's IT system accessible via the Internet by exploiting a vulnerability accessible from the Internet or by connecting with legitimate login information for a remote access service.

  - Spear-phishing email attack targeting an employee of the designer.

  - Attack exploiting the trust relationship with a subcontractor to gain access to the designer's IT system.

- **SS5 – State Actor – Theft of plans or data related to a maritime drone or autonomous ship project**

  This scenario corresponds to the theft by a state actor of plans or data related to a maritime drone or autonomous ship project for the purpose of strategic and economic espionage. This scenario corresponds to the feared events ER2 and ER5 (cf. Annex 1). To achieve its goal, the state actor may use several attack vectors:

  - Direct attack on the supply chain's information systems (designers, equipment suppliers, integrators) by exploiting a vulnerability accessible via the Internet or by using legitimate credentials to access a remote service.

  - Spear-phishing email attack targeting an employee in the supply chain.

MARITIMES DRONES AND AUTONOMOUS SHIPS: CYBERSECURITY RECOMMANDATIONS

In cybersecurity, a single measure is often bypassable and therefore insufficient to address a cyber attack. It is therefore necessary to follow a defense-in-depth approach by implementing complementary and coherent measures, including regulatory, organizational, human, and technological aspects.[39]

As previously mentioned, these measures are most effective when planned and defined during the design phase of maritime drones or autonomous ships. Their implementation may sometimes take time or represent a financial investment for the organization implementing them. It is often necessary to seek external support and expertise.

This White Paper proposes a selection of measures whose implementation can be effective in countering state-sponsored, cybercriminal, terrorist, or activist cyber threats. These measures, specific to the discussed operational context, do not replace the measures specified by the regulatory framework to be applied by the operator. Not all of the mentioned measures fall under the responsibility of the shipowner or operator. They cover governance, protection, detection/response, and resilience.

The primary objective is to integrate cybersecurity into the governance of maritime drone and autonomous ship systems. Eight measures are proposed in this White Paper.

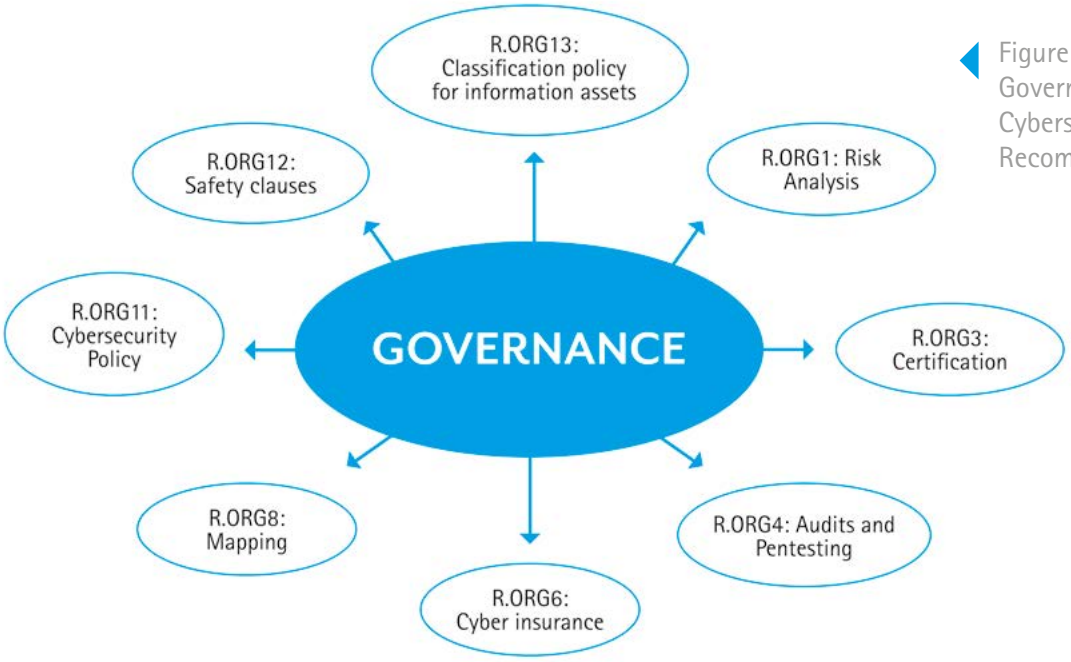

Figure 6: Governance Cybersecurity Recommandations.

[39] Defense in depth concept applied to information systems, ANSSI: https://www.ssi.gouv.fr/uploads/IMG/pdf/mementodep-v1-1.pdf

The second objective is to ensure defense in depth for maritime drone and autonomous ship systems. Thirteen associated measures have been identified.

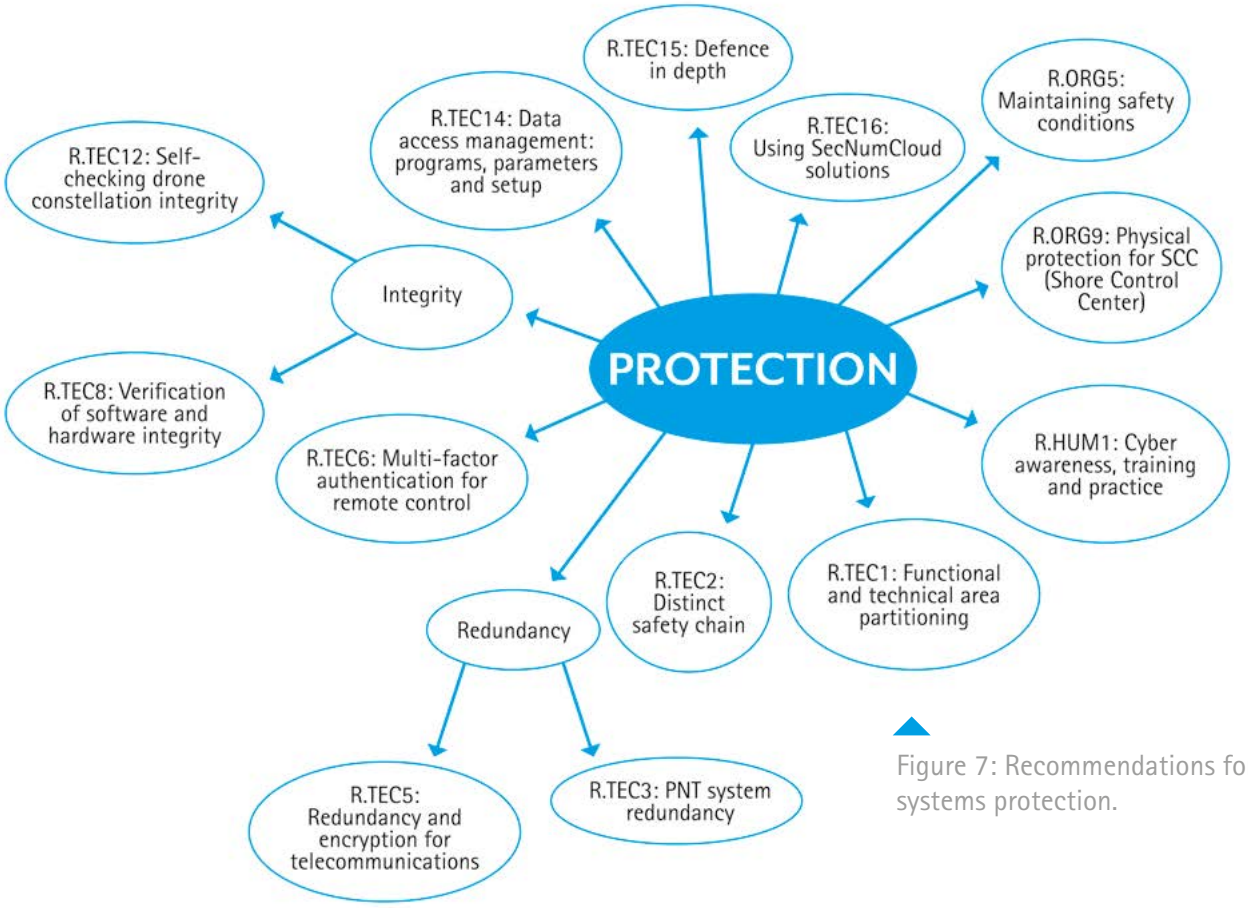

Figure 7: Recommendations for systems protection.

The third effect relates to the ability to detect and respond to cyber alerts.

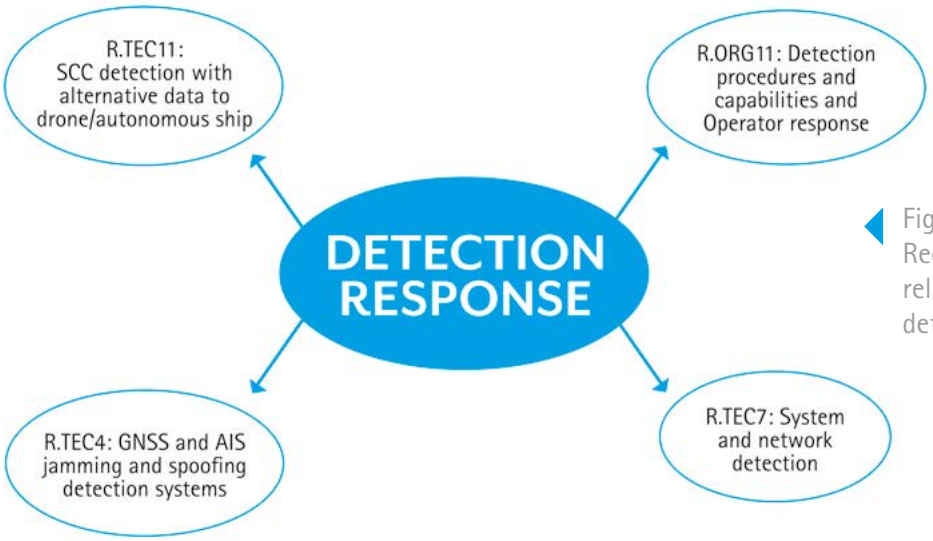

Figure 8: Recommendations related to cyberattacks detection and response.

Finally, the last effect concerns the resilience of the systems in question.

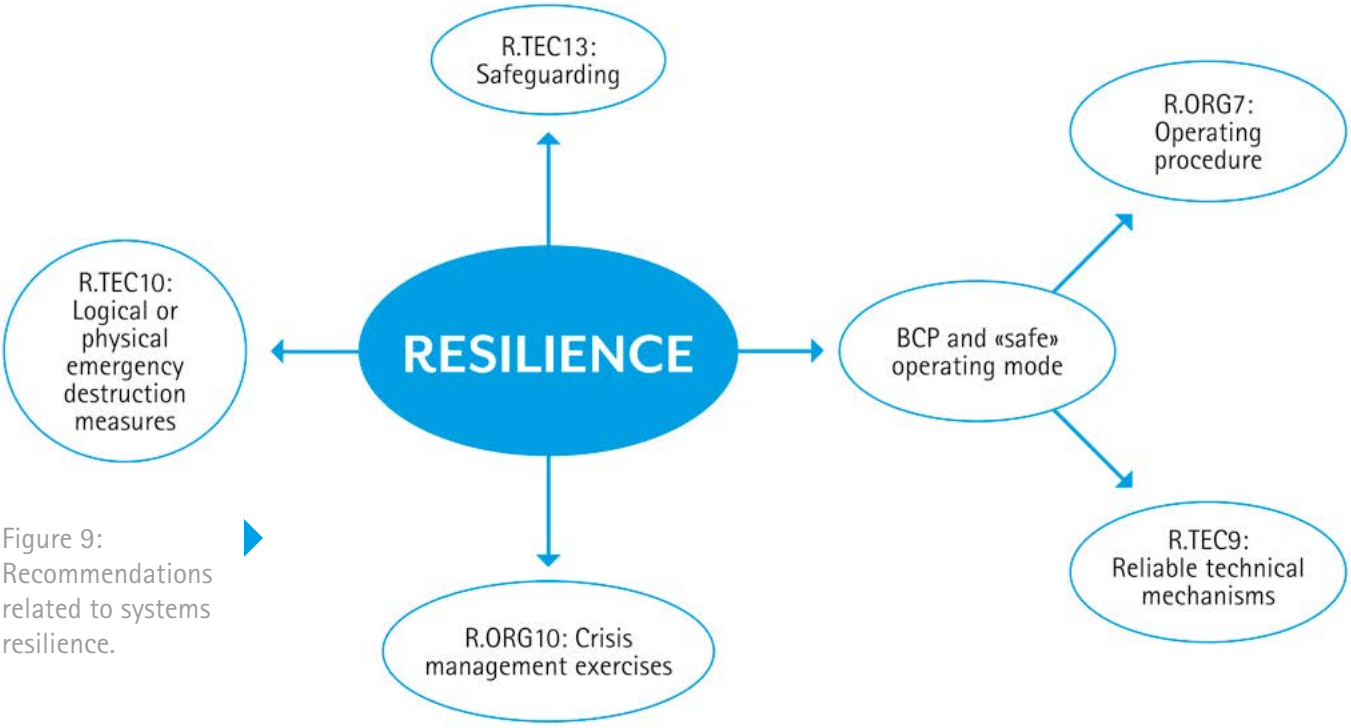

Figure 9: Recommendations related to systems resilience.

Organizational Recommendations (R. ORG)

R. ORG1: The analysis of the information system's scope of the maritime drone / autonomous ship and stakeholders should be carried out. This analysis, and the resulting measures, should take into account and remain rational with regard to the degree of autonomy and the business values supported by the information systems. This cyber risk analysis can rely on elements from this document (strategic scenarios, in particular), as well as on best practices in the field, especially those derived from guides prepared by ANSSI (French National Cybersecurity Agency).[40]

R. ORG2: Depending on the risk tolerance and the operational context of maritime drones and autonomous ships, it is essential that a cybersecurity certification process for these systems be conducted by a qualified authority.[41] Integrating cybersecurity from the design phase and throughout the lifecycle will help reduce associated costs.[42] Consideration may be given to certification from a classification society.

R. ORG3: Regular audits and penetration tests should be conducted on the entire ecosystem of maritime drones and autonomous ships, both during the design phase and in the operational phase.

R. ORG4: Processes and procedures for maintaining security should be formalized and implemented to reduce the occurrence or consequences of a cyber attack to a level acceptable to the qualifying authority. Special attention should be paid to the risks of digital obsolescence within the various systems.

[40] https://cyber.gouv.fr/en/publications/ebios-risk-manager-method
[41] https://www.ssi.gouv.fr/guide/lhomologation-de-securite-en-neuf-etapes-simples/
[42] https://www.ssi.gouv.fr/administration/guide/gissip-guide-dintegration-de-la-securite-des-systemes-dinformation-dans-les-projets/

R. ORG5: Special attention will be given to insurance coverage for autonomous operations and platforms with regard to cyber risk.

R. ORG6: The procedures implemented by the operator of the maritime drone/autonomous ship must include a return to a "safe" mode of operation in case of malfunction or major anomaly.

R. ORG7: A comprehensive software and hardware mapping of all digital components of the maritime drone/autonomous ship and its ecosystem, including the shore control center, will be carried out and kept up to date. This mapping can be based on existing best practices in the field.[43]

R. ORG8: The shore control center, or any equivalent shore organization, being particularly sensitive parts of the command and control chain of the maritime drone/autonomous ship, special attention will be given to its cybersecurity organization, physical and logical protection in depth, maintenance processes and operations performed therein, as well as its external dependencies (Virtual Private Network, routing, satellite connection, cloud computing, etc.).

R. ORG9: Regular cyber crisis management exercises, adapted to the specific context of the maritime drone/autonomous ship, will be conducted. They should cover the entire scope (including the shore control center), involve all stakeholders (supervisors, teleoperators, maintainers), and be based on realistic and up-to-date scenarios in response to threats.

R. ORG10: The organization operating the system must have internal or external means and procedures for analyzing, investigating, and responding to cyber incidents. These resources should cover the phases of anticipation, alert, and incident response coordination (involving a Computer Emergency Response Team), real-time monitoring (Security Operations Center), and incident response. If deemed necessary or required by regulations due to the criticality of the drone's mission, the use of providers qualified by ANSSI (Security Incident Detection Service Provider (PDIS)/Security Incident Response Service Provider (PRIS)) should be considered.

R. ORG11: The organizational, human, and technical cybersecurity measures implemented by the operator to reduce risks should be formalized in an Information Systems Security Policy (ISSP) tailored specifically to the maritime drone/autonomous ship, its installations, interfaces, and maintenance. This ISSP will define procedures for system integration, access control, password management, security maintenance, and incident management (incidents such as data loss, unauthorized data or software modification, unauthorized software installation, connection to unsecured systems or devices, etc.). Additionally, key performance indicators should be defined and monitored during the implementation phase of the PSSI to verify the effectiveness of its measures over time and to adjust or strengthen them if necessary.[44]

R. ORG12: To ensure that security concerns are properly addressed by the maritime drone or autonomous ship ecosystem, security clauses should be included in contracts with various stakeholders. These clauses will specify requirements related to audits/intrusion testing, security maintenance, mapping, crisis management, and awareness/training/exercises. Additionally, these contracts should require the provision of Security Assurance Plans in which third parties describe the measures taken to comply with security clauses.

R. ORG13: A policy for protecting the informational assets of the maritime drone or autonomous ship ecosystem should be defined. It will specify the protection measures associated with each level of information protection and/or classification throughout the information's lifecycle. Encryption of the most sensitive information in terms of confidentiality should be specifically addressed. Furthermore, this classification policy will ensure compliance with any regulatory requirements related to the protection of national defense secrets or personal data (architecture, technologies, software, hardware, parameters). Several guides can be used for this purpose.[45]

[43] https://www.ssi.gouv.fr/guide/cartographie-du-systeme-dinformation/
[44] https://www.ssi.gouv.fr/guide/pssi-guide-delaboration-de-politiques-de-securite-des-systemes-dinformation/
[45] See the following guide https://www.ssi.gouv.fr/guide/recommandations-pour-les-architectures-des-systemes-dinformation-sensibles-ou-diffusion-restreinte/

Human recommendations (R. HUM)

R. HUM1: The methods for raising awareness, training, and preparing all stakeholders for the cybersecurity of maritime drones and autonomous ships (administrations, designers-integrators, equipment suppliers, maintenance operators, shipowners, operators of the shore control center, etc.), at all levels of responsibility, will be formalized in the information systems security policy specific to the maritime drone/autonomous ship. These methods will be specified through contractual agreements and implemented from the system's design phase.

Technological recommendations (R. TEC)[46]

R. TEC1: Logical or physical separation and filtering between the different functional and technical areas of the maritime drone or autonomous ship are essential. For the onboard portion, effective logical or physical compartmentalization and protocol filtering between external telecommunication systems, sensors, actuators, control-command computers, navigation management systems, mission management systems, and administrative systems must be ensured. [47] Filtering between each zone should be carried out by a firewall providing effective protocol filtering, blocking all flows by default and only allowing authorized flows to pass through, with actions being logged.

R. TEC2: It is strongly recommended that a separate safety chain, consisting of safety Programmable Logic Controllers (PLC), be added in parallel to the production installation, especially for navigation systems, industrial control systems, and the mission payload. Maximum values and potentially non-compliant cases should be tested during the deployment of this security chain in real-world situations.

R. TEC3: For systems that do not have any human presence on board, it is essential that the Positioning, Navigation, and Timing (PNT) systems are redundant with alternative systems (other GNSS constellations, e.g., Galileo in addition to GPS), or by using alternative positioning methods (stellar positioning, inertial, e-LORAN, alternative satellite PNT systems, such as Satellite Time and Location (STL), for example), and by using special antenna systems (e.g., Controlled Radiation Pattern Antenna or CRPA) to reduce the risk of GNSS spoofing or jamming. Tests for GNSS jamming and spoofing should be conducted by accredited organizations to ensure the proper behavior of the drone/autonomous vessel in such situations.

R. TEC4: Systems providing surface situational awareness must be coupled with mechanisms for detecting GNSS and AIS (Automatic Identification System) spoofing or jamming. Tests for AIS jamming and spoofing should be conducted by accredited organizations to ensure the proper behavior of the drone/autonomous vessel in such cases.

R. TEC5: The means of communication within a drone constellation, with the carrier vessel, or with onshore centers (operational or maintenance) must be redundant and use encryption mechanisms in accordance with the rules recommended by ANSSI[48], depending on the mission's criticality, the communication means used (satellite, Wi-Fi, radio, etc.), the degree of autonomy of the drones, and the risk aversion. This will help avoid any risk of interception, intrusion, or loss of availability. It is strongly recommended that the required security criteria undergo independent evaluation by specialized organizations.

R. TEC6: The takeover of the maritime drone or autonomous vessel for control, supervision, or preventive or corrective maintenance, locally or remotely, must undergo multi-factor authentication. Any attempt or success should be logged. A secure backup mode (such as a "virtual safety glass") should be provided and qualified in case of multi-factor authentication malfunction.

[46] Most recommendations can also be applied to the information systems of the shore control center.
[47] Also called payload.
[48] https://www.ssi.gouv.fr/guide/mecanismes-cryptographiques/

R. TEC7: Intrusion detection systems, adapted to analyze the specific protocols used on the maritime drone or autonomous vessel, should be implemented. Signatures and/or behavior-based detection should be adapted to all modes of operation of the maritime drone / autonomous vessel. The intrusion detection system should be isolated from the networks it monitors by passive Test Access Port (TAP) equipment. Intrusion detection systems should be certified by ANSSI, with the choice of label (certification, qualification, and approval) depending on regulatory requirements and security needs. Where possible, detected cyber events will be logged by logging systems and processed in real-time or delayed by log correlation and analysis systems such as those operated by a Security Operations Center (SOC).

R. TEC8: The proper functioning and software and hardware integrity of the maritime drone / autonomous vessel will be checked at regular intervals, depending on the criticality and degree of autonomy of the information systems. In case of an anomaly, autonomous reinstallation of the software and, if necessary, the use of an alternative support or computer should be possible. To the extent possible, cyber events affecting the software and hardware integrity of the maritime drone or autonomous vessel will be transmitted in real-time or delayed to a CERT or SOC.

R. TEC9: The return to a "safe" operating mode must be formally described and tested using reliable technical mechanisms in case of malfunction or major anomaly.

R. TEC10: In specific cases (mission criticality, onboard hardware or software), emergency logical or physical destruction measures should be able to be implemented.

R. TEC11: The detection of anomalies (such as track anomalies) by the shore control center must be ensured using alternative means to the data transmitted by the maritime drone or autonomous vessel (e.g., track anomaly detection via satellite).

R. TEC12: In the case of a constellation of maritime drones / autonomous vessels, a self-integrity check of the entire constellation and each of its members must be possible. In the event of an anomaly, mechanisms should be in place to allow for the reinstallation of software to a safe state, the use of alternative equipment, or the exclusion of one or more members of the constellation depending on the situation.

R. TEC13: Backups of the entire ecosystem will be securely stored offline. Local or remote restoration tests will be regularly conducted.

R. TEC14: Access to data related to the programs, settings, and configurations of maritime drones and autonomous vessels must be guaranteed and logged to ensure the protection of potential secrets and to maintain their integrity and availability.

R. TEC15: Defense in depth of the system will be implemented, from the system's design phase throughout its lifecycle, by applying secure configuration measures to all operational and administrative digital equipment (hardening, proper management of access rights and accounts, user and administrator identification and authentication, use of secure protocols, encryption of digital media, changing default passwords, etc.).[49]

R. TEC16: Special attention will be given, in the case of using cloud computing technologies, to the location and security of hosting. Whenever possible, the use of a SecNumCloud certified hosting provider will be sought.[50]

[49] See the technical guides techniques of ANSSI on secure configurations at the following URL: https://www.ssi.gouv.fr/uploads/2014/10/anssi-catalogue-guides-notes-techniques.pdf
[50] See the list of qualified providers here: https://www.ssi.gouv.fr/uploads/liste-produits-et-services-qualifies.pdf

Regulatory recommendations (R. REG)

In addition to the investment made by shipowners, shipyards, operators, and manufacturers, the role of the regulator (international, European, or national) is considered essential to ensure the cybersecurity of maritime drones and autonomous vessels. Therefore, it is necessary for the use cases of maritime drones and autonomous vessels to be taken into account in existing regulations and recommendations, beyond the specific question of the seaworthiness of these equipment in the context of SOLAS regulations.

R. REG1: At the IMO level, efforts should take into account the cybersecurity of such systems, for example, within the future MASS (Maritime Autonomous Surface Ships) code.

R. REG2: The issuance of a navigability certificate, the registration procedure for drones, or the study for authorization for an autonomous ship to navigate experimentally should be conditional on the issuance of formal evidence of the adoption of suitable cybersecurity measures (at a minimum: specific risk analysis, implementation of appropriate protective measures, audits, and correction of identified gaps, and maintaining security conditions). This evidence could correspond to the system's approval decision or the issuance of an appropriate rating by a classification society.

R. REG3: In the absence of drones and autonomous ships, the NIS Directive v2, or its transposition into national laws, should include within its scope the shore control centers, when they perform an essential function or when a cyber incident happening their could pose a major risk (operational, environmental, or human).

ANNEXES

ANNEX 1

Details of the risk analysis

• Missions, business values and supporting assets

As mentioned earlier, the missions, business values, and supporting assets of maritime drones and autonomous ships are as follows:

Mission 1	Business values	
Design, build, and integrate maritime drones or autonomous ships.	Produce the maritime drone/autonomous ship	Data related to the architecture, programming, or production of the maritime drone/autonomous ship
Supporting assets	Systems for the design and development of maritime drones or autonomous ships: • Servers, storage spaces • Digital design, engineering, and development networks	

Mission 2	Business values	
Maintaining maritime drones or autonomous ships in service	Maintain the maritime drone/autonomous ship in operational use	Data related to the maintenance of the maritime drone/autonomous ship
Supporting assets	System for the operational maintenance of maritime drones or autonomous ships: • Servers, storage spaces • Digital maintenance networks • Mobile maintenance stations • Specific links dedicated to maintenance and/or remote monitoring	

Mission 3	Business values	
Navigate safely and in compliance with international regulations	Prepare for navigation and navigate safely and securely	Data related to navigation preparation and the operation of the maritime drone maritime/autonomous ship
Supporting assets	Onboard navigation management system for the maritime drone or autonomous vessel: • Position, navigation and time (PNT) and AIS sensors • Industrial Control Systems for mobility (energy, propulsion, etc.) • Computers • Satellite communication systems (long distance) and/or radio systems for proximity (Line of Sight (LoS)) Digital management systems (onboard and onshore): • Servers and storage space for the programs required for the operation of the drone or autonomous vessel • Digital networks for managing operations • Digital media/workstations for reading and writing the necessary information for operation	

Mission 4	Business values	
Fulfill their assigned mission	Carry out the activities planned within the scope of the mission	Data delivered, collected or produced during the mission
Supporting assets	Mission management system: varies depending on the type of maritime drone/autonomous vessel, sensor/effector, and the context of use Digital management systems (onboard and onshore): • Servers, storage spaces for the programs necessary for the operation of the drone or autonomous vessel • Digital networks for managing operations • Drives/workstations to read and write data necessary for operation	

It should be noted that the associated supporting assets are multiple and will depend on the size, type, and degree of autonomy of the maritime drone or autonomous vessel:

- For missions M1 and M2, the designers, equipment manufacturers, integrators, and maintainers (internal or external) of these systems will use, for example, servers, storage spaces, and digital networks for design, engineering, development, and maintenance. They may also perform the programming of specific equipment using mobile maintenance stations and/or dedicated links for predictive, preventive, corrective maintenance or remote monitoring.
- For mission M3, the maritime drone or autonomous vessel will use, on one hand, sensors such as position, navigation, and time (GNSS systems, RADAR, LIDAR (Laser Imaging Detection And Ranging), sonar, optical sensors, AIS/VDES (VHF Data Exchange System), log, compass) and associated calculators. On the other hand, it will use industrial control systems to ensure its mobility (power, propulsion, steering control, etc.). In the vast majority of cases, these are off-the-shelf equipment available in the maritime industry and can be interconnected using industry standards like NMEA 0183/2000. The role of calculators is particularly important for sensor data fusion, autonomous navigation, decision-making, and actuator management. Communication with ground control centers or carrier vessels will use various radio communication methods, including satellite (INMARSAT, VSAT, Thuraya, Starlink, Iridium, etc.) for long-distance links and Line of Sight (LoS) radio for communication with nearby drones and vessels, such as within a constellation. Digital media used for reading and writing information and storing the programs required for the operation of the drone/autonomous vessel will be particularly sensitive support assets.
- For mission M4, the supporting assets (such as sensors, effectors, calculators, communication systems, and storage media) can vary depending on the type of maritime drone/autonomous vessel, sensor/effector, and operational context. The protection (integrity, confidentiality, availability, traceability, non-repudiation) of the processes ensuring the transfer of information to and from the maritime drone and autonomous vessel will depend on the sensitivity of the transmitted information and the specific mission-related requirements. Therefore, the required protection levels between a scientific research-oriented drone and a naval combat drone are likely to be quite different.

• Stakeholders

Many malicious actors are known to exploit various links in the supply chain (partners, subcontractors, etc.), often with lower maturity levels, to target a significant or sensitive organization. It is essential to consider all stakeholders to identify potential attack vectors in a system.

To conduct the risk analysis of a maritime drone or autonomous vessel, the following stakeholders should be considered:

- PP1: Designers, equipment suppliers, integrators;
- PP2: Operators
- PP3: Crew members[51]
- PP4: Internal or external maintenance operators
- PP5: telecommunication or reference broadcasting operators (positioning, navigation, time)

• Sources of risk

Given that unintentional threats are not considered by EBIOS Risk Manager, the identified sources of risk could include the following, with their prioritization depending on the context of use of the maritime drone or autonomous ship and the operator's risk aversion:

- SR1: Revenge from a former employee or maintenance operator whose accounts may not have been revoked, for example.
- SR2: Activists opposed to maritime drones and autonomous ships or opportunistic attackers who would have managed to take control of a ship to expose its weaknesses.
- SR3: A competitor seeking sensitive data about the maritime drone or autonomous ship, either discreetly through espionage or detructively.
- SR4 Cybercriminal actors looking for financial gain who might hold hostage the onshore or onboard information systems related to the maritime drone or autonomous ship.
- SR5: Terrorists attempting to destroy the ship or use it to cause harm to a third party.
- SR6: State actors seeking to spy by retrieving mission data from the maritime drone/autonomous ship, destroy it, take control, or damage the drone or autonomous ship.

• Feared events

The feared events related to maritime drones and autonomous shipscan be identified, and their classification in termes of severity depends on the organization's risk aversion. Although this risk aversion may vary depending on the type of carrier (drone/ship), its mission and its operator, the following feared events could be identified:

Feared events related to the design and production of autonous drones or ships can be identified as follows (Mission 1) :

- ER1: Disruption or interruption of the production of the maritime drone or autonomous ship.

  Impacts: operational impacts, financial impacts, legal impacts, impacts on reputation and trust
- ER2: Data leak related to the architecture, programming, or production of a maritime drone or autonomous ship.

  Impacts: financial impacts, impacts on governance
- ER3: Altration of data related to architecture, programming, or production of a maritime drone or autonomous ship.

  Impacts: impacts on safety, impacts on reputation and trust, legal impacts

[51] for degrees 1 and 2 autonomous ships

Feared events relating to the maintenance of the drone or autonomous ship (Mission 2):

- ER4: Disruption or interruption of maintenance for maritime drone or autonomous ship.

  Impacts: operational impacts, financial impacts, legal impacts, impacts on reputation and trust, impacts on safety

- ER5: Data leak related to the maintenance of a maritime drone or autonomous ship.

  Impacts: financial impacts, impacts on gouvernance, impacts on reputation and trust

- ER6: Alteration of maintenance data for a maritime drone or autonomous ship

  Impacts: impacts on safety, impacts on image and trust, legal impacts

Feared events relating to the safe navigation capability of the drone or autonomous ship (Mission 3):

- ER7: Disruption or interruption of the preparation for the navigation of a the maritime drone or autonomous ship

  Impacts: financial impacts, operational impacts

- ER8: Alteration or destruction of the maritime drone or autonomous ship

  Impacts: financial impacts, impacts on safety, operational impacts, environmental impacts, human impacts

- ER9: Seizure of the maritime drone or autonomous vessel

  Impacts: financial impact, operational impacts, impacts on gouvernance

- ER10: Alteration of data relating to the preparation of the navigation phase, of the navigation itself and to the proper operation of the maritime drone/autonomous vessel

  Impacts: impacts on safety, operational impacts, financial impacts

Feared events relating to the mission of the maritime drone or autonomous ship (Mission 4):

- ER11: Disruption or diversion of the mission

  Impacts: operational impacts, financial impacts, impacts on governance, impacts on safety

- ER12: Leak of data collected during its mission

  Impacts: financial impacts, impacts on governance, impacts on reputation and trust

- ER13: Alteration of data collected during its mission

  Impacts: operational impacts, financial impacts, impacts on governance

ANNEX 2

Reducing risks associated with strategic scenarios

The objective of this table is to demonstrate the reduction of risks associated with strategic scenarios through the implementation of the proposed organizational, human, and technical measures.

SS1: The compromise of the equipment providing the connection with the Shore Control Center or the operations taking place there results in a loss of communication with the maritime drone or autonomous vessel, disrupting its mission.
R. ORG1 R. ORG2 R. ORG3 R. ORG4 R. ORG5 R. ORG6 R. ORG7 R. ORG8 R. ORG9 R. ORG10 R. ORG11 R. ORG12 R. HUM1 R. TEC1 R. TEC2 R. TEC5 R. TEC6 R. TEC7 R. TEC9 R. TEC11 R. TEC13 R. TEC15 R. TEC16 R.TEC17
SS2: The disruption by spoofing or jamming of the information received by the sensors of the maritime drone or autonomous vessel (GNSS, AIS, RADAR, etc.) leads to a temporary or permanent disruption of the operational mission.
R. ORG1 R. ORG2 R. ORG3 R. ORG5 R. ORG6 R. ORG7 R. ORG9 R. ORG11 R. ORG12 R. HUM1 R. TEC2 R. TEC3 R. TEC4 R. TEC9 R. TEC11 R.TEC17
SS3: Compromising the information systems of the maritime drone or autonomous vessel during maintenance leads to a mission interruption or diversion.
R. ORG1 R. ORG2 R. ORG3 R. ORG4 R. ORG5 R. ORG6 R. ORG7 R. ORG9 R. ORG10 R. ORG11 R. ORG12 R. HUM1 R. TEC1 R. TEC2 R. TEC5 R. TEC6 R. TEC7 R. TEC8 R. TEC9 R. TEC 10 R. TEC11 R.TEC12 R. TEC13 R.TEC14 R. TEC15 R.TEC17
SS4: Compromising the calculation and decision-making algorithms of the maritime drone or autonomous vessel during the design phase leads to a serious incident during its commissioning.
R. ORG1 R. ORG2 R. ORG3 R. ORG4 R. ORG5 R. ORG6 R. ORG7 R. ORG8 R. ORG9 R. ORG10 R. ORG11 R. ORG12 R. HUM1 R. TEC1 R. TEC2 R. TEC8 R. TEC9 R. TEC10 R. TEC11 R.TEC12 R. TEC13 R .TEC14 R.TEC17
SS5: An attack on the supply chain (designers, equipment suppliers, integrators) results in the theft of plans or data related to a drone or autonomous vessel project.
R. ORG1 R. ORG2 R. ORG3 R. ORG4 R. ORG5 R. ORG6 R. ORG7 R. ORG8 R. ORG9 R. ORG10 R. ORG11 R. ORG12 R. HUM1 R. TEC10 R. TEC13 R. TEC15 R. TEC16 R. TEC 17

ANNEX 3

Compliance with the requirements of the European NIS Directive.

The European NIS Directive sets 23 security rules. Without prejudging the evolution of these measures related to the publication, and then the transposition into French law, of its second version, this White Paper proposes to verify that the measures proposed for maritime drones and autonomous ships are consistent with this directive. The details of the measures are not included in the table but are included in the order published in the French Official Journal.[52] The entire ecosystem of maritime drones and autonomous ships currently does not have an obligation to comply with the order transposing the NIS Directive into French regulations. However, depending on the criticality of the missions, teleoperation centers may be required to comply with it, either currently or within the framework of version 2 of the directive.

As these measures are also good generic and cross-sectoral practices, they are effective in preventing a significant number of incidents in any case. It should be noted that version 2 of the directive provides more detailed specifications for certain measures, including specifying degrees based on the organization's status and/or the system's criticality.

Of course, the effectiveness of the coverage will depend on the effectiveness of the measures implemented. The coverage mentioned here by the proposed measures is indicative to better assess the effectiveness of certain rules.

NIS Rule Number	Description	Covered by rule(s)
Rule 1	Conduct and maintain a risk analysis.	R. ORG1
Rule 2	Develop, maintain, and implement an information security policy.	R. ORG11
Rule 3	Security Certification of Essential Information Systems.	R. ORG2
Rule 4	Evaluation and update of key performance indicators.	R. ORG11
Rule 5	Conduct of cybersecurity audits.	R. ORG3
Rule 6	Elaboration and update of digital map of assets.	R. ORG7
Rule 7	Secure configuration of information systems.	R. TEC15
Rule 8	Partitioning of information systems.	R. TEC1
Rule 9	Remote access to information systems.	R. TEC6
Rule 10	Filter access to information systems.	R. TEC1
Rule 11	Priviledged accounts management.	R. TEC15
Rule 12	Management of information systems.	R. TEC15

[52] https://www.legifrance.gouv.fr/loda/id/JORFTEXT000037444012

Rule 13	Identification of users.	R. TEC15
Rule 14	Authentification of users.	R. TEC15
Rule 15	Access rights to the information system.	R. TEC15
Rule 16	Patch management processes.	R. ORG4
Rule 17	Physical and environmental security.	R. ORG8 R. TEC10
Rule 18	Security incidents detection.	R. TEC7
Rule 19	Logging.	R. TEC1 R. TEC6 R.TEC8
Rule 20	Logs correlation and analysis.	R. ORG10
Rule 21	Incident response.	R. ORG10
Rule 22	Alerts management.	R. ORG10
Rule 23	Crisis management.	R. ORG9 R. HUM1

GLOSSARY

A

AIS: Automatic Identification System
ANSSI: Agence Nationale de la Sécurité des Systèmes d'Information
AUV: Autonomous Underwater Vehicle

C

CRPA : Controlled Radiation Pattern Antenna

D

Decommissionning: End of life of a software or of a digital asset.
Denial of service: Action that has the effect of preventing or severely limiting a system's ability to provide the expected service.
DGAMPA: Direction Générale des Affaires Maritimes, de la Pêche et de l'Aquaculture.

E

EBIOS: Expression des Besoins et Identification des Objectifs de Sécurité
ENSM: École nationale supérieure maritime

G

GICAN: Groupement des Industries de Construction et Activités Navales
GNSS: Global Navigation Satellite System
GPS: Global Positioning System

H

HALE: High Altitude, Long Endurance

I

IACS: International Association of Classification Societies
ISM : International Safety Management Code

L

LIDAR: Laser Detection And Ranging
LoS: Lign of Sight

M

MALE: Medium Altitude, Long Endurance
MASS: Maritime Autonomous Surface Ship
MFA: Multiple Factor Authentification is a method by which a user can access a computer resource (a computer, a smartphone, or a website) after presenting two separate identity proofs to an authentication mechanism
MMCM: Maritime Mine Counter Measures

N

NATO: North Atlantic Treaty Organization
NIS: Network Information Security
NMEA: National Maritime Electronics Association

O

OIV: Opérateur d'Importance Vitale
OSE: Opérateur de Service Essentiel

P

PNT: Position, Navigation, Time

R

RADAR : RAdio Detection And Ranging
Rançongiciel : Forme d'extorsion imposée par un code malveillant sur un utilisateur du système. Le terme anglophone est *ransomware*.
Ressources : Ensemble des composants, matériels ou logiciels, connectés à un ordinateur. Tout composant de système interne est une ressource. Les ressources d'un système virtuel incluent les fichiers, les connexions au réseau, et les zones de mémoire.
ROV : Remotely Operated Vehicle

S

SOLAS: Safety Of Life At Sea
SIIV: Système d'Information d'Importance Vitale
SCC: Shore Control Center

U

UAV: Unmanned Aerial Vehicle)
UMS: Universal Measurement System
USV: Unmanned Surface Vehicle
UUV: Unmanned Underwater Vehicle

V

VDES : Very High Frequency Data Exchange System
VPN : Virtual Private Network
VSAT : Very Small Aperture Terminal

IN COOPERATION WITH

MARINE NATIONALE

GENDARMERIE MARITIME

FRANCE CYBER MARITIME

Le Grand Large
Quai de la douane, 2ème éperon
29200 BREST

CONTACT

02 57 52 09 87
contact@france-cyber-maritime.eu
www.france-cyber-maritime.eu
France Cyber Maritime
@FrCyberMaritime

www.france-cyber-maritime.eu

SUPPORTED BY

FRANCE RELANCE
PREMIER MINISTRE Liberté Égalité Fraternité
Secrétariat général de la mer
RÉPUBLIQUE FRANÇAISE Liberté Égalité Fraternité
ANSSI
Région BRETAGNE
Brest Métropole