LIVRE BLANC

CYBERSÉCURITÉ DES DRONES MARITIMES ET NAVIRES AUTONOMES

14/09/2023

AVEC LE SOUTIEN DE

PREMIER MINISTRE
Liberté Égalité Fraternité

Secrétariat général de la mer

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

Région BRETAGNE

Brest MÉTROPOLE

AVANT-PROPOS

France Cyber Maritime est une association Loi 1901 dont la mission est de contribuer au renforcement de la cybersécurité du secteur maritime et portuaire français. La question de la cybersécurité des drones maritimes et navires autonomes est un sujet sur lequel nous avons été rapidement sollicités. Cette question fait l'objet d'échanges fréquents avec nos adhérents et partenaires, ainsi qu'avec l'Administration, et est régulièrement abordée lors de conférences et tables rondes, en France comme à l'étranger.

Le sujet des drones et navires autonomes, maritimes et navals n'est plus seulement un cas d'étude « pour le futur ». Les premières conceptions, réalisations et emplois opérationnels ont lieu dès aujourd'hui. La mise en œuvre de ces engins pose des problèmes spécifiques, réglementaires, humains, technologiques et organisationnels qui nécessitent une réponse adaptée. Fortement numérisés, ces mobiles, dont l'autonomie est assurée par des algorithmes complexes, regorgent de capteurs et d'actionneurs et dépendent de systèmes de télécommunication et de navigation pour assurer leurs missions. Étant donné leur emploi stratégique actuel et futur, dans notre « économie bleue » et pour notre sécurité, ils présentent, ainsi que les entreprises qui les conçoivent, un intérêt réel pour des cyber attaquants étatiques, criminels ou terroristes. Outre la menace cyber sur ces engins dont la production souveraine est un véritable enjeu, le risque de défaillances liées à leurs systèmes d'information n'est pas à écarter. Les drones maritimes et navires autonomes joueront un rôle essentiel dans la connaissance, l'exploration et la maîtrise des océans, enjeux stratégiques pour notre avenir[1]. C'est donc l'ensemble de leur écosystème numérique qu'il faut protéger contre les cyberattaques, de la conception à l'exploitation.

Dans ce Livre blanc, nous souhaitons apporter au lecteur une vision la plus complète possible sur ce sujet et dégager les points d'attention et les recommandations réglementaires, humaines, technologiques et organisationnelles pour la conception et l'exploitation cybersécurisée des drones et navires autonomes. Notre objectif est de permettre un éclairage que nous espérons objectif et complet sur ces enjeux pour le monde maritime et portuaire.

Nous espérons démontrer que la mise en place de mécanismes de cybersécurité adaptés sur ce type d'engin est possible, pour peu que ce sujet soit traité dès les phases de conception. Pour cela, l'engagement de l'État et l'action des concepteurs, équipementiers, armateurs, opérateurs et marins, entreprises et personnels en charge de leur maintenance, assureurs et sociétés de classification sont essentiels.

En tant qu'acteur du monde maritime et portuaire ou de la cybersécurité, et sans nécessairement devenir expert, nous espérons que la lecture de ce Livre blanc vous permettra de disposer d'un avis éclairé pour contribuer efficacement à la cybersécurité des drones maritimes et navires autonomes.

M. FRÉDÉRIC MONCANY DE SAINT-AIGNAN
Président de France Cyber Maritime

[1] Le ministère des Armées s'est doté d'une stratégie de maîtrise des fonds marins en février 2022 : https://www.defense.gouv.fr/sites/default/files/ministere-armees/20220211_GT%20MAITRISE%20FONDS%20MARINS_dossier%20de%20presse.pdf

LES CONTRIBUTEURS

Nous tenons à remercier toutes les personnes et organismes, publics et privés, qui ont contribué à la création de ce Livre blanc. Leur expertise et leur expérience sur le sujet ont été particulièrement précieuses pour aboutir à un travail collaboratif de qualité.

France Cyber Maritime tient à remercier les organismes suivants, par ordre alphabétique :

- 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

SOMMAIRE

AVANT-PROPOS 3

LES CONTRIBUTEURS 4

INTRODUCTION 7
POURQUOI LIRE CE LIVRE BLANC ? 7
SYSTÈME D'INFORMATION ET CYBERESPACE 9
LA CYBERSÉCURITÉ 9
LA GESTION DES RISQUES CYBER 10

DRONES MARITIMES ET NAVIRES AUTONOMES : CARACTÉRISTIQUES ET CONTEXTES D'EMPLOI 11
LES DRONES MARITIMES 12
Les drones aériens (UAVs) évoluant dans un contexte maritime 12
Les drones maritimes de surface (USVs) 14
Les drones sous-marins (UUVs) 14
Contexte d'emploi 16
Contraintes 16

LES NAVIRES AUTONOMES 17
Contexte d'emploi 17
Contraintes 18

ARCHITECTURE D'ENSEMBLE ET FONCTIONNELLE DES DRONES ET NAVIRES AUTONOMES 18

DRONES MARITIMES ET NAVIRES AUTONOMES : VULNÉRABILITÉS ET SCÉNARIOS DE MENACE 20
RÉGLEMENTATION ET MEILLEURES PRATIQUES APPLICABLES 20
BESOINS DE SÉCURITÉ 23
ANALYSE DE RISQUES 23
Périmètre de l'analyse de risques 24
Scénarios stratégiques 24

DRONES MARITIMES ET NAVIRES AUTONOMES : RECOMMANDATIONS DE CYBERSÉCURITÉ 26
RECOMMANDATIONS ORGANISATIONNELLES (R. ORG) 28
RECOMMANDATIONS HUMAINES (R. HUM) 30
RECOMMANDATIONS TECHNOLOGIQUES (R. TEC) 30
RECOMMANDATIONS RÉGLEMENTAIRES (R. REG) 32

ANNEXE 1 – DÉTAILS DE L'ANALYSE DE RISQUES 34
MISSIONS, VALEURS MÉTIERS ET BIENS SUPPORTS 34
PARTIES PRENANTES 35
SOURCES DE RISQUES 36
ÉVÈNEMENTS REDOUTÉS 36

ANNEXE 2 - RÉDUCTION DES RISQUES ASSOCIÉS AUX SCÉNARIOS STRATÉGIQUES 38

ANNEXE 3 – RESPECT DES EXIGENCES DE LA DIRECTIVE EUROPÉENNE NIS 39

GLOSSAIRE 41

INTRODUCTION

Pourquoi lire ce Livre blanc ?

Comme tous les secteurs industriels, le secteur maritime s'est fortement transformé depuis les années 2000. D'un recours majoritaire aux systèmes analogiques et mécaniques, en passerelle comme en salle des machines, les installations critiques des navires ont aujourd'hui fortement recours au numérique, qu'il s'agisse de communiquer avec la terre, de piloter le navire, d'avoir la connaissance de la situation surface ou de la situation météorologique, mais aussi pour l'accomplissement des missions. Cette situation vaut tout autant pour les navires civils que militaires. Plus personne n'imagine aujourd'hui faire appareiller un navire sans ses systèmes d'information, ses systèmes de contrôle industriels ou encore ses systèmes de télécommunication.

En parallèle, et de manière plus récente, les drones maritimes et navires autonomes deviennent progressivement une réalité. Les objectifs de leurs emplois sont multiples : améliorer l'endurance de la présence en mer, assurer des missions peu valorisantes ou dangereuses pour l'homme ou l'armateur et donc améliorer la sécurité des marins, pallier le manque de personnel, assurer des missions de surveillance ou de transport, etc.

La numérisation et l'automatisation permettent de limiter la réalisation de tâches autrefois répétitives ou dangereuses par l'homme : elle est donc un vecteur d'amélioration de la sécurité, de la sûreté et de la productivité de notre monde maritime. Cette transition engendre également des gains de rapidité, de flexibilité et de sécurité pour l'ensemble du secteur maritime et portuaire. Les flux logistiques, souvent tendus, gagnent en performance dans un secteur particulièrement concurrentiel. Le numérique devient ainsi un vecteur parfois différenciant pour les armateurs ou les ports. Dans certains cas, il permet aussi de réduire certains coûts.

Pour autant, le numérique n'est pas exempt de faiblesses : l'utilisation de protocoles non sécurisés, de logiciels et de matériels obsolètes ou conçus sans prise en compte de la cybersécurité, la difficulté de maintien en conditions de sécurité et la mise en place d'architectures déficientes sont régulièrement exploitées par les attaquants étatiques, criminels ou activistes pour mener des cyberattaques.

Les cyberattaques, aux objectifs variés (espionnage, demande de rançon, sabotage, etc.) et aux conséquences tout sauf virtuelles (atteinte à l'image de marque, perte financière, impact cyber-physique, etc.) touchent durement le secteur depuis plusieurs années[2] : la mécanique pourtant bien huilée du secteur s'enraye alors brutalement avec, parfois, des impacts opérationnels importants à court terme.

C'est fort de ce constat et en l'appliquant au cas particulier des drones maritimes et navires autonomes que nous avons souhaité aborder des thèmes qui nous semblent essentiels pour comprendre leur fonctionnement, leurs forces et faiblesses, les risques associés et les moyens de les protéger. Si les risques cyber liés aux drones maritimes et navires autonomes sont, généralement, communs avec d'autres systèmes du même type, les réponses apportées par le secteur seront propres à chacun, car elles dépendront intimement de la stratégie de l'organisation, de sa perception des risques cyber et du contexte d'emploi de l'équipement, mais aussi de son budget.

Ces travaux ont été menés par France Cyber Maritime lors d'un groupe de travail organisé dans le cadre du Conseil Cybersécurité du Monde Maritime, piloté par le Secrétariat Général de la Mer.

[2] Consulter, à ce titre, la base de données « ADMIRAL » entretenue par le M-CERT opéré par France Cyber Maritime sur les incidents publics touchant le secteur : https://gitlab.com/m-cert/admiral

Ce Livre blanc est divisé en trois grandes parties : en premier lieu, nous rappellerons les caractéristiques physiques, techniques et de conception des drones et navires autonomes, ainsi que leurs contextes d'emploi, afin de faciliter l'utilisation d'un vocabulaire et de concepts communs.

Ensuite, nous détaillerons les vulnérabilités et scénarios de menaces potentiels pour ce type d'engin. Enfin, nous émettrons des recommandations spécifiques de cybersécurité, afin d'améliorer leur niveau de cybersécurité et ce, de leur conception jusqu'à leur retrait du service.

Bien entendu, un sujet aussi complexe et technologique que la cybersécurité des drones maritimes et navires autonomes ne peut être traité de manière exhaustive en quelques pages et le soutien, pour les armateurs, ports, équipementiers et intégrateurs, d'un écosystème cyber de qualité tel que celui représenté au sein de notre association France Cyber Maritime sera essentiel.

Nous espérons que ce Livre blanc vous apportera un premier éclairage, appellera des développements ultérieurs et contribuera au renforcement de la cybersécurité des drones maritimes et navires autonomes français.

Web illustrations by Storyset*

*https://storyset.com/web

Système d'information et cyberespace

Le terme « système d'information » fait l'objet de nombreuses définitions et interprétations en fonction des pays, des personnes et des organisations. De manière générale, il peut être défini comme un « système manuel ou automatisé, comme un système de traitement automatique de données, un système informatique ou un réseau informatique, s'appuyant sur des infrastructures techniques et composé de personnes, de machines et de méthodes et qui est organisé pour réaliser des fonctions de collecte, de traitement, de transmission et de diffusion de données qui représentent de l'information. »[3]

Par extension, le cyberespace, nouveau « champ de confrontation à part entière », comprend, d'après l'OTAN, « l'information elle-même, les individus, organisations et systèmes qui la reçoivent, la traitent et la transmettent, et l'espace cognitif, virtuel et physique dans lequel cela se produit ».[4]

Le cyberespace est donc interdépendant de l'air, de la terre, de la mer et de l'espace, domaines dont il est cependant transverse puisqu'il peut se retrouver en chacun d'eux.

La cybersécurité

D'après une définition fréquemment acceptée, « la cybersécurité est un état recherché pour un système d'information, lui permettant de résister à des évènements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises, et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. »[5]

On entendra aussi souvent parler de :

- **cyberprotection** (ou sécurité des systèmes d'information), en tant qu'état recherché pour que les systèmes d'information soient sûrs et performants en termes de disponibilité, d'intégrité et de confidentialité dès leur conception et tout au long de leur cycle de vie ;
- **cyberdéfense**, qui comprend les « mesures techniques et non techniques permettant à un état de défendre dans le cyberespace les systèmes d'information jugés essentiels »[5] ;
- **cyber résilience**, qui représente la « capacité d'un système d'information à résister à une panne et à revenir à son état initial après l'incident »[5],

la cybersécurité en constituant donc l'ensemble.

On parlera aussi régulièrement des propriétés de sécurité suivantes, dont la recherche permet d'assurer la cybersécurité et de réduire les risques :

- la **disponibilité**, qui permet de garantir un accès permanent et résilient aux ressources du système d'information ;
- l'**intégrité**, qui garantit l'absence de modification illégitime ou involontaire du système d'information ;
- la **confidentialité**, qui garantit qu'une information n'est accessible et divulguée qu'aux personnes, organisations ou processus autorisés à en avoir connaissance ;

[3] Olivier Jacq. Détection, analyse contextuelle et visualisation de cyber-attaques en temps réel : élaboration de la *Cyber Situational Awareness* du monde maritime. Cryptographie et sécurité [cs.CR]. École nationale supérieure Mines-Télécom Atlantique, 2021. Français. NNT : 2021IMTA0228. tel-03145173 (https://theses.hal.science/tel-03145173v1/file/2021IMTA0228_Jacq-Olivier.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)

- la **traçabilité**, qui assure que tout action manuelle ou automatique sur un système d'information fait l'objet d'un suivi idoine permanent ;
- la **non-répudiation**, qui garantit que l'auteur de toute action manuelle ou automatique ne peut nier *a posteriori* avoir mené une action.

Enfin, il convient de souligner que, si la cybersécurité fait aujourd'hui souvent uniquement mention des attaques externes et intentionnelles, la menace interne (involontaire ou malveillante), d'une part, et le risque accidentel (panne, dysfonctionnement, erreur…) ne doivent jamais être sous-estimés.

La gestion des risques cyber

La surface d'attaque, la complexité de certains systèmes, l'incapacité à traiter certaines vulnérabilités spécifiques ou systémiques rendent la sécurisation d'un système *in extenso* souvent impossible. La gestion des risques cyber a donc pour vocation d'identifier les risques à considérer pour le système et à en assurer un traitement optimal et rationnel, afin de réduire l'occurrence du scénario à un seuil acceptable.

Deux approches sont essentielles à cette gestion des risques cyber :

- le traitement des risques par conformité, afin de répondre à des contraintes juridiques ou réglementaires générales, sectorielles, normatives, ou encore liées à un statut ou à une politique de cybersécurité existante de l'organisme ;
- le traitement des risques après analyse et formalisation des scénarios stratégiques et opérationnels de risques pour le système considéré, en fonction de ses caractéristiques et de son contexte d'emploi et, ce, afin d'obtenir une analyse la plus rationnelle possible.

Ce traitement des risques n'est réellement efficace, et moins coûteux, que lorsqu'il est réalisé dès la conception du système considéré. Un traitement des risques en aval, souvent plus long et complexe à mettre en œuvre, ne permet généralement pas un traitement homogène, pertinent et « en profondeur » des risques. En phase de conception, et en fonction des risques considérés et du périmètre numérique, il est généralement reconnu que la mise en œuvre de mesures de cybersécurité représente un investissement nécessaire de l'ordre de 5 à 10 % du montant du projet global. Cet investissement peut se transformer en surcoût de l'ordre de 10 à 15 % du projet s'il n'a pas été réalisé en amont.

La méthode d'analyse des risques aujourd'hui recommandée par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) est EBIOS Risk Manager[6].

[6] https://www.ssi.gouv.fr/entreprise/management-du-risque/la-methode-ebios-risk-manager/

DRONES MARITIMES ET NAVIRES AUTONOMES : CARACTÉRISTIQUES ET CONTEXTES D'EMPLOI

L'Organisation Maritime Internationale (OMI) travaille sur un projet de code adossé à la convention SOLAS (*Safety Of Life At Sea*)[7], visant à préciser l'applicabilité des conventions internationales aux navires autonomes.

Les drones maritimes ne sont pas concernés par ces travaux internationaux, la distinction entre drones et navires autonomes étant propre au cadre actuellement mis en place en France. En effet, la France a créé un régime spécifique d'exploitation expérimentale de ces engins, établi par l'arrêté du 20 mai 2020, relatif aux modalités d'expérimentation de la navigation des engins flottants maritimes autonomes ou commandés à distance[8]. Le nouveau régime, applicable aux phases expérimentales, introduit par l'ordonnance n°2021-1330 du 13 octobre 2021, relative aux conditions de navigation des navires et des drones maritimes[9], n'entrera en vigueur qu'une fois les textes d'application publiés (décret modifiant le décret 84-810 et arrêtés techniques d'exploitation). Cette ordonnance précise la terminologie de drone maritime et de navire autonome :

- Un drone maritime est un engin flottant de surface ou sous-marin opéré à distance ou par ses propres systèmes d'exploitation, sans personnel, passager ni fret à bord, et dont les caractéristiques techniques, notamment les limites de taille, de puissance et de vitesse, sont définies par voie réglementaire, sans que sa jauge brute puisse être supérieure ou égale à 100 unités UMS (*Universal Measurement System*) ;
- Un navire autonome est un navire opéré à distance ou par ses propres systèmes d'exploitation, qu'il y ait ou non des gens de mer à bord.

La notion de drone maritime n'est cependant pas fonction des seules caractéristiques physiques de l'engin, mais tout autant des conditions précises de son exploitation (voir notamment l'article L.5000-2-2 du Code des transports[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

Les drones maritimes

Les drones maritimes prennent usuellement une appellation spécifique en fonction du milieu dans lequel ils évoluent[11] :

- *Unmanned Aerial Vehicles* (UAVs) ou drones aériens maritimes ;
- *Unmanned Surface Vehicles* (USVs) ou drones maritimes de surface ;
- *Unmanned Underwater Vehicles* (UUVs) ou drones sous-marins.

Il convient de noter que certains drones peuvent changer de milieu en fonction de leurs missions (par exemple : UAV vers USV, USV vers UUV), être porteurs d'autres types de drones (par exemple : USV porteur d'UUV ou d'USV) ou être portés par des navires autonomes.

Par ailleurs, les drones maritimes peuvent évoluer seuls, ou en flotte de plusieurs vecteurs, coordonnés par un drone-mère ou synchronisés entre eux.

Figure 1 : Exemple d'USV porteur d'UUV. Source : Thales

Les drones aériens (UAVs) évoluant dans un contexte maritime

Les drones aériens (UAVs) évoluant en environnement maritime mènent des missions diverses : surveillance maritime, recherche et sauvetage en mer, cartographie des côtes, surveillance de la pêche, surveillance de la pollution marine...

Ils ne sont pas considérés comme des drones maritimes et relèvent de la réglementation élaborée par la Direction Générale de l'Aviation Civile (DGAC) pour encadrer l'usage des drones aériens en France. Ils peuvent être pilotés à distance depuis un centre de contrôle terrestre ou un navire porteur, ou être programmés pour voler de manière autonome selon un itinéraire spécifique.

[11] Brochure « Drones et systèmes autonomes maritimes 2022 » du GICAN : https://gican.asso.fr/wp-content/uploads/2023/06/2022.10-GICAN-BROCHURE-MARITIME-DRONES-AUTONOMOUS-SOLUTIONS.pdf

Ces drones peuvent être classés selon leur taille :

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

Ou leur endurance, c'est-à-dire leur capacité à s'éloigner de leur base :

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

Les termes de MALE (*Medium Altitude, Long Endurance*) ou HALE (*High Altitude, Long Endurance*) peuvent également être trouvés dans la littérature.

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

Tableau 1 : Classification des UAVs d'après le département américain de la défense. Source : psu.edu[12]

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

• Les drones maritimes de surface (USVs)

Les drones maritimes de surface sont conçus pour fonctionner sur l'eau et être pilotés à distance pour diverses applications. Ces drones peuvent être utilisés pour une variété de tâches, telles que la surveillance maritime, la collecte de données océanographiques, la recherche dans le cadre d'opérations de sauvetage (détection et repérage, soutien aux sauveteurs), la cartographie des fonds marins, la protection de l'environnement marin, la lutte contre la pollution ou les actions de combat naval.

Les drones maritimes de surface sont souvent équipés de capteurs pour collecter des données sur l'environnement sous-marin, tels que des capteurs de température, de salinité, de profondeur et de turbidité de l'eau, ainsi que des caméras pour prendre des photos et des vidéos de la surface de l'eau et de la vie marine.

Ils peuvent être contrôlés à distance à partir d'un navire porteur, d'un centre de contrôle à terre ou d'un autre drone, et peuvent être programmés pour effectuer des missions spécifiques de manière autonome.

Les drones maritimes de surface offrent également un moyen efficace et économique pour surveiller et collecter des données sur les zones maritimes éloignées et difficiles d'accès.

Figure 2 : Exemple d'USV : le DriX d'Exail.[13]

• Les drones sous-marins (UUVs)

Les drones sous-marins sont conçus pour se déplacer sous l'eau et effectuer différentes tâches, telles que la recherche océanographique, la cartographie des fonds marins, l'inspection d'infrastructures sous-marines ou la surveillance de l'environnement marin. Équipés de sonars, caméras et capteurs de profondeur et d'effecteurs (bras robotisés, par exemple), ils offrent ainsi un moyen efficace et rentable d'opérer dans des zones sous-marines éloignées et difficiles d'accès.

Il convient de noter que les drones sous-marins téléopérés par connexion filaire (*Remotely Operated Vehicles* ou ROV) sont considérés comme des extensions des navires porteurs et relèvent de la réglementation applicable aux robots.

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

Les drones sous-marins peuvent être classés selon leur mode de déplacement et leur profondeur d'évolution (de quelques mètres à des milliers de mètres de profondeur) :

<table>
<tr><td colspan="2">Engins de surface : drones conçus pour évoluer à la surface de l'eau</td></tr>
<tr><td colspan="2">Engins plongeurs libres : drones qui utilisent la technique de la plongée libre pour se déplacer, c'est-à-dire qu'ils plongent ou remontent à la surface en utilisant leurs systèmes de flottaison et en modifiant leur densité. En revanche, ils ne disposent ni de moteur, ni d'hélice et ne peuvent donc pas se déplacer latéralement sous l'eau. Ces drones sont adaptés à des missions d'exploration autonome à des profondeurs relativement faibles.</td></tr>
<tr><td>Engins nageurs : drones qui utilisent des moteurs et des hélices pour se déplacer sous l'eau. Ils sont donc capables de se déplacer dans toutes les directions. Ces drones sont adaptés aux opérations nécessitant un déplacement rapide et précis sous l'eau.</td><td>Planeurs ou gliders : drones qui utilisent des ailes pour effectuer des glissements horizontaux et des variations de densité pour plonger et remonter à la surface. Ces drones sont adaptés à des explorations de longue durée[14].</td></tr>
<tr><td colspan="2">Engins de fond : drones équipés de roues ou de chenilles qui se déplacent sur des surfaces sous-marines (fond marin ou parois de pipelines).</td></tr>
</table>

Tableau 2 : Classification des drones sous-marins.

Figure 3 : Exemple d'engin de fond : le work class ROV HECTOR 7 opéré par Orange Marine.
Source : L. MIQUEL, Armateurs de France.[15]

[14] Les travaux actuels relatifs au décret d'application excluent les planeurs de la catégorie des drones maritimes.
[15] https://www.armateursdefrance.org/actualite/chapitre-2-journal-linfirmiere-bord-du-pierre-fermat-sonia-meriaux-avril-mai-2020

Contexte d'emploi

Le contexte d'emploi des drones maritimes et navals est particulièrement varié :

- Contexte naval : lutte contre les mines, patrouille de surface, aérienne, ou sous-marine, renseignement, action de l'État en mer, sauvegarde de la vie en mer, actions offensives, maîtrise et surveillance des fonds marins ;
- Contexte environnemental : mesures de paramètres environnementaux, lutte contre la pollution, mesures de pollution dans l'environnement marin, surveillance maritime et lutte contre la pêche illicite ;
- Contexte scientifique : mesures hydrographiques et océanographiques, recherche archéologique, suivi de la biodiversité ;
- Plongée sous-marine : l'emploi du drone permet de prolonger l'autonomie temporelle et spatiale des plongées et d'éviter les risques pour les hommes ;
- Construction et maintenance : sondages, travaux (EMR, offshore), pose et maintenance de câbles sous-marins (télécommunication, énergie), inspection et maintenance de coques de navires et d'ouvrages portuaires, surveillance de sites ou de zones.

Contraintes

Du fait de leur contexte d'emploi, les drones sont soumis à des besoins et à des contraintes physiques et environnementales particulièrement importantes dans leur conception et leur emploi :

- Positionnement 2D/3D précis, notamment sous-marin et en environnement dégradé ;
- Prévention des collisions (avec les autres usagers en mer, le fond, des obstacles, le navire porteur ou d'autres drones) ;
- Evolution précise dans un environnement où les contraintes physiques sont importantes et variables (courant, température, vent, vagues...) ;
- Détection de l'environnement aérien, en surface et sous l'eau à courte, moyenne et longue portée suivant les cas et les conditions de propagation ;
- Collecte et stockage sécurisés à bord des données ou éléments captés dans le cadre de la mission ;
- Télécommunications sécurisées haut débit par radiofréquence, par satellite ou par signal acoustique avec le navire porteur, la terre ou d'autres drones, pour assurer la télécommande, la transmission bilatérale d'informations relatives à la mission, en temps quasi-réel ou différé, les opérations de maintenance, etc., avec une difficulté particulière dans le cadre d'opérations sous-marines ;
- Autonomie et maîtrise des dépenses d'énergie ;
- Survivabilité à bord en cas d'embarquement de personnel (cas des navires autonomes de degrés 1 et 2) ;
- Fonctionnement sous fortes contraintes physiques environnementales : pression, corrosion ;
- Résilience en cas de panne.

Des engins autonomes ou semi-autonomes maritimes sont déjà largement utilisés dans les contextes maritimes ou navals.

Les navires autonomes

L'OMI a proposé une catégorisation des navires autonomes, Maritime Autonomous Surface Ships (MASS) selon leur degré d'autonomie[16]. Ces quatre degrés d'autonomie proposés par l'OMI sont issus d'un travail de comparaison réglementaire mené en 2021.

Degré	Signification
1er	Le navire utilise des processus automatisés avec une capacité de décision autonome : les marins présents à bord opèrent et contrôlent les systèmes et fonctions du navire, certaines pouvant être automatisées et parfois non supervisées. Les marins à bord sont prêts à reprendre la main en cas de besoin.
2ème	Le navire est contrôlable à distance, mais dispose toujours de marins à bord : le navire est contrôlé et opéré depuis une position distante, mais les marins présents à bord peuvent prendre le contrôle du navire et opérer les systèmes embarqués en cas de besoin.
3ème	Aucune présence humaine à bord : le navire est totalement contrôlé à distance.
4ème	Les navires sont totalement autonomes : le système d'exploitation du navire prend des décisions et détermine ses actions en toute autonomie.

Tableau 3 : Regroupement des navires autonomes selon leur degré d'autonomie. Source : OMI.

Les degrés d'autonomie ne sont pas destinés à jouer un rôle structurant dans le projet de code MASS, notamment car les conditions d'exploitation des navires autonomes peuvent être variables et amener un engin à évoluer selon plusieurs niveaux d'autonomie. Ainsi, lors du comité MSC.107 de juin 2023, il a été proposé de remplacer la notion de « degré d'autonomie » par celle de « mode opératoire », qui apparaît plus cohérente avec la réalité de l'utilisation des navires autonomes[17].

• Contexte d'emploi

Les contextes d'emploi des navires autonomes sont, là aussi, particulièrement riches :

- Transport de marchandises : containers ou en vrac (solides ou liquides), aujourd'hui essentiellement dans un contexte littoral, portuaire ou fluvial ;
- Transport de passagers et de véhicules, aujourd'hui sur de courtes distances ;
- Opérations portuaires : remorqueur, pousseur ;
- Opérations navales : navires de combat.

En prenant l'exemple de la convention SOLAS[18] ou de la convention sur le règlement international pour prévenir les abordages en mer (COLREG)[19], il paraît difficile voire impossible, en l'état actuel, d'employer un navire autonome dans le cadre d'une navigation internationale.

[16] http://www.imo.org/en/MediaCentre/HotTopics/Pages/Autonomous-shipping.aspx : il convient de noter que cette définition devrait faire l'objet d'une révision à l'été 2023.
[17] https://www.imo.org/fr/MediaCentre/MeetingSummaries/Pages/MSC-107th-session.aspx
[18] https://www.imo.org/fr/About/Conventions/Pages/International-Convention-for-the-Safety-of-Life-at-Sea-(SOLAS),-1974.aspx
[19] https://www.imo.org/fr/about/Conventions/Pages/COLREG.aspx

En effet, le chapitre V de la convention SOLAS requiert que tout navire ait à bord un équipage suffisant pour assurer sa sécurité, ou pour porter assistance à un navire en difficulté : les navires autonomes de degré 3 et 4 ne pourront pas respecter cet impératif. De même, s'agissant de COLREG, sa règle 5 précise que « tout navire doit en permanence assurer une veille visuelle et auditive appropriée, en utilisant également tous les moyens disponibles qui sont adaptés aux circonstances et conditions existantes, de manière à permettre une pleine appréciation de la situation et du risque d'abordage ».

Les navires autonomes sont encore largement en phase d'expérimentation : même si aucun frein technologique majeur ne demeure, comme l'ont montré diverses expérimentations et mises en œuvre (Yara Birkeland[20], ROSS[21], SVAN[22]), les contraintes réglementaires, économiques voire sociales peuvent peser sur une exploitation plus systématique.

• Contraintes

Les contraintes liées aux navires autonomes sont variées :

- Positionnement 2D/3D précis, notamment en environnement dégradé ;
- Prévention des collisions (avec le fond, avec des obstacles, avec les autres navires, autonomes ou non) ;
- Evolution précise dans un environnement où les contraintes physiques sont importantes et variables (courant, température, vent, vagues…) ;
- Détection de l'environnement en surface à courte, moyenne et longue portée ;
- Collecte et stockage sécurisés à bord des données ou éléments captés dans le cadre de la mission ;
- Télécommunication sécurisée haut débit avec la terre ou d'autres drones, pour assurer la télécommande, la transmission bilatérales d'informations relatives à la mission, en temps quasi-réel ou différé, les opérations de maintenance, etc. ;
- Autonomie et maîtrise des dépenses d'énergie ;
- Survivabilité à bord en cas d'embarquement de personnel ;
- Résilience en cas de panne.

Architecture d'ensemble et fonctionnelle des drones et navires autonomes

L'architecture d'ensemble des drones maritimes et navires autonomes peut, de manière générique, être séparée en plusieurs modules :

- Les stations terrestres (voire embarquées), qui peuvent être en charge du pilotage de l'équipement (ROV, MASS 2ème et 3ème degrés) ou de la préparation et du suivi de leur mission ;
- Les systèmes de télécommunication (satellite ou radio), permettant la communication avec le navire porteur ou la station à terre ;
- Les ensembles de capteurs (positionnement, RADAR, LIDAR, caméras, laser, sonars, etc.)
- Les ensembles d'actionneurs (propulsion, navigation, flottaison, gestion de l'énergie, etc.)
- Le système numérique de gestion de l'ensemble.

[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

Plus précisément, et suivant son niveau d'autonomie et le type de mission :

- Le drone maritime ou navire autonome est chargé d'une mission qu'il réalise, soit en suivant une route donnée, soit en navigant de manière partiellement ou totalement autonome ;
- Pour se guider, il obtient des références géographiques de capteurs de type PNT (Position, Navigation, Temps) et adapte également son attitude de navigation en fonction de paramètres environnementaux (puissance disponible, état de la mer) et de la situation surface, par exemple (présence d'autres navires, etc.) ;
- Il agit pour faire évoluer sa navigation sur ses actionneurs (propulsion, barre), en adaptant leur efficacité en fonction des conditions environnementales ;
- Il réalise, en parallèle, ses missions spécifiques éventuelles non directement liées au comportement du porteur ;
- L'ensemble de la coordination et de la réalisation de la mission est généralement porté par un ou plusieurs calculateurs coordinateurs redondants et spécifiques (par exemple : un calculateur pour le porteur, un calculateur pour la mission).

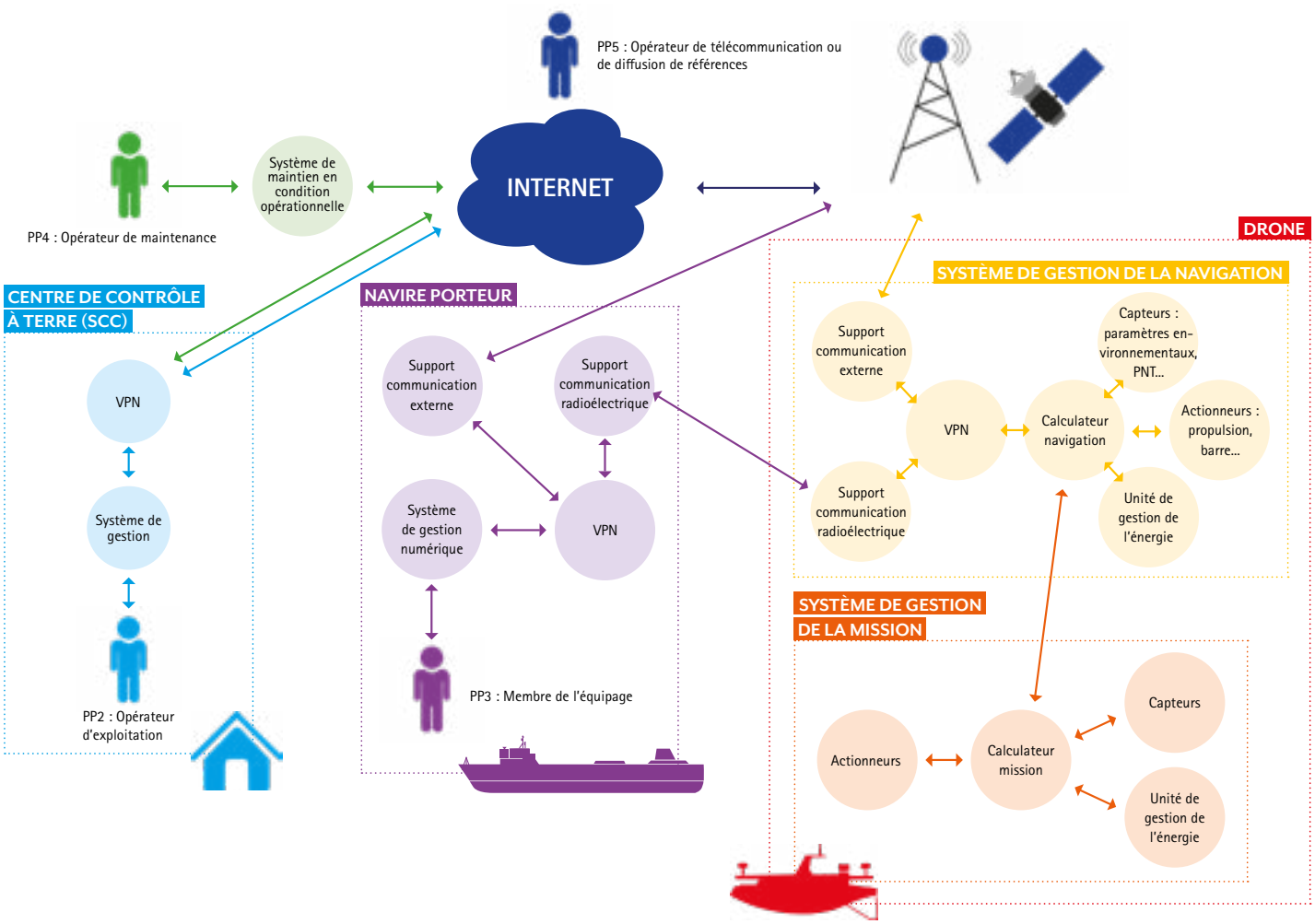


Figure 4 : Schéma d'architecture d'ensemble et fonctionnelle des drones maritimes et des navires autonomes.

DRONES MARITIMES ET NAVIRES AUTONOMES : VULNÉRABILITÉS ET SCENARIOS DE MENACE

Réglementation et meilleures pratiques applicables

Avant d'évoquer les vulnérabilités et scénarios de menace, il convient d'évoquer la réglementation qui pourrait s'appliquer aux drones maritimes et navires autonomes en termes de cybersécurité.

Au niveau international, les objectifs du Code international de gestion de la sécurité (*International Safety Management Code*, ISM)[23] consistent à définir des pratiques d'exploitation permettant d'opérer dans un environnement de travail sans danger, à évaluer tous les risques identifiés pour les navires, leur personnel et l'environnement, à établir des mesures de précaution appropriées et à améliorer constamment les compétences du personnel à terre et à bord des navires. A ce titre et en complément, la Résolution MSC.428(98)[24] de l'OMI, relative à la gestion des cyber-risques maritimes dans le cadre des systèmes de gestion de la sécurité, a été adoptée en 2017.

Ce code pourrait s'appliquer aux navires autonomes, en fonction de leur taille et de leur contexte d'emploi. Cependant, l'absence de personnel à bord sur des navires à degré d'autonomie fort nécessiterait une adaptation des modalités pratiques d'application de la résolution. Le futur code MASS (*Maritime Autonomous Surface Ship*) de l'OMI, qui devrait être promulgué en 2025 pour devenir contraignant en 2028, voire 2029 au plus tard, pourrait inclure des mesures spécifiques adaptées relatives à la cybersécurité pour les navires autonomes.

Au niveau européen et français, la Loi de Programmation Militaire (LPM) et le statut d'Opérateur d'Importance Vitale (OIV) exploitant des Systèmes d'Information d'Importance Vitale (SIIV) pourrait s'appliquer aux armateurs et opérateurs mettant en œuvre des systèmes de drones maritimes et de navires autonomes en fonction des critères d'application et de déclaration spécifiques à la Loi de Programmation Militaire suivant le secteur d'activité concerné[25].

Le Parlement européen et le Conseil de l'Union européenne ont adopté, en juillet 2016, la directive concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, également appelée directive NIS (*Network and Information Security*[26]). Transposée en droit français en 2018, cette directive avait pour objectif d'augmenter le niveau de cybersécurité des acteurs majeurs de dix secteurs d'activité regroupant notamment le transport maritime. Avec ce premier dispositif, les grands acteurs de ces secteurs d'activités, reconnus comme Opérateurs de Service Essentiel (OSE), ont été soumis à l'obligation de déclarer leurs incidents de sécurité à l'ANSSI, de mettre en œuvre les mesures de sécurité préventives nécessaires pour réduire fortement l'exposition de leurs systèmes les plus critiques aux risques cyber, mais aussi d'être en capacité de réagir de manière adéquate en cas d'incident.

[23] https://www.imo.org/fr/OurWork/HumanElement/Pages/SafetyManagement-Default.aspx
[24] Résolution MSC.428(98) adoptée le 16 juin 2017 pour la gestion des cyber-risques maritimes dans le cadre des systèmes de gestion de la sécurité : https://wwwcdn.imo.org/localresources/fr/OurWork/Security/Documents/MSC%2098-23-Add.1.pdf
[25] Voir notamment https://www.ssi.gouv.fr/administration/protection-des-oiv/protection-des-oiv-en-france/
[26] https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016L1148

En 2022, la directive NIS 2 a été adoptée[27] par le parlement et le conseil européens. Elle élargit les objectifs et le périmètre d'applicabilité pour apporter davantage de protection par rapport à la première version de la directive.

La version 2 de cette Directive permettra d'inclure de nouveaux acteurs du secteur maritime, et notamment des opérateurs ou concepteurs de drones maritimes et navires autonomes mais aussi, de manière plus explicite pour sa transposition en droit français, les centres de téléopération. Aucune des versions de la Directive n'intègre cependant les navires, qui en sont même explicitement exclus. Cette Directive ne serait donc pas non plus applicable aux drones maritimes et navires autonomes pour le statut d'Entité Essentielle (EE), à l'exception des centres de contrôle à terre.[28]

La Direction Générale des Affaires Maritimes, de la Pêche et de l'Aquaculture (DGAMPA) élabore les textes d'application de l'ordonnance n°2021-1330, notamment le projet de décret modifiant le décret n° 84-810 du 30 août 1983 sur le régime applicable aux navires autonomes et aux drones maritimes[29]. Ce décret sera complété par des arrêtés techniques qui préciseront les dispositions relatives à la cybersécurité, en particulier pour ce qui concerne les équipements de sécurité.

Au niveau sectoriel français, le Cluster Maritime Français a émis en juin 2020 un « Guide de bonnes pratiques relatives aux drones maritimes », qui évoque le sujet de la cybersécurité[30]. Ce guide émet les recommandations suivantes, notamment en s'appuyant sur le cadre de cybersécurité proposé par l'organisme américain *National Institute of Standards and Technology* (NIST)[31] :

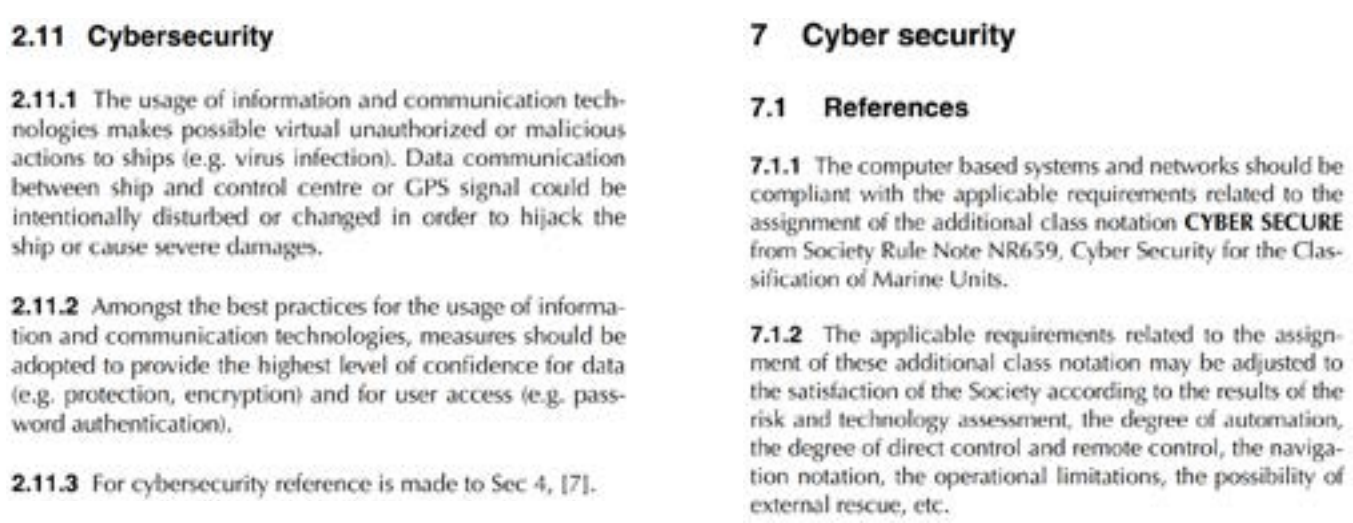
13.7.1	La protection des systèmes d'information impliqués dans les fonctions de sécurité d'un drone maritime doit être assurée autant que possible afin de préserver la confidentialité, l'intégrité et la disponibilité des informations. En particulier, il est recommandé de mener une analyse des risques relatifs à la modification des données (par erreur d'une personne autorisée ou par malveillance d'une personne non autorisée), à leur utilisation abusive ou à l'interdiction involontaire de leur accessibilité.
13.7.2	Même si les dispositions de la Directive NIS ne s'appliquent pas aux navires, les fabricants, exploitants et/ou opérateurs doivent conduire des audits et apporter les mesures correctives nécessaires pour assurer une exploitation en toute sécurité. En particulier, sur la base de l'étude des risques cyber, il s'agit de : • Identifier : préciser les rôles du personnel et les responsabilités pour le management des systèmes d'information, et identifier les risques qui pèsent sur les différents éléments du système et peuvent compromettre la sécurité ou les opérations ; par exemple, le risque qu'un tiers accède par erreur au système de contrôle-commande du drone • Protéger : implanter les mesures de protection et de contingence contre les risques identifiés et permettre la continuité des opérations ; par exemple, disposer de mots de passe d'accès contrôlé au système • Détecter : développer et implanter les moyens de détecter un événement cyber en temps utile ; par exemple repérer une nouvelle connexion au système d'information • Répondre : mettre en place les mesures permettant de réagir à l'événement et maintenir les fonctions essentielles du système ; par exemple, bloquer les accès • Recouvrer : mettre en place les mesures de sauvegarde et de restauration du système ; par exemple, disposer d'une version de référence du logiciel pouvant être réinstallée.

Tableau 4 : Recommandations de cybersécurité pour les drones maritimes
Source : Cluster Maritime Français.

[27] Voir https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32022L2555&qid=1689168337809
[28] Voir notamment https://www.ssi.gouv.fr/administration/reglementation/directive-nis/nis-un-dispositif-de-cybersecurite-pour-les-operateurs-de-service-essentiel/
[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

Les sociétés de classification ont émis plusieurs guides et recommandations relatives aux navires autonomes. On peut notamment citer :

- La note NI 641 DT R01 E de BUREAU VERITAS « *Guidelines for autonomous shipping* », qui fait notamment référence à la cybersécurité et prévoit, pour les unités couvertes par cette note, l'application des prescriptions de la NR659 applicables pour la notation de classe additionnelle CYBER SECURE.[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 : Recommandations issues de la note NI 641 DR R01E. Source : BUREAU VERITAS.

- La note NR 659 DT R02 de BUREAU VERITAS de janvier 2023[33] qui, même si elle ne fait pas directement référence aux drones maritimes ou navires autonomes, est en grande partie applicable et adaptée pour répondre aux enjeux et contraintes spécifiques de ces engins.
- Les UR E26 et E27 publiés par l'*International Association of Classification Societies* (IACS)[34] qui entreront pour leur part en service le 1er janvier 2024 pour les constructions neuves.

En décembre 2017, le Lloyd's Register a émis un document « *Cyber-enabled ships: ShipRight procedure assignment for cyber descriptive notes for autonomous & remote access ships* »[35].

Enfin, sans les citer, de nombreux articles de recherche, en France comme à l'étranger, évoquent le sujet de la cybersécurité des drones maritimes et navires autonomes, tant sous l'aspect analyse de risques que sur des réponses techniques envisageables.

On pourra notamment citer les travaux de l'École nationale supérieure maritime (ENSM) sur le sujet dans le cadre du projet de recherche Sea4M[36], ainsi qu'un article de recherche[37] du centre d'excellence de l'OTAN sur la cybersécurité (*NATO Cooperative 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 et 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/projet-recherche-ensm-sea4m/
[37] https://ccdcoe.org/uploads/2022/09/Cybersecurity_Considerations_in_Autonomous_Ships.pdf

Besoins de sécurité

Les drones maritimes et navires autonomes cumulent les besoins de sécurité des navires plus classiques[38], dont ils reprennent souvent nombre de protocoles et d'équipements divers (capteurs, actionneurs, systèmes de télécommunication, systèmes PNT...).

A ceux-ci s'ajoutent de nouveaux besoins liés aux particularités des équipements autonomes, à savoir :

- une dépendance plus forte aux systèmes de télécommunication, notamment satellitaires, dont la disponibilité, l'intégrité et la confidentialité deviennent bien souvent essentielles, lorsque le degré d'autonomie est faible, ou lorsque la mission impose des échanges fréquents avec la terre ;
- l'importance de la confiance accordée aux capteurs électroniques, visuels et sonores, qui doivent être particulièrement intègres et, là aussi, disponibles ;
- enfin, le fort recours à l'algorithmie dans la prise de décision et, de manière plus générale, dans la conduite du navire et de ses installations.

A cela, il convient également de rappeler le risque physique : si arraisonner un navire avec du personnel à bord a été – historiquement – un risque majeur et qu'il le demeure dans certaines zones de navigation, sa réalisation peut s'avérer hasardeuse et dangereuse. Le risque de capture d'un drone maritime ou navire autonome fait également encourir des risques sur la confidentialité des systèmes d'information (rétro-ingénierie, recherche de vulnérabilités, capture d'informations sensibles, compromission du lien montant...). Outre la sécurité du drone maritime, du navire autonome et du *Shore Control Center*, leur sûreté constitue également un enjeu majeur.

Analyse de risques

Tout d'abord, il est intéressant de noter que le secteur maritime et naval n'est pas le seul à s'intéresser à la cybersécurité des véhicules autonomes. Des parallèles intéressants et des études et projets communs pourraient être menés avec des secteurs comme le secteur des transports par voie routière ou avec le transport aérien et ce, même si le contexte maritime et les contraintes qu'il supporte sont particulières.

L'objectif de ce paragraphe n'est pas de réaliser une analyse de risques exhaustive pour les drones et navires autonomes, mais de présenter les grands principes à respecter pour mener ce type de démarche ainsi que les principaux scénarios d'attaque de haut niveau à considérer, appelés scénarios stratégiques.

Si la gestion des risques cyber doit être prise en compte dans des démarches plus globales de maîtrise des risques, par exemple dans le cadre des démarches liées à l'immatriculation, les méthodologies éprouvées et spécifiques à la cybersécurité doivent être appliquées.

Quelques points importants sont à souligner avant de dérouler une analyse de risques cyber sur ce type de systèmes :

1. Les drones maritimes et navires autonomes peuvent être autonomes par conception. Il peut aussi s'agir de navires plus ou moins anciens sur lesquels une composante d'autonomie est rajoutée, soit à des fins d'expérimentation, soit de production, même si ce cas semble moins probable. En effet, les navires autonomes « gagnent » en efficacité et en rentabilité lorsque les systèmes, les locaux et les infrastructures liés à la vie à bord sont supprimés, ce qui entraîne un gain important, notamment en poids et en consommation d'énergie.

[38] Les vulnérabilités des navires plus classiques sont notamment identifiées dans le guide publié par BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF et WORLD SHIPPING COUNCIL pour la prise en compte de la cybersécurité à bord des navires : https://www.bimco.org/-/media/bimco/about-us-and-our-members/publications/ebooks/guidelines-on-cyber-security-onboard-ships-v4.ashx

2. Le traitement cyber à réaliser dans les deux cas diffère assez fortement car, si dans le premier cas, la cybersécurité doit être intégrée par conception, dans le second, les systèmes déjà présents à bord, potentiellement anciens et peu sécurisés, doivent être interconnectés à des installations de contrôle et de pilotage autonomes. Dans ce cas, l'analyse de risques est particulièrement importante, car l'élongation de ces systèmes ou leur accessibilité depuis la terre présente un risque important.

• Périmètre de l'analyse de risques

Il est essentiel que l'analyse de risques réalisée ne se limite pas au seul système navigant à proprement parler, mais englobe aussi le(s) centre(s) de contrôle à terre (*Shore Control Center*, SCC), les navires porteurs – ou ceux depuis lesquels les drones sont opérés - ainsi que les moyens d'élongation par satellite, par exemple. De même, les opérations de maintenance présentent un risque important de compromission pour ce type d'équipement : les personnes, processus et outils associés doivent faire l'objet d'une attention particulière afin de réduire le risque d'attaques liées à la chaîne logistique également appelées « *Supply Chain Attacks* ». C'est donc **l'écosystème complet du drone maritime/navire autonome qui doit être pris en compte.**

Le périmètre métier et technique de l'analyse de risques est précisé en Annexe 1, au travers de la définition des missions des drones et navires autonomes, de leurs valeurs métier (c'est-à-dire les informations et processus importants qu'il convient de protéger), des biens supports associés (éléments techniques sur lesquels reposent les valeurs métiers) et des évènements redoutés.

• Scénarios stratégiques

Les scénarios stratégiques (SS) suivants pourraient être retenus sur la base de l'analyse de risques réalisée :

- **SS1 – Un acteur de type cybercriminel réalise une attaque par rançongiciel du système de gestion du centre de contrôle à terre**

  Ce scénario correspond à une attaque par rançongiciel du système de gestion du centre de contrôle à terre entraînant une perte de communication avec le drone maritime ou navire autonome et une interruption de la mission, afin d'obtenir le paiement d'une rançon. Ce scénario correspond aux évènements redoutés ER7 et ER11 (cf. Annexe 1). Pour atteindre son objectif, le groupe cybercriminel serait susceptible de passer par plusieurs chemins d'attaques :

  - Attaque directe du système de gestion en exploitant une vulnérabilité logicielle accessible depuis Internet ou en se connectant avec des identifiants légitimes à un service d'accès à distance (par exemple : réseau privé virtuel) ;

  - Attaque par courriel de harponnage (*spearphishing*) d'un opérateur d'exploitation et récupération d'identifiants légitimes ;

- **SS2 : Un acteur étatique ou pseudo-étatique sabote le drone maritime ou le navire autonome en mission**

  Ce scénario correspond au sabotage par un groupe étatique ou pseudo-étatique des systèmes de gestion d'un drone maritime ou d'un navire autonome (navigation et mission), afin de perturber, voire empêcher, la mission assurée par le drone maritime ou le navire autonome. Ce scénario correspond aux évènements redoutés ER8, ER9, ER10, ER11, ER12 et ER13 (cf. Annexe 1). Pour atteindre son objectif, l'acteur serait susceptible de passer par plusieurs chemins d'attaques :

  - Perturbation par leurrage, brouillage des informations reçues par les capteurs du drone ou navire autonome (GNSS, AIS, RADAR, liaisons satellitaires etc.) ou destruction logique ou physique des équipements associés ;

  - Attaque directe des systèmes de gestion du drone maritime ou du navire autonome en exploitant une vulnérabilité accessible depuis Internet ou en se connectant avec des identifiants légitimes à un service d'accès distance (opération, maintenance, etc.).

- **SS3 : Un acteur étatique se pré-positionne sur le drone maritime ou le navire autonome en phase de maintenance**

  Ce scénario correspond au pré-positionnement d'un acteur étatique sur les systèmes de gestion d'un drone maritime ou d'un navire autonome (navigation et mission) lors des phases de maintenance, afin de compromettre le drone maritime ou le navire autonome et sa mission ou de réaliser une opération d'espionnage économique et stratégique (vol des données captées durant la mission ou de celles relatives à l'architecture ou la programmation du drone maritime ou du navire autonome). Ce scénario correspond aux évènements redoutés ER1, ER3, ER4, ER6, ER7, ER8, ER9, ER10, ER11, ER12 et ER13 (cf. Annexe 1). Pour atteindre son objectif, l'acteur étatique serait susceptible de passer par plusieurs chemins d'attaques :

  - Attaque du SI du mainteneur externe ou du SI de gestion du centre de contrôle à terre (si la maintenance est assurée en interne) en exploitant une vulnérabilité présente sur un équipement exposé à Internet ou en se connectant avec des informations de connexion légitimes à un service d'accès à distance, avant de rebondir vers les systèmes de gestion du drone maritime ou du navire autonome ;

  - Attaque par courriel de harponnage (*spearphishing*) d'un opérateur de maintenance (interne ou externe) ;

  - Attaque de la chaîne d'approvisionnement pour compromettre les mises à jour et rebondir ensuite vers les systèmes de gestion du drone maritime ou du navire autonome.

- **SS4 : Terroriste – Sabotage du drone maritime ou du navire autonome en phase de conception**

  Ce scénario correspond au sabotage par un concurrent ou un tiers agissant pour un concurrent des algorithmes de calcul et de prise de décision du drone maritime ou du navire autonome en phase de conception, dans l'objectif de créer un incident grave lors de sa mise en service afin de le décrédibiliser. Ce scénario correspond aux évènements redoutés ER3, ER7, ER8 et ER10 (cf. Annexe 1). Pour atteindre son objectif, le concurrent serait susceptible de passer par plusieurs chemins d'attaques :

  - Attaque directe du SI du concepteur accessible par Internet en exploitant une vulnérabilité accessible depuis Internet ou en se connectant avec les informations de connexion légitimes à un service d'accès à distance

  - Attaque par courriel de harponnage (*spearphishing*) d'un employé du concepteur

  - Attaque en exploitant la relation de confiance avec un sous-traitant pour rebondir sur le SI du concepteur

- **SS5 : Acteur étatique – Vol des plans ou des données relatifs à un projet de drone maritime ou de navire autonome**

  Ce scénario correspond au vol par un acteur étatique des plans ou des données relatifs à un projet de drone maritime ou de navire autonome à des fins d'espionnage stratégique et économique. Ce scénario correspond aux évènements redoutés ER2 et ER5 (cf. Annexe 1). Pour atteindre son objectif, le concurrent serait susceptible de passer par plusieurs chemins d'attaques :

  - Attaque directe des SI de la chaîne d'approvisionnement (concepteurs, équipementiers, intégrateurs) en exploitant une vulnérabilité accessible par Internet ou en se connectant avec des identifiants légitimes à un service d'accès à distance

  - Attaque par courriel de harponnage (*spearphishing*) d'un employé de la chaîne d'approvisionnement.

DRONES MARITIMES ET NAVIRES AUTONOMES : RECOMMANDATIONS DE CYBERSECURITÉ

Comme il est d'usage en matière de cybersécurité, une mesure seule est bien souvent contournable et donc insuffisante pour pallier une cyber attaque. Il est donc nécessaire de suivre une démarche de défense en profondeur, en mettant en œuvre des mesures complémentaires et cohérentes réglementaires, organisationnelles, humaines et technologiques[39].

Comme cela a déjà été évoqué, ces mesures sont plus efficaces lorsqu'elles sont prévues et définies dès la phase de conception du drone maritime ou du navire autonome. Leur application peut parfois prendre du temps ou représenter un investissement financier de la part de l'organisation qui les met en place. Il est bien souvent nécessaire de rechercher un soutien et une expertise extérieure.

Ce Livre blanc propose une sélection de mesures dont la mise en œuvre peut s'avérer efficace pour lutter face à des menaces cyber étatiques, cybercriminelles, terroristes ou activistes. Ces mesures, assez spécifiques au contexte d'emploi évoqué, ne se substituent pas à la mise en œuvre des mesures prévues par le référentiel réglementaire à appliquer par l'opérateur. Les mesures citées ne sont également pas toutes de la responsabilité de l'armateur ou de l'opérateur. Elles concernent la gouvernance, la protection, la détection/réaction et la résilience.

Le premier effet recherché est d'intégrer la cybersécurité dans la gouvernance des systèmes de drones maritimes et de navires autonomes. Huit mesures sont proposées dans le cadre de ce Livre blanc.

Figure 6 : Recommandations de cybersécurité relatives à la gouvernance.

[39] Concept de défense en profondeur appliquée aux systèmes d'information de l'ANSSI : https://www.ssi.gouv.fr/uploads/IMG/pdf/mementodep-v1-1.pdf

Le second effet recherché est d'assurer la défense en profondeur des systèmes de drones maritimes et navires autonomes. Treize mesures associées ont été identifiées.

Figure 7 : Recommandations relatives à la protection des systèmes.

Le troisième effet est relatif à la capacité de détecter et de réagir en cas d'alerte cyber.

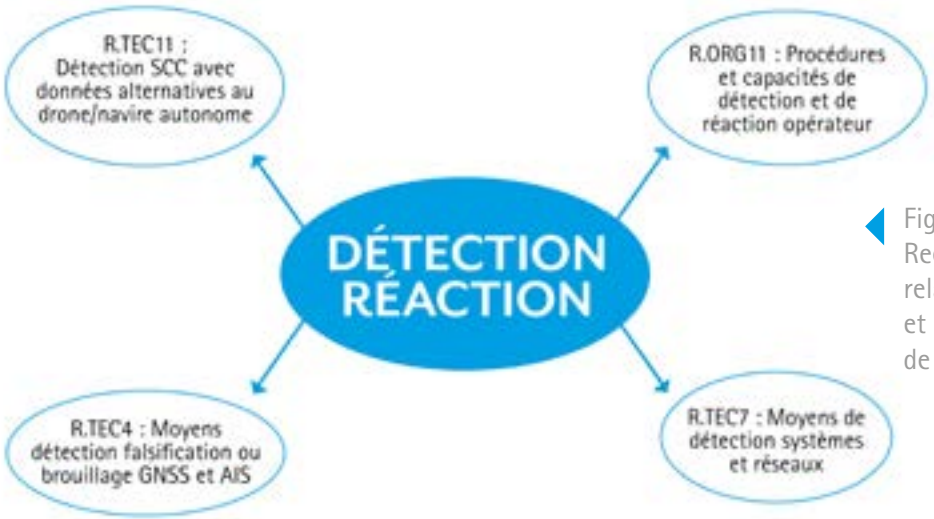


Figure 8 : Recommandations relatives à la détection et à la réaction en cas de cyber attaque.

Enfin, le dernier effet concerne la résilience des systèmes considérés.

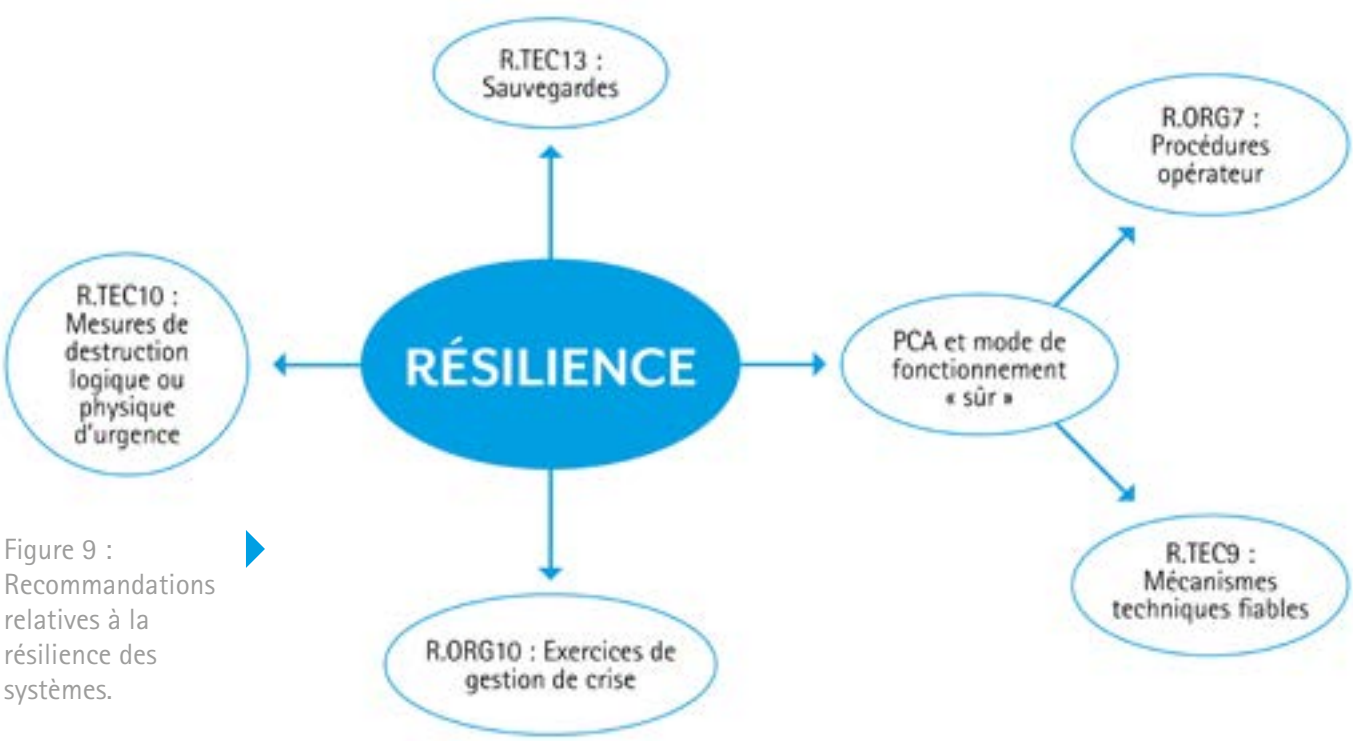


Figure 9 : Recommandations relatives à la résilience des systèmes.

Recommandations organisationnelles (R. ORG)

R. ORG1 : Afin d'identifier les risques associés aux drones maritimes et navires autonomes, une analyse de risques sur l'ensemble du périmètre du système d'information du drone maritime / navire autonome et des parties prenantes devra être réalisée. Cette analyse, et les mesures qui en découlent, devront prendre en compte et rester rationnelles vis-à-vis du degré d'autonomie et les valeurs métiers supportées par les systèmes d'information. Cette analyse de risques cyber pourra s'appuyer sur les éléments issus du présent document (scénarios stratégiques, notamment), de même que sur les meilleures pratiques en la matière, notamment issues des guides rédigés par l'ANSSI.[40]

R. ORG2 : En fonction de l'aversion au risque et du contexte d'emploi des drones maritimes et navires autonomes, il apparaît essentiel qu'une démarche d'homologation de cybersécurité de ces systèmes soit menée par une autorité qualifiée.[41] Une intégration de la cybersécurité dès la conception, et tout au long du cycle de vie, réduira les coûts induits.[42] Le recours à une certification auprès d'une société de classification pourra être envisagé.

R. ORG3 : Des audits et tests d'intrusion réguliers devront être réalisés sur l'ensemble de l'écosystème des drones maritimes et navires autonomes, en phase de conception comme en phase d'exploitation.

R. ORG4 : Des processus et modalités de maintien en condition de sécurité devront être formalisés et mis en œuvre afin de réduire les occurrences ou conséquences d'une cyber attaque à un niveau acceptable par l'autorité d'homologation. Tout particulièrement, l'attention sera portée sur les risques d'obsolescence numérique au sein des différents systèmes.

[40] https://www.ssi.gouv.fr/administration/management-du-risque/la-methode-ebios-risk-manager/
[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 : Une attention particulière sera portée sur la couverture assurantielle des opérations et plateformes autonomes vis-à-vis du risque cyber.

R. ORG6 : Les procédures mises en œuvre par l'opérateur du drone maritime/navire autonome doivent prévoir un retour à un mode de fonctionnement « sûr » en cas de dysfonctionnement ou d'anomalie majeure.

R. ORG7 : Une cartographie logicielle et matérielle exhaustive de l'ensemble des composants numériques du drone maritime/navire autonome et de son écosystème, dont le centre de contrôle à terre, sera réalisée et maintenue à jour. Cette cartographie pourra s'appuyer sur les bonnes pratiques existantes en la matière[43].

R. ORG8 : Le centre de contrôle à terre, ou tout organisme à terre équivalent étant des organes particulièrement sensibles de la chaîne de commande et de contrôle du drone maritime / navire autonome, une attention toute particulière sera portée sur l'organisation de sa cybersécurité, sur sa protection physique et logique en profondeur et sur les processus et opérations de maintenance qui y sont réalisés, ainsi que sur ses éventuelles dépendances externes (VPN, routage, connexion satellitaire, recours à l 'informatique en nuage, etc.).

R. ORG9 : Des exercices de gestion de crise cyber, adaptés au contexte spécifique du drone maritime / navire autonome seront réalisés régulièrement. Ils devront couvrir l'ensemble du périmètre (dont le centre de contrôle à terre), des acteurs (superviseurs, téléopérateurs, mainteneurs) et s'appuyer sur des scénarios réalistes et actualisés en fonction de la menace.

R. ORG10 : L'organisme opérant le système devra disposer de modalités et de moyens internes ou externes d'analyse, d'investigation et de réaction en cas d'incident cyber. Ces moyens devront couvrir les phases d'anticipation, d'alerte et de coordination de la réponse à incident (recours à un *Computer Emergency Response Team*), de surveillance temps-réel (*Security Operations Center*), et de réponse à incident. Dans la mesure où cela s'avère nécessaire ou réglementaire, en raison de la criticité de la mission effectuée par le drone, le recours à des prestataires qualifiés par l'ANSSI (Prestataire de Détection d'Incident de Sécurité/Prestataire de Réponse à Incident de Sécurité) sera recherché.

R. ORG11 : Les mesures organisationnelles, humaines et techniques de sécurité informatiques mises en œuvre par l'opérateur, pour réduire les risques devront être formalisées dans une Politique de Sécurité des Systèmes d'Information (PSSI) particularisée notamment au drone maritime/navire autonome, à ses installations, ses interfaces et sa maintenance. Cette PSSI définira notamment les procédures d'intégration de système, de contrôle d'accès, de gestion des mots de passe, de maintien en condition de sécurité et de gestion d'incidents (des incidents comme la perte de données, la modification non autorisée de données ou de logiciels, l'installation de logiciels non autorisées, la connexion à des systèmes ou des appareils non sécurisés, etc.). Par ailleurs, des indicateurs de suivi de la réalisation des mesures de la PSSI devront être définis et suivis, afin de vérifier son efficacité dans le temps et de faire évoluer certaines de ses mesures ou les renforcer si nécessaire.[44]

R. ORG12 : Afin de garantir la bonne prise en compte des enjeux de sécurité par l'écosystème du drone maritime ou du navire autonome, des clauses de sécurité devront être prévues dans les contrats conclus avec les différentes parties prenantes. Ces clauses spécifieront notamment les exigences en matière d'audit/de test d'intrusion, de maintien en condition de sécurité, de cartographie, de gestion de crise et de sensibilisation/formation/entraînement. Par ailleurs, ces contrats devront exiger la fourniture de Plans d'Assurance Sécurité (PAS) dans lesquels seront décrites les dispositions prises par les tiers pour respecter les clauses de sécurité.

R. ORG13 : Une politique de protection du patrimoine informationnel de l'écosystème du drone maritime ou du navire autonome devra être définie. Elle précisera pour chacun des niveaux de protection et/ou de classification de l'information les mesures de protection associées sur toutes les phases de cycle de vie de l'information. Un chiffrement des données les plus sensibles en confidentialité devra être notamment prévu. Par ailleurs, cette politique de classification veillera à prendre en compte les obligations réglementaires éventuelles liées à la protection du secret de la défense nationale ou aux données à caractère personnel (architecture, technologies, logiciels, matériels, paramètres). Pour cela, plusieurs guides pourront être utilisés[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] Voir notamment le guide https://www.ssi.gouv.fr/guide/recommandations-pour-les-architectures-des-systemes-dinformation-sensibles-ou-diffusion-restreinte/

Recommandations humaines (R. HUM)

R. HUM1 : Les modalités de sensibilisation, de formation et d'entraînement de l'ensemble des parties prenantes à la cybersécurité des drones maritimes et navires autonomes (administrations, concepteurs-intégrateurs, équipementiers, opérateurs de maintenance, armateurs, opérateurs du centre de contrôle à terre, etc.), à tous les niveaux de responsabilité, seront formalisées dans la PSSI particularisée au drone maritime/navire autonome, spécifiées par voie contractuelle et mises en œuvre dès la phase de conception du système.

Recommandations technologiques (R. TEC)[46]

R. TEC1 : La séparation logique ou physique et le filtrage entre les différentes zones fonctionnelles et techniques du drone maritime ou navire autonome sont essentiels. Ainsi, pour la partie embarquée, un cloisonnement logique ou physique et un filtrage protocolaire efficace entre les systèmes de télécommunication externes, les capteurs et les actionneurs, les calculateurs de contrôle-commande, les systèmes de gestion de navigation, les systèmes de gestion de la mission[47] et les systèmes d'administration doivent être assurés. Le filtrage entre chaque zone doit être réalisé par un pare-feu assurant un filtrage protocolaire efficace en bloquant par défaut l'ensemble des flux en ne laissant passer que les flux autorisés et dont l'action doit être journalisée.

R. TEC2 : Il est vivement recommandé qu'une chaîne distincte de sécurité, composée d'automates de sécurité, soit ajoutée en parallèle de l'installation en production, notamment pour les systèmes de navigation, les systèmes de contrôle industriels et la charge utile de mission. Les valeurs maximales et les cas potentiellement non conformes seront testés lors de mises en situation de cette chaîne de sécurité.

R. TEC3 : Sur les systèmes pour lesquels aucune présence humaine à bord n'est réalisée, il est indispensable que les systèmes de positionnement, navigation et temps (PNT) soient redondés par des systèmes alternatifs (autres constellations GNSS : par exemple Galileo en complément du GPS), ou par l'utilisation de moyens alternatifs de positionnement (positionnement stellaire, inertiel, e-LORAN, PNT satellitaires alternatifs (*Satellite Time and Location* (STL), par exemple), et par l'utilisation de moyens antennaires particuliers (type *Controlled Radiation Pattern Antenna* (CRPA), par exemple), afin de réduire le risque de leurrage ou de brouillage GNSS. Des essais de brouillage et de leurrage GNSS doivent être réalisés par des organismes accrédités, afin de vérifier le comportement adéquat du drone/navire autonome dans ce cas.

R. TEC4 : Les systèmes assurant la situation de surface doivent être couplés avec des mécanismes de détection de falsification ou de brouillage GNSS et AIS (*Automatic Identification System*). Des essais de brouillage et de leurrage AIS doivent être réalisés par des organismes accrédités, afin de vérifier le comportement adéquat du drone/navire autonome dans ce cas.

R. TEC5 : Les moyens de télécommunication au sein d'une constellation de drones, avec le navire porteur ou avec les centres à terre (opérationnels ou de maintenance) doivent être redondés, d'une part, et utiliser des mécanismes de cryptographie conformes aux règles préconisées par l'ANSSI[48], en fonction de la criticité de la mission, des moyens de communication utilisés (satellite, Wi-Fi, radio…), du degré d'autonomie des drones et de l'aversion au risque. Cela permettra d'éviter tout risque d'interception, d'intrusion, ou de perte de disponibilité. Il est vivement recommandé que les critères de sécurité requis fassent l'objet d'une évaluation indépendante par des organismes spécialisés.

R. TEC6 : La prise en main du drone maritime ou navire autonome à des fins de contrôle, de supervision ou de maintenance préventive ou corrective localement ou à distance doit faire l'objet d'une authentification multi-facteurs. Toute tentative ou réussite devra être journalisée. Un mode sécurisé de secours (type « vitre brisée virtuelle ») doit être prévu et qualifié en cas de dysfonctionnement de l'authentification multi facteurs.

[46] La majorité de ces mesures est également applicable aux systèmes d'information du centre de contrôle à terre.
[47] Également appelés « charge utile ».
[48] https://www.ssi.gouv.fr/guide/mecanismes-cryptographiques/

R. TEC7 : Des systèmes de détection d'intrusion systèmes et réseau adaptés et aptes à analyser les protocoles spécifiques utilisés sur le drone maritime ou navire autonome doivent être mis en œuvre. Les signatures et/ou la détection par comportement doivent être adaptés à tous les modes de fonctionnement du drone maritime / navire autonome. Le système de détection d'intrusion devra être isolé des réseaux qu'il surveille par des équipements de type TAP (*Test Access Port*) passifs. Les systèmes de détection d'intrusion devront être labellisés par l'ANSSI, le choix du label (certification, qualification et agrément) dépendant des obligations réglementaires et des besoins en sécurité. Dans la mesure du possible, les évènements cyber détectés seront enregistrés par des systèmes de journalisation et exploités en temps réel ou différé par les systèmes de corrélation et d'analyse de journaux tels que ceux opérés par un SOC.

R. TEC8 : Le bon fonctionnement et l'intégrité logicielle et matérielle du drone maritime / navire autonome seront vérifiés à intervalles réguliers, en fonction de la criticité et du degré d'autonomie des systèmes d'information. En cas d'anomalie, la réinstallation autonome du logicielle et, si nécessaire, l'emploi d'un support ou calculateur alternatif doit être possible. Dans la mesure du possible, les évènements cyber portant atteinte à l'intégrité logicielle et matérielle du drone maritime ou du navire autonome seront transmises en temps réel ou différé vers un CERT ou un SOC.

R. TEC9 : Le retour à un mode de fonctionnement « sûr » doit être formellement décrit et testé par des mécanismes techniques fiables en cas de dysfonctionnement ou d'anomalie majeure.

R. TEC10 : Dans des cas spécifiques (criticité de la mission, des matériels ou des logiciels embarqués), des mesures de destruction logique ou physique d'urgence devront pouvoir être mises en œuvre.

R. TEC11 : La détection d'anomalies (de trajectographie, par exemple) par le centre de contrôle à terre doit être assurée par des moyens alternatifs aux seules données transmises par le drone maritime / navire autonome (par exemple : détection d'anomalie de trajectoire par satellite).

R. TEC12 : Dans le cas d'une constellation de drones maritimes / navires autonomes, une auto-vérification d'intégrité d'ensemble de la constellation et de chacun de ses membres doit pouvoir être assurée. En cas d'anomalie, des mécanismes doivent être prévus pour permettre la réinstallation de logiciels à un état sûr, l'utilisation d'équipements alternatifs ou l'exclusion d'un ou plusieurs membres de la constellation en fonction des situations.

R. TEC13 : Les sauvegardes de l'ensemble de l'écosystème seront conservées de manière sécurisée et hors ligne. Des tests de restauration locale ou à distance seront éprouvés régulièrement.

R. TEC14 : L'accès aux données relatives aux programmes, paramètres et configurations des drones maritimes et navires autonomes, devra être garanti et tracé afin d'assurer la protection d'éventuels secrets et d'assurer leur intégrité et disponibilité.

R. TEC15 : La défense en profondeur du système sera mise en œuvre, dès la conception du système et tout au long de son cycle de vie, en appliquant des mesures de configuration sécurisée pour l'ensemble des équipements numériques opérationnels et d'administration (durcissement, bonne gestion des droits d'accès et des comptes d'accès, identification et authentification des utilisateurs et administrateurs, emploi de protocoles sûrs, chiffrement des supports numériques, changement des mots de passe par défaut, etc.)[49].

R. TEC16 : Une attention particulière sera portée, en cas d'utilisation de technologies de type *cloud computing*, sur la localisation et la sécurisation de l'hébergement. Dans la mesure du possible, l'emploi d'un hébergeur labellisé SecNumCloud sera recherché[50].

[49] Voir notamment les guides techniques de l'ANSSI sur la configuration sécurisée disponibles à l'adresse suivante : https://www.ssi.gouv.fr/uploads/2014/10/anssi-catalogue-guides-notes-techniques.pdf
[50] Voir la liste des prestataires qualifiés ici : https://www.ssi.gouv.fr/uploads/liste-produits-et-services-qualifies.pdf

Recommandations réglementaires (R. REG)

En complément de l'investissement des armateurs, chantiers navals, opérateurs et constructeurs, le rôle du régulateur (international, européen ou national) est jugé essentiel pour assurer la cybersécurité des drones maritimes / navires autonomes. Il apparaît donc nécessaire que le cas d'emploi des drones maritimes et navires autonomes soit pris en compte dans les règlements et recommandations existants, et cela en-dehors de la question précise de la navigabilité de ces équipements au sens de la réglementation SOLAS.

R. REG1 : Au niveau de l'OMI, les travaux devront prendre en compte la cybersécurité de ce type de systèmes, par exemple au sein du futur code MASS.

R. REG2 : La délivrance d'un certificat de navigabilité, la procédure d'inscription au registre propre aux drones ou l'étude en vue de l'autorisation pour un navire autonome de naviguer à titre expérimental devrait être conditionnées à la délivrance d'une preuve formelle de prise en compte de mesures adaptées de cybersécurité (au minimum : analyse de risques spécifique, mise en œuvre de mesures de protection adaptées, audits et correction des écarts identifiés, maintien en conditions de sécurité). Cette preuve pourrait correspondre à la décision d'homologation du système ou par la délivrance d'une notation appropriée par une société de classification.

R. REG3 : La directive NIS v2, ou sa transposition dans les droits nationaux, devrait intégrer dans son périmètre d'application, à défaut des drones maritimes et navires autonomes, les centres de téléopération (*Shore Control Center*), dès lors qu'ils assurent une fonction essentielle ou présentent un risque majeur (opérationnel, environnemental, humain) en cas d'incident.

ANNEXES

ANNEXE 1

Détails de l'analyse de risques

• Missions, valeurs métiers et biens supports

Comme évoqué précédemment, les missions, valeurs métier et biens supports des drones maritimes et navires autonomes sont les suivants :

Mission 1	Valeurs métiers	
Concevoir, réaliser et intégrer des drones maritimes ou navires autonomes	Produire le drone maritime/navire autonome	Informations liées à l'architecture, la programmation ou la production du drone maritime/navire autonome
Biens supports	Systèmes de conception et de développement du drone maritime ou du navire autonome : • Serveurs, espaces de stockage • Réseaux numériques de conception, d'ingénierie et de développement	

Mission 2	Valeurs métiers	
Maintenir en service des drones maritimes ou navires autonomes	Maintenir en condition opérationnelle le drone maritime/navire autonome	Informations liées à la maintenance du drone maritime/navire autonome
Biens supports	Système pour le maintien en condition opérationnelle du drone maritime ou du navire autonome : • Serveurs, espaces de stockage • Réseaux numériques de maintenance • Stations mobiles de maintenance • Liens spécifiques dédiés à la maintenance et/ou au suivi à distance	

Mission 3	Valeurs métiers	
Naviguer en sécurité et en conformité avec la réglementation internationale	Préparer la navigation et naviguer en toute sûreté et sécurité	Informations relatives à la préparation de la navigation, à la navigation et au fonctionnement du drone maritime/navire autonome
Biens supports	Système embarqué de gestion de la navigation du drone maritime ou du navire autonome : • Capteurs de type position, navigation et temps (PNT) et AIS • Systèmes de contrôle industriel pour assurer la mobilité (énergie, propulsion,...) • Calculateurs • Supports de communication satellitaires (de longue distance) et/ou radioélectriques de proximité (à portée de vue, *Line of Sight* (LoS)) Systèmes de gestion numérique (à bord et à terre) : • Serveurs, espaces de stockage pour les programmes nécessaires au fonctionnement du drone ou du navire autonome • Réseaux numériques pour gérer le fonctionnement • Supports numériques/postes pour la lecture et l'écriture des informations nécessaires au fonctionnement	

Mission 4	Valeurs métiers	
Assurer la mission qui leur est confiée	Assurer les activités prévues dans le cadre de la mission	Informations délivrées, collectées ou produites lors de la mission
Biens supports	Système de gestion de la mission : variable selon le type de drone maritime/navire autonome, de capteur/effecteur et en fonction du contexte d'emploi. Systèmes de gestion numérique (à bord et à terre) : • Serveurs, espaces de stockage pour les programmes nécessaires au fonctionnement du drone ou du navire autonome • Réseaux numériques pour gérer le fonctionnement • Supports/postes pour la lecture et l'écriture des informations nécessaires au fonctionnement	

Il convient de noter que les biens supports associés sont multiples, et vont dépendre de la taille, du type et du degré d'autonomie du drone maritime ou navire autonome :

- Pour les missions M1 et M2, les concepteurs, équipementiers, intégrateurs et mainteneurs (internes ou externes) de ces systèmes vont utiliser, par exemple, des serveurs, espaces de stockage et réseaux numériques de conception, d'ingénierie, de développement et de maintenance. Ils pourront également assurer la programmation d'équipements particuliers à l'aide de stations mobiles de maintenance et/ou de liens spécifiques dédiés à la maintenance (prédictive/préventive/corrective) ou au suivi à distance.
- Pour la mission M3, le drone maritime ou navire autonome va utiliser, d'une part, des capteurs de type position, navigation et temps (systèmes GNSS, RADAR, LIDAR (*Laser Imaging Detection And Ranging*), sondeurs, capteurs optiques, AIS/VDES (*VHF Data Exchange System*), loch, compas) et les calculateurs associés, d'autre part, des systèmes de contrôle industriel pour assurer sa mobilité (énergie, propulsion, commande de barre, etc.). Dans la grande majorité, ces équipements sont des équipements disponibles « sur étagère » au sein du monde maritime et interconnectables par le biais de standards du secteur comme NMEA 0183/2000. Le rôle des calculateurs est particulièrement important pour assurer la fusion des informations issues des capteurs, gérer la navigation autonome et la prise de décision, ainsi que la gestion des actionneurs. La communication avec les centres de contrôle à terre ou les navires porteurs utilisera des supports radioélectriques divers, et notamment satellite (INMARSAT, VSAT, Thuraya, Starlink, Iridium, etc.) pour les liaisons longues distance, et radioélectriques « *Lign of Sight* (LoS) » pour échanger avec les drones et navires à proximité, par exemple dans le cadre d'une constellation. Les supports numériques utilisés pour la lecture et l'écriture des informations et le stockage des programmes nécessaires au fonctionnement du drone/navire autonome seront des biens supports particulièrement sensibles.
- Pour la mission M4, les biens supports (type capteurs, effecteurs, calculateurs, systèmes de communication et supports de stockage) peuvent varier en fonction du type de drone maritime/navire autonome, de capteur/effecteur et du contexte d'emploi. La protection (intégrité, confidentialité, disponibilité, traçabilité, non répudiation) des processus assurant le transfert d'information de et vers le drone maritime et navire autonome va dépendre de la sensibilité des informations transmises et des besoins spécifiques liés à la mission. Ainsi, les niveaux de protection à garantir entre un drone à vocation scientifique et un drone de combat naval seront très certainement différents.

• Parties prenantes

De nombreux acteurs malveillants sont réputés pour exploiter les différents maillons de la chaîne logistique (partenaires, sous-traitants…), d'un niveau de maturité parfois inférieur, afin de viser une organisation importante ou sensible. Il convient donc de prendre en compte l'ensemble des parties prenantes pour identifier les chemins d'attaque d'un système.

Pour l'analyse de risques d'un drone maritime ou d'un navire autonome, les parties prenantes suivantes pourraient ainsi être considérées :

- PP1 : concepteurs, équipementiers, intégrateurs ;
- PP2 : opérateurs d'exploitation ;
- PP3 : membres de l'équipage[51] ;
- PP4 : opérateurs de maintenance internes ou externes ;
- PP5 : opérateurs de télécommunication ou de diffusion de références (positionnement, navigation, temps).

• Sources de risques

Les menaces non intentionnelles n'étant pas prises en compte par EBIOS Risk Manager, les sources de risques identifiées pourraient être les suivantes, leur priorisation dépendant là également du contexte d'emploi du drone maritime ou navire autonome et de l'aversion au risque de l'opérateur :

- SR1 : La vengeance d'un ancien employé ou d'un opérateur de maintenance dont, par exemple, les comptes n'auraient pas été révoqués ;
- SR2 : Des activistes opposés aux drones maritimes et navires autonomes ou des attaquants opportunistes qui parviendraient à prendre le contrôle d'un navire pour en montrer les faiblesses ;
- SR3 : Un concurrent qui chercherait à obtenir des données sensibles sur le drone maritime ou le navire autonome, soit de manière discrète (espionnage), soit de manière destructrice ;
- SR4 : Acteurs cybercriminels à la recherche de profit financier, qui prendraient en otage les systèmes d'information à terre ou embarqués liés au drone maritime ou navire autonome ;
- SR5 : Terroriste cherchant à détruire le navire ou à l'utiliser pour causer des dommages à autrui ;
- SR6 : Acteurs étatiques cherchant à espionner en récupérant les données de mission du drone maritime/navire autonome, à le détruire, à prendre la main ou à endommager le drone ou le navire autonome.

• Évènements redoutés

Les évènements redoutés relatifs aux drones maritimes et navires autonomes peuvent être identifiés, leur classement en termes de gravité dépendant de l'aversion au risque de l'organisation. Même si cette aversion peut varier suivant le type de porteur (drone/navire), sa mission et son opérateur, les évènements redoutés suivants pourraient être identifiés :

<u>Évènements redoutés relatifs à la conception et la production du drone ou navire autonome (Mission 1)</u> :

- ER1 : Perturbation ou interruption de la production du drone maritime ou du navire autonome.

  Impacts : impacts opérationnels, impacts financiers, impacts juridiques, impacts sur l'image et la confiance
- ER2 : Fuite de données relatives à l'architecture, la programmation ou la production d'un drone maritime ou de navire autonome.

  Impacts : impacts financiers, impacts sur la gouvernance
- ER3 : Altération des données relatives à l'architecture, la programmation ou la production d'un drone maritime ou de navire autonome

  Impacts : impacts sur la sécurité, impacts sur l'image et la confiance, impacts juridiques

[51] pour les navires autonomes de degrés 1 et 2

Évènements redoutés relatifs à la maintenance du drone ou navire autonome (Mission 2) :

- ER4 : Perturbation ou interruption de la maintenance du drone maritime ou du navire autonome.

  Impacts : impacts opérationnels, impacts financiers, impacts juridiques, impacts sur l'image et la confiance, impacts sur la sécurité

- ER5 : Fuite de données relatives à la maintenance d'un drone maritime ou de navire autonome.

  Impacts : impacts financiers, impacts sur la gouvernance, impacts sur l'image et la confiance

- ER6 : Altération des données relatives à la maintenance d'un drone maritime ou de navire autonome

  Impacts : impacts sur la sécurité, impacts sur l'image et la confiance, impacts juridiques

Évènements redoutés relatifs à la capacité de navigation en sécurité du drone ou navire autonome (Mission 3) :

- ER7 : Perturbation ou interruption de la phase de préparation de la navigation du drone maritime ou navire autonome

  Impacts : impacts financiers, impacts opérationnels

- ER8 : Altération ou destruction du drone maritime ou du navire autonome

  Impacts : impacts financiers, impacts sur la sécurité, impacts opérationnels, impacts environnementaux, impacts humains

- ER9 : Capture du drone maritime ou du navire autonome

  Impacts : impacts financiers, impacts opérationnels, impacts sur la gouvernance

- ER10: Altération des données relatives à la préparation de la navigation, à la navigation et au fonctionnement du drone/navire autonome

  Impacts : impacts sur la sécurité, impacts opérationnels, impacts financiers

Évènements redoutés relatifs à la mission du drone ou navire autonome (Mission 4) :

- ER11 : Perturbation ou détournement de la mission

  Impacts : impacts opérationnels, impacts financiers, impacts sur la gouvernance, impacts sur la sécurité

- ER12 : Fuite de données captées durant sa mission

  Impacts : impacts financiers, impacts sur la gouvernance, impacts sur l'image et sur la confiance

- ER13 : Altération des données captées durant sa mission

  Impacts : impacts opérationnels, impacts financiers, impacts sur la gouvernance

ANNEXE 2

Réduction des risques associés aux scénarios stratégiques

L'objectif de ce tableau est de démontrer la réduction des risques associés aux scénarios stratégiques par la mise en œuvre des mesures organisationnelles, humaines et techniques proposées.

SS1 : La compromission des équipements assurant la liaison avec le *Shore Control Center* ou les opérations qui s'y déroulent entraîne une perte de communication avec le drone maritime ou navire autonome, qui en perturbe la 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 : La perturbation par leurrage ou brouillage des informations reçues par les capteurs du drone ou navire autonome (GNSS, AIS, RADAR, etc.) entraîne une perturbation ou une interruption temporaire ou définitive de la mission opérationnelle.
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 : La compromission en phase de maintenance des systèmes d'information du drone ou navire autonome entraîne une interruption ou un détournement de la mission.
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 : La compromission des algorithmes de calcul et de prise de décision du drone maritime ou navire autonome en phase de conception entraîne un incident grave lors de sa mise en service.
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 : L'attaque de la chaîne d'approvisionnement (concepteurs, équipementiers, intégrateurs) entraîne le vol des plans ou des données relatifs à un projet de drone ou de navires autonomes.
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

ANNEXE 3

Respect des exigences de la directive européenne NIS

La directive européenne NIS fixe 23 règles de sécurité. Sans présager de l'évolution de ces mesures liées à la parution, puis à la déclinaison en droit français, de sa seconde version, ce Livre blanc propose de vérifier que les mesures proposées pour les drones maritimes et navires autonomes sont cohérentes par rapport à cette directive. Le détail des mesures n'est pas repris dans le tableau mais figure dans l'arrêté publié au Journal Officiel[52]. L'ensemble de l'écosystème des drones maritimes et navires autonomes n'a pas aujourd'hui d'obligation de répondre à l'arrêté déclinant la directive NIS dans la réglementation française mais, suivant la criticité des missions, les centres de téléopération pourraient être amenés à le devenir, soit actuellement soit dans le cadre de la version 2 de la directive.

S'agissant également de bonnes pratiques génériques et intersectorielles, ces mesures sont dans tous les cas efficaces pour prévenir un nombre important d'incidents. Il est à noter que la version 2 de la directive précise plus en détail certaines mesures, en fixant notamment des degrés en fonction du statut de l'organisme et/ou de la criticité du système.

Bien entendu, la performance de la couverture dépendra de l'efficacité des mesures mises en place. La couverture mentionnée ici par les mesures proposées reste donc indicative, afin de permettre de mieux jauger l'efficacité de certaines règles.

Numéro de règle NIS	Description	Couverture par règles
Règle 1	Effectuer et maintenir une analyse de risques.	R. ORG1
Règle 2	Élaborer, maintenir et mettre en œuvre une politique de sécurité des systèmes d'information.	R. ORG11
Règle 3	Homologation de sécurité des Systèmes d'Information Essentiels.	R. ORG2
Règle 4	Évaluation et mise à jour d'indicateurs.	R. ORG11
Règle 5	Réalisation d'audits de cybersécurité.	R. ORG3
Règle 6	Élaboration et mise à jour de la cartographie.	R. ORG7
Règle 7	Configuration sécurisée des systèmes d'information.	R. TEC15
Règle 8	Cloisonnement des systèmes d'information.	R. TEC1
Règle 9	Accès distant aux systèmes d'information.	R. TEC6
Règle 10	Filtrage d'accès aux systèmes d'information.	R. TEC1
Règle 11	Gestion des comptes d'administration.	R. TEC15
Règle 12	Administration des systèmes d'information.	R. TEC15

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

Règle 13	Identification des utilisateurs.	R. TEC15
Règle 14	Authentification des utilisateurs.	R. TEC15
Règle 15	Droits d'accès au système d'information.	R. TEC15
Règle 16	Maintien en conditions de sécurité.	R. ORG4
Règle 17	Sécurité physique et environnementale.	R. ORG8 R. TEC10
Règle 18	Détection des incidents de sécurité.	R. TEC7
Règle 19	Journalisation.	R. TEC1 R. TEC6 R.TEC8
Règle 20	Corrélation et analyse de journaux.	R. ORG10
Règle 21	Réponse aux incidents.	R. ORG10
Règle 22	Traitement des alertes.	R. ORG10
Règle 23	Gestion de crises.	R. ORG9 R. HUM1

GLOSSAIRE

A

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

C

Chiffrement des données : Technique rendant les données illisibles, sauf si une action spécifique (déchiffrement) est exercée pour en autoriser l'accès.
CRPA : Controlled Radiation Pattern Antenna

D

Décommissionnement : Fin de vie d'une application ou d'un équipement informatique.
Déni de service : Action ayant pour effet d'empêcher ou de limiter fortement la capacité d'un système à fournir le service attendu.
DGAMPA : Direction Générale des Affaires Maritimes, de la Pêche et de l'Aquaculture.

E

EBIOS : Expression des Besoins et Identification des Objectifs de Sécurité
EMR : Énergies Marines Renouvelables
ENSM : École nationale supérieure maritime

F

FSN : Fournisseur de Service Numérique

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
Ingénierie sociale : Manipulation consistant à obtenir un bien ou une information, en exploitant la confiance, l'ignorance ou la crédulité de tierces personnes.
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
MCS (Maintien en Conditions de Sécurité) : il s'agit des procédures, des femmes et hommes et des outils permettant d'assurer la défense en profondeur des systèmes d'information tout au long de leur cycle de vie et permettant notamment la bonne application des correctifs de sécurité.
MFA : Multiple Factor Authentification ou vérification en deux étapes, est une méthode par laquelle un utilisateur peut accéder à une ressource informatique (un ordinateur, un téléphone intelligent ou encore un site web) après avoir présenté deux preuves d'identité distinctes à un mécanisme d'authentification.
MMCM : Maritime Mine Counter Measures

N

NIS : Network Information Security
NMEA : National Maritime Electronics Association

O

OIV : Opérateur d'Importance Vitale
OMI : Organisation Maritime Internationale
OSE : Opérateur de Service Essentiel
OTAN : Organisation du Traité de l'Atlantique Nord

P

PCA (Plan de Continuité d'Activité) : Ce plan détaillant les procédures (techniques, organisationnelles, humaines) a pour vocation de formaliser les modalités de continuité d'activité de l'entité en cas de perte temporaire de l'un de ses systèmes d'information.
PNT : Position, Navigation, Temps
Porte dérobée : Accès dissimulé, soit logiciel soit matériel, qui permet à un utilisateur malveillant de se connecter à une machine de manière furtive.
PRA (Plan de Reprise d'Activité) : Ensemble de procédures (techniques, organisationnelles, humaines) qui permet à une entreprise de prévoir par anticipation, les mécanismes pour reconstruire et remettre en route un système d'information en cas de sinistre important ou d'incident critique.

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
Surface d'attaque : ensemble de la surface exposée d'un système d'information, comprenant des vulnérabilités qui pourraient être exploitées par un attaquant.
SIIV : Système d'Information d'Importance Vitale
SCC : Shore Control Center
Système d'information : ensemble des matériels contenant les informations nécessaires pour accomplir la mission de l'entreprise et des réseaux permettant leurs échanges.

U

UAV (Unmanned Aerial Vehicle) : système de drone aérien
UMS (Universal Measurement System) : unité de mesure de jauge brute
USV (Unmanned Surface Vehicle) : système de drone de surface
Utilisateurs privilégiés : Dans un système, il existe en général des utilisateurs disposant de droits spéciaux leur permettant d'administrer le système.
UUV (Unmanned Underwater Vehicle) : système de drone sous-marin

V

VDES : Very High Frequency Data Exchange System
VPN (Virtual Private Network) : Système permettant de créer un lien direct entre des ordinateurs distants, via un réseau qui sécurise l'échange.
VSAT : Very Small Aperture Terminal

EN COOPÉRATION AVEC

MARINE NATIONALE

GENDARMERIE MARITIME

FRANCE CYBER MARITIME

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

CONTACTS

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

www.france-cyber-maritime.eu

AVEC LE SOUTIEN DE

PREMIER MINISTRE
Liberté
Égalité
Fraternité

Secrétariat général de la mer

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Région BRETAGNE

Brest Métropole