Mastère Spécialisé
Cyber sécurité des systèmes industriels et des opérations maritimes et portuaires

Yvon Kermarrec
Professeur IMT Atlantique
Titulaire de la chaire cyber navale

#1.

Contexte

Contexte

- La chaire de cyber défense des systèmes navals : son ancrage dans le domaine et ses 2 volets : formation et recherche
- Un lien fort avec la Marine nationale, Naval Group et Thales
- 4 écoles impliquées dans la chaire : 3 partenaires académiques (Ecole navale, ENSTA Bretagne et IMT Atlantique) et un académique associé (Ecole Marine Marchande)
- Besoin avéré d'ingénieurs en cyber sécurité pour le domaine maritime qui n'est pas réellement exploré
- Besoin de personnels (navigants, officiers, acteurs des ports….) qualifiés et formés en lien avec les navires et les ports, depuis la conception jusqu'à la fin de vie en passant par l'opérationnel

Contexte

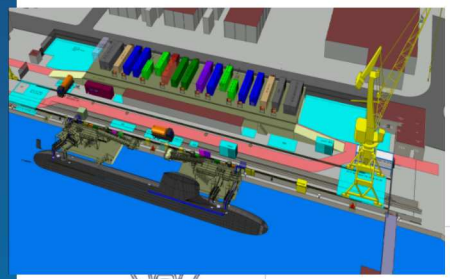
- Une dualité civile et militaire puisque les mêmes technologies, méthodologies et équipements se retrouvent sur les 2 types de bateaux et 2 types d'installations à quai ou stations terrestres
- Une continuité à assurer entre le navire et les infrastructures portuaires et une sécurisation des liens et réseaux (au sens large)
- Des enjeux forts du fait des menaces et des impacts potentiels d'attaques sur les navires et/ou les infrastructures portuaires … et un début de prise de conscience des enjeux et des menaces
- Une demande de la Marine nationale de formation pour ses officiers

Contexte et prise de conscience des différents acteurs civils et militaires

- Rapport du SG Mer, le GICAN, le Cluster Maritime Français; Armateurs et Ports de France : nov 2018 :
  « *appelle à créer une culture cyber qui prenne en compte les impératifs de sécurité dès la phase de mise en chantier d'un projet allant du simple système au navire tout entier* »
- Guide ANSSI sur les bonnes pratiques pour les acteurs maritimes : « *Les systèmes d'information et réseaux informatiques ont progressivement envahi le milieu maritime et sont désormais omniprésents sur les navires. Cette évolution expose chaque jour les équipages à de nouveaux risques : vol d'informations, prise de contrôle à distance de systèmes informatiques, sabotage, etc.* »
- BIMCO, OMI, OTAN : « *Ships are increasingly using systems that rely on digitisation, digitalisation, integration, and automation, which call for cyber risk management on board. As technology continues to develop, information technology (IT) and operational technology (OT) onboard ships are being networked together – and more frequently connected to the internet. This brings the greater risk of unauthorised access or malicious attacks to ships' systems and networks.* «

Contexte

- Des équipements à la mer
  - Isolation partielle – équipage réduit
  - Technologie avancée et complexité des systèmes
  - Durée de vie des programmes > 30 ans
- Des infrastructures portuaires
  - Très sensibles
  - Vecteurs majeurs du commerce mondial
  - Technologies et internet des objets
  - Gros volumes de trafic
- Energie
  - EMR, off shore …



ECOLE NAVALE

ENSTA Bretagne

IMT Atlantique Bretagne-Pays de la Loire École Mines-Télécom

NAVAL GROUP

THALES

PÔLE D'EXCELLENCE CYBER

Région BRETAGNE

ENSM

#2.
Le mastère

Calendrier

- Convention cadre entre partenaires : automne 2019
- Labélisation CGE (début 2020)
- Labélisation pôle mer début 2020
- Sélection des candidats : mai 2020
- Début des cours : 1er octobre 2020
- Anticiper une labélisation ANSSI : SecNumEdu

Ambitions

- Le mastère spécialisé cyber marine est le premier mastère spécialisé dédié à la cybersécurité du monde maritime
- Il bénéficie du partenariat établi entre les partenaires de la chaire cyber navale et de leurs soutiens
- Le partenariat stratégique avec la Marine nationale s'en retrouve renforcé
- Le mastère pourra aussi contribuera à l'innovation et au développement d'un nouvel écosystème cyber à la pointe de la Bretagne associant les différents acteurs du monde marine
- Une formation à la pointe et reconnue par les différentes autorités et labélisée

Ambitions

- Un curriculum qui réponde aux attentes de la Marine nationale mais plus généralement des acteurs du monde maritime (civil et militaire)
- Une formation qui reprend les grandes orientations du PEC (via le référentiel de formation)
- Des compétences techniques, scientifiques pour anticiper, prévenir, et gérer les crises cyber
- Un ensemble de cours, travaux pratiques et un projet transverse qui donnera un fil conducteur pour l'ensemble de la formation et qui sera en lien directs avec les acteurs du monde maritime

Cibles et métiers visés

Les diplômés pourront exercés plusieurs métiers listés dans le référentiel de l'ANSSI, avec une spécialisation pour leur application au monde maritime :

- Administrateur sécurité
- Analyste de la menace
- Architecte sécurité
- Chef de projet sécurité
- Développeur sécurité
- Évaluateur sécurité
- Expert réponse à incident
- Intégrateur de sécurité
- Responsable du plan de continuité d'activité (RPCA)
- Spécialiste en gestion de crise cyber

Cibles et métiers visés

En termes de débouchés, les étudiants diplômés pourront rejoindre :

- Le ministère des armées, plus particulièrement la marine nationale comme officier embarqué, expert ou pour la conduite de programmes d'armement ;
- Les sociétés d'armateurs ;
- Les opérateurs d'infrastructures portuaires ;
- Les industriels des filières de la mer (chantiers, équipementiers de rang 1..) comme responsables de projet ou responsables sécurité numérique sur un programme;
- Des start-ups et entreprises innovantes qui pourront être lancées sur les nouveaux marchés en lien avec la sécurité et le domaine maritime

#4.

Conclusions et perspectives

Conclusion et perspective

- Une équipe sur le terrain et motivée
- Des soutiens des industriels et acteurs du monde académique, maritime et portuaire
- Un soutien fort et une commande de la part de la Marine nationale
- Une offre unique de formation et un potentiel d'innovation attendu

- https://www.chaire-cyber-navale.fr/
- https://www.imt-atlantique.fr/sites/default/files/document/mastere-specialise-cybersecurite-systemes-maritimes-portuaires.pdf

#4.

Annexe

Trame plus détaillée

- **UE 1 : Introduction et tronc commun**
  - Fondamentaux : les réseaux, cyberattaques récentes
  - Aspects sociaux et sociétaux dont gestion de confiance et de réputation numérique
  - Sécurité et informatique : cours par exemple de l'ANSSI sur les langages de programmation
  - Architecture des ordinateurs
  - Bases des réseaux : protocoles, architectures,
  - Bases des systèmes d'exploitation : Linux et Wi
  - Chiffrement et confidentialité des données, protection des secrets, méthodes,
  - Classes et natures des attaques : virus, chevaux de Troyes, malware, ransomware
  - Cryptologie (cryptographie/chiffrement
  - Sténographie et tatouage
  -
- **UE 2 : Questions politiques et juridiques**
  - Les attaques dans le cyber espace : nouvel environnement
  - Contexte stratégique et de souveraineté nationale – enjeux
  - Connaissance normes, standards et gouvernance
  - Politique de cybersécurité (europ et nationale)
  - Droit et réglementation (europe, national)
  - Introduction à la cyberdéfense
  - Droit et mer : spécificités
- **UE 3 : Cyber et conduite de projets maritimes**
  - Développement et ingénierie logicielle
  - Prise en compte de la sécurité dans les projets : analyse de risques, audits organisationnel et technique
  - Contributions des architectures à la sécurité
  - Certification des produits
  - Gestion de la sécurité
  - Spécificités marine et infrastructures portuaires
- **UE 4 : Sécurité des systèmes logiciels (Systèmes d'exploitation**
  - Réseaux et protocoles
  - Bases de données
  - Services externalisés (cloud, calcul déporté..)
  - Sécurité et système d'exploitation
- **UE 5 : Protéger les équipements et les équipages :**
  - Conception – sécurity by design
  - Modélisation de la menace
  - Equipements et architectures des réseaux :
    - firewall, filtrage, organisation du réseau et urbanisation, leurage
  - mise en œuvre des protection du système d'exploitation, virtualisation
  - plan de protection : plan de reprise d'activités PRA/PCA, résilience
  - obligations légales, cadre réglementaire, OIV….ISO
  - homologation
  - Tester la solidité de la protection : test de pénétration, …. Audit de sécurité
  - Prise en compte de l'évolution des vulnérabilités
  - Gestion des identités, contrôle des droits et des accès
  - Politique de sécurité dans l'entreprise
  - Cas maritime
- **UE 6 : sécurité des systèmes industriels et des composants (appliqué) (70h)**
  - Electronique et architecture matérielle
  - ICS et SCADA
  - Systèmes spécifiques et communications
  - Sécurité physique et sureté de fonctionnement
  - Spécificités – différences de la sécurité IT et OT
  - Pratique et programmation des SCADA
  - Attaques et challenges de la protection des équipement Scada
  - Organisation de la protection des équipements et du SI
  - Exemple d'attaques
  - MCO / MCS de ces systèmes de systèmes couplant IT / OT
  -
- **UE 7 : Réponse à incident / réaction à attaque / cyber résilience :**
  - CERT
  - SOC
  - Organisation d'une équipe cyber
  - Cadre réglementaire
  - Résillience, restauration, reprise, mode dégradé
  - Partage et mise en commun de bonnes pratiques
  - Suivi des vulnérabilités
  - Les entrainements des équipes et les exercices cyber
  - Gestion des patchs et mise à niveau logiciel : évaluer l'impact d'une menace
  - Visite d un SOC Marine et ou opérateur maritime
-

Trame plus détaillée

- **UE8 : Détecter une attaque :**
  - Intrusion détection IDS
  - Technique de collecte et traitement de logs : outils de type ELK
  - Analyse forensics
  - Analyse avancée : data science, IA, ….
  - Outil de monitoring des activites et tableaux de bord
  - Techniques pour réduire les faux positifs et améliorer les IDS
  - Système de surveillances
  - Les sondes et analyse des alertes
  - Cas marine
- **UE 9 : contexte Maritime**
  - Des activités transverses - avec des visites et mises en situation pour découvrir le milieu
  - Retours d expérience et analyse d'attaques récentes
  - Spécificités du milieu Maritime et des ports
  - Le bateau connecté – la flotte connectée – le port connecté
  - Un exercice cyber avec un contexte marine à préparer
  - Maintien en condition opérationnelle / sécurité – MCO / MCS et Marine
  - Aspects drones - navires autonomes -
  -

- **UE 5 : Projet industriel**
-

Un projet et PFE

- Un projet transverse :
  - Idéalement qui recoupe plusieurs thématiques couvertes par le MS et les UE
  - Couplé avec l'UV gestion de projets maritimes
  - Un sujet qui pourrait être établi en lien avec un des partenaires de la chaire et/ou un académique
  - Un projet tutoré avec un académique

- Un PFE / mémoire
  - En lien avec un des métiers identifiés
  - Un sujet validé et suivi par un académique