

# Maritime Cyber Situational Awareness

Utilisation d'un jeu de données d'incidentologie maritime pour renforcer la protection, la détection et la résilience du secteur maritime

Olivier JACQ

Chaire de cyberdéfense des systèmes navals

24 septembre 2026

© 2026 - Olivier JACQ



Ce document est marqué **TLP:CLEAR**. Les règles de diffusion attendues sont :

Divulgateur libre, les destinataires peuvent diffuser cette information dans le monde entier sans aucune limite. Les sources peuvent utiliser l'appellation **TLP:CLEAR** lorsque les informations présentent un risque minimal ou nul de mauvaise utilisation, conformément aux règles et procédures applicables à la diffusion publique. Sous réserve des règles standard de copyright, les informations mentionnées en **TLP:CLEAR** peuvent être partagées sans restriction.

Référence : FIRST - Traffic Light Protocol (TLP) v2.0

### ■ Parcours professionnel

- Ancien officier supérieur de la Marine nationale, ancien CTO/CSO - France Cyber Maritime
- *Registered Expert* EMSA et ENISA
- Ingénieur R&D chez DIATEAM
- Chercheur associé à l'IRENAV
- CEO et fondateur de CYBERMOOV

### ■ Formation

- Mastère spécialisé cybersécurité - CentraleSupélec
- Titre Expert SSI - ANSSI
- Doctorat en informatique - IMT Atlantique

### ■ Associatif / projets

- Créateur de <https://cybermaretique.fr>
- Co-organisateur <https://unlockyourbrain.bzh>



# Ouverture

- Un sujet
- Des questions de recherche
- Des expérimentations
- Des jeux de données et des outils
- Des publications
- Un manuscrit
- Une soutenance

Particularité : thèse conduite en étant officier supérieur de la Marine nationale, en poste opérationnel deux années sur trois.

# La thèse

### La marétique

L'ensemble des systèmes informatiques et électroniques utilisés dans la gestion et l'utilisation des opérations relatives aux activités maritimes, fluviales et portuaires.

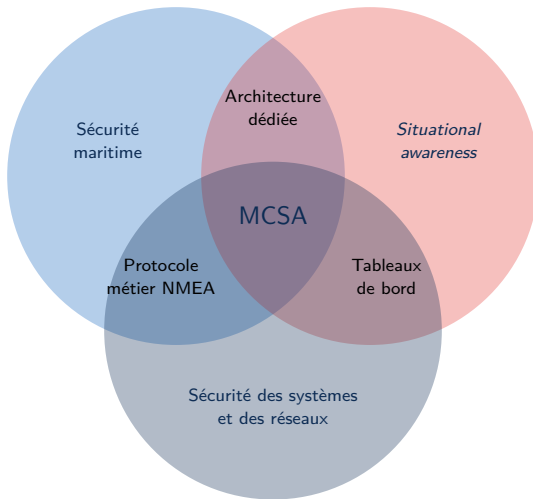
*« Comment améliorer la qualité et le temps de réaction nécessaires à la détection, la compréhension et la réaction face à une menace cyber, afin de prendre les bonnes décisions dans ce secteur maritime particulier ? »*

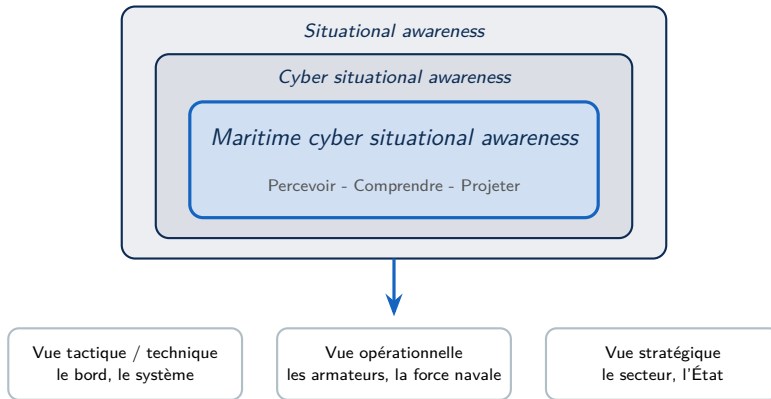
### Les particularités de la marétique

- Des systèmes de systèmes aux caractéristiques combinées
- Une connectivité contrainte, chère et intermittente
- Des cycles de vie très longs, des équipements propriétaires
- Un facteur humain et des opérations qui priment

### L'inadéquation des outils classiques

- Des volumes de données trop importants
- Des systèmes hétérogènes et répartis
- Trop de faux positifs

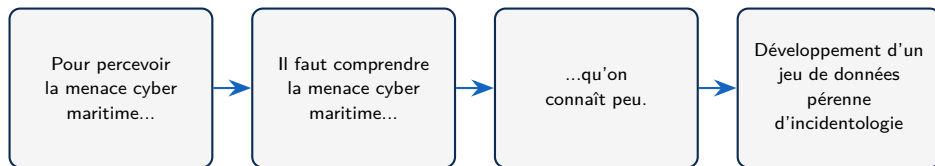




Une approche de la cybersurveillance finalement très duale...

- QR1, modéliser et collecter : la MCSA (travaux de Dr. M. Endsley enrichis), architectures bord et terre
- QR2, analyser et représenter : qualité des données, risque dynamique par graphes
- QR3, détecter en contexte maritime : le *Naval Cyber Range*, l'alerte au profit du marin

Les apports opérationnels militaires ne seront pas précisés ici.

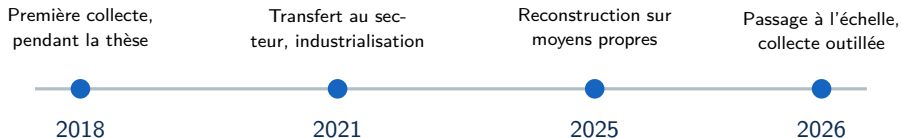


Commencé sur un blog, [cybermaretique.fr](http://cybermaretique.fr), avec une trentaine d'incidents. Aujourd'hui plus de 4 100, et un véritable outillage.

# L'outil

*« Poursuivre l'enrichissement du concept d'évaluation dynamique des risques avec des données complémentaires, comme les TTP, afin de faciliter l'analyse. »*

Pour enrichir avec les TTP, encore faut-il un référentiel de ce qui frappe le secteur, et il n'existait pas.



Cette thèse a produit un outil toujours opérationnel et amélioré de manière continue.

### Le corpus

- Plus de 4 100 incidents documentés, de 1980 à aujourd'hui
- 160 pays touchés, 333 sources de menaces
- Plus de 7 800 références sourcées

### La fabrique

- Une fiche par incident, en texte, versionnée
- Taxonomies contrôlées, chaque valeur définie par écrit
- Un périmètre maritime et portuaire explicite, à géométrie variable
- Validation automatique au dépôt, collecte partiellement outillée

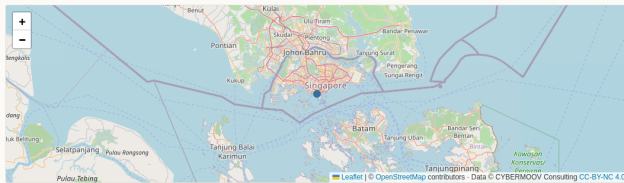
Source : jeu de données personnel de l'auteur, relevé du 21 septembre 2026.

- Cotation Admiralty par fiche : fiabilité de la source, crédibilité de l'information
- Statut de la revendication : confirmée, démentie, contestée, recyclée
- Donnée manquante déclarée, jamais remplie d'une valeur de confort
- Impact visé et effet mesuré séparés

*Sans oublier un cycle de mise à jour régulier...*

### Maritime and Port Authority of Singapore

|                           |                                                                                                  |
|---------------------------|--------------------------------------------------------------------------------------------------|
| Date                      | 10/03/2025                                                                                       |
| Country (incident)        |  Singapore (SG) |
| Victim                    | <a href="#">Maritime and Port Authority of Singapore</a>                                         |
| Activity                  | <a href="#">Port</a>                                                                             |
| Threat type               | <a href="#">Spearphishing</a>                                                                    |
| Threat actor              | <a href="#">SideWinder</a>                                                                       |
| Malware family            | <a href="#">StealerBot</a>                                                                       |
| Attributed to (country)   | IN                                                                                               |
| Origin category           | State sponsored                                                                                  |
| Impact (CIA)              | Confidentiality                                                                                  |
| Exploited vulnerabilities | <a href="#">CVE-2017-0199</a> <a href="#">CVE-2017-11882</a>                                     |
| Admiralty code            | <b>A 2</b>                                                                                       |
| TLP                       | <b>TLP: CLEAR</b>                                                                                |

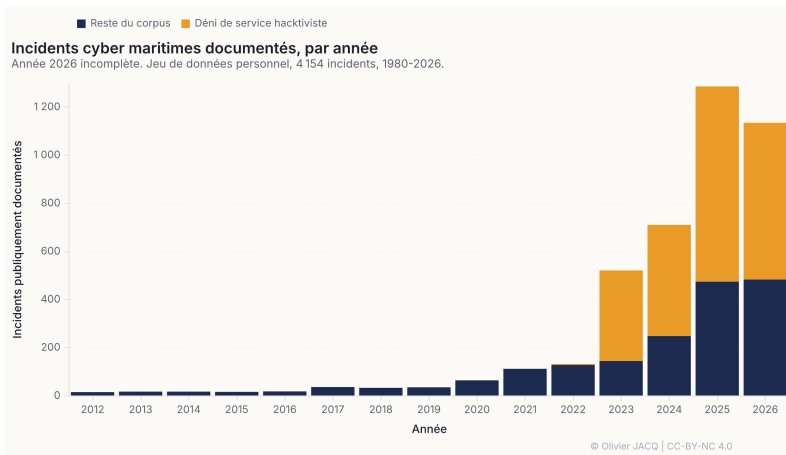


Maritime and Port Authority of Singapore (MPA) - city

### Ce que porte une fiche

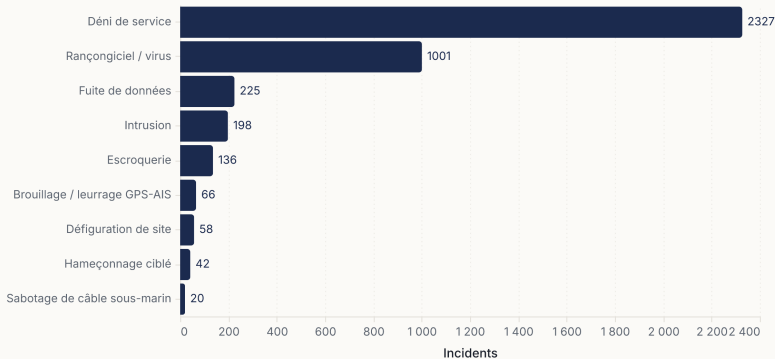
- Cotation Admiralty A2 : source fiable, information très probable
- Le commanditaire, l'État, distinct de l'acteur qui exécute
- L'effet mesuré, s'il existe
- Des sources indépendantes, toutes publiques
- Une géolocalisation quand elle est possible

# Lecture du corpus



### Répartition par type de menace

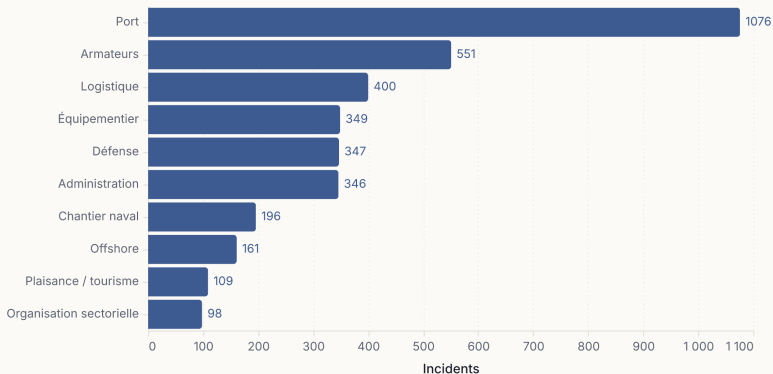
Le déni de service pèse plus de la moitié du corpus.



© Olivier JACQ | CC-BY-NC 4.0

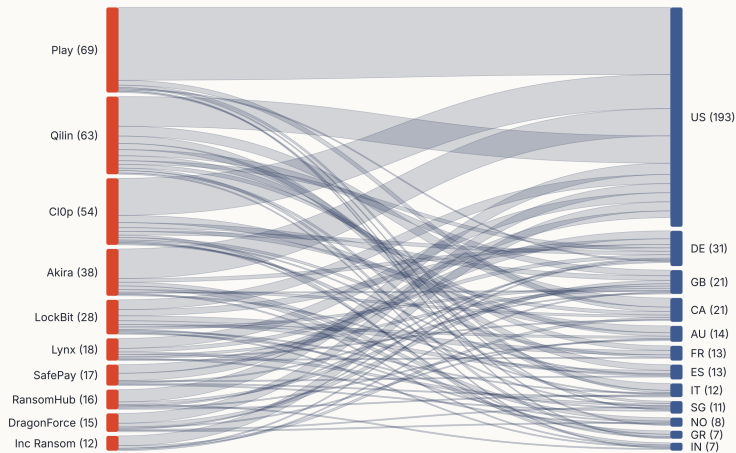
### Répartition par activité de la victime

Le monde maritime attaqué n'est pas d'abord le navire.

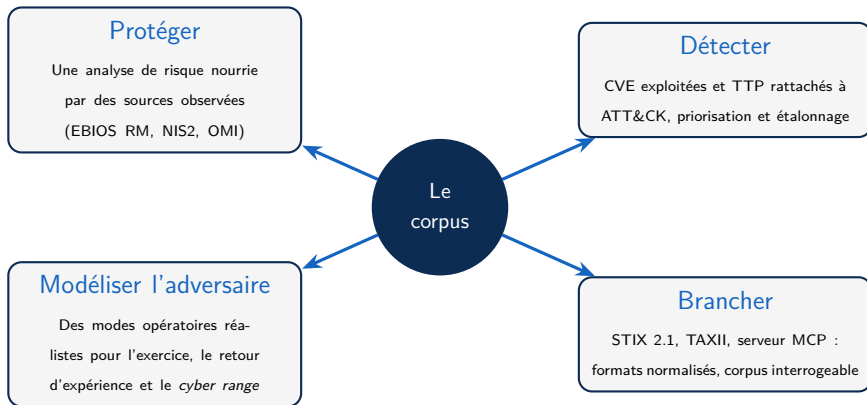


© Olivier JACQ | CC-BY-NC 4.0

### Acteurs de rançongiciel et pays visés



© Olivier JACQ | CC-BY-NC 4.0



Ces quatre usages se déclinent en appui direct : ateliers, exercices sur table, formation.

# Limites et ouverture

1. On ne documente que ce qui devient public : le secteur déclare peu et tard, et la source primaire est souvent l'attaquant
2. Les collecteurs se recopient, et le poids de l'acteur et du collecteur dominants est recalculé à chaque publication
3. Le périmètre est le mien : écrit et assumé, mais non comparable à un autre corpus
4. Pas de dénominateur : on compte les incidents sans les rapporter à aucune population
5. Pas d'économie de l'incident : moins de 2 % des fiches portent un montant
6. Pas de gravité comparable : un site vitrine et un terminal à l'arrêt comptent pour un
7. Toute croissance mêle la menace réelle et l'amélioration de la collecte

## Sur la donnée

- Qualifier automatiquement sans perdre la traçabilité de la décision
- Construire une échelle de gravité comparable entre incidents
- Estimer la sous-déclaration plutôt que la subir

## Sur les usages

- Fusionner incidentologie et anomalies de navigation
- Situer l'humain dans la chaîne de qualification

# Les débouchés de la thèse

## Conférences

- ICCSCI 2017 : une plateforme de sensibilisation en contexte maritime
- CSNet 2018 : un centre d'opérations de cybersécurité maritime
- IEEE Cyber SA 2019 : détection temps réel et conscience de situation navale
- SuriCon 2019 : Suricata, ELK et Neo4j pour la défense réseau
- MSAW 2019 : la MCSA pour les drones et les navires autonomes

## Autres écrits

- *Lettre Cybersécurité et politiques publiques* 2018 : les enjeux de la cyber-marétique
- *Cybersécurité maritime, regards croisés* 2020 : drones maritimes et navires autonomes

## Prix

- Beauplet-Rollinat 2019, Alliance Navale
- Daveluy 2022 du chef d'état-major de la Marine, « Sciences de l'ingénieur »
- Cyber 2022, concours « Crypto, Cyber et Compliance », BLL Consulting

## Prolongements scientifiques

- IEEE CSR 2021 : projet Cyber-MAR, risque portuaire
- IEEE Cyber SA 2021 : anomalies de navigation
- OCEANS 2021 : interdépendances des systèmes navals
- NMIOTC 2021 (OTAN) et *Maritime cyber ranges* 2021 : architecture et cas d'usage
- *Le Droit Maritime Français* et *Sciences navales* 2022 : réglementation et synthèse sectorielle

## Diffusion et *keynotes*

- Hack.lu 2023 et SPI 2023
- OCEANEXT 2024, Seanergy 2024 sur les énergies marines renouvelables
- Colloque Détroits et cybersécurité 2024
- *Keynote* FPS 2025
- Séminaire ESIWA+ Bangkok 2026
- SEAMLESS 2026 : paysage de menace des systèmes maritimes autonomes

## En cours

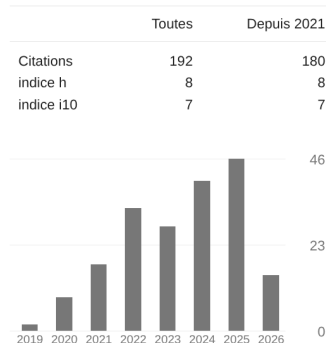
- 4 articles

## Après la soutenance

- 180 des 192 citations sont postérieures à 2021
- L'année la plus citée est 2025, cinq ans après la soutenance
- Les deux articles les plus repris sont ceux écrits dans la chaire

Source : Google Scholar, relevé de septembre 2026. 2026 est incomplète.

Citée par



## Transmettre

- Participation à la création du Mastère Spécialisé « Cybersécurité des systèmes maritimes et portuaires »
- Enseignement : Centrale Supélec, IMT Atlantique, Centrale Méditerranée, École navale, ENSIBS, IUT de Lorient, UBO
- Encadrement de stagiaires, d'alternants et de doctorants

## Chercher et entreprendre

- Chercheur associé à l'IRENav
- Expertise auprès de l'EMSA et de l'ENISA
- Recherches et interventions (OTAN)
- Participation à la création de France Cyber Maritime
- Développement du M-CERT
- Création de CYBERMOOV
- 15 MOOC de cybersécurité maritime

# Conclusion

La thèse a permis la naissance d'un outil et d'un jeu de données, observatoire de l'incidentologie cyber maritime.

Au-delà, la Chaire a été la première initiative mondiale de type écosystème sur le domaine de la cybersécurité maritime. Ses apports ont été essentiels.

# Merci pour votre attention !



LinkedIn