Opération
i-Naval

Innovations du domaine naval de défense
https://i-naval.fr

1. Périmètre de l'opération

DGA Techniques navales (DGA TN) et l'Université de Toulon organisent entre fin juin et mi-juillet 2022 à Toulon (Var) l'événement « Opération i-Naval 2022 », en partenariat avec la Marine nationale, l'Université de Toulon, la Métropole TPM (TVT Innovation) et la Région Sud-PACA.

Cet événement vise à mettre en lumières des innovations technologiques nationales intéressant le domaine naval de défense, au travers d'une démonstration au profit de parties intéressées locales et nationales (élus, autorités civiles et militaires, monde académique, industrie).

Un scénario opérationnel validé par la Marine nationale permettra d'alterner pitchs et séquences de démonstrations de technologies innovantes (démonstrations physiques ou projetées sur écrans géants) :

- le scénario, restant à affiner, s'articulera autour de 4 séquences maximum parmi les suivantes :
  - combat connecté sous-marin,
  - entrainement au combat des marins,
  - réaction à un incident cyber,
  - lutte contre la pollution,
  - lutte contre la piraterie et les trafics.
- chaque séquence permettra de mettre en situation opérationnelle 3 ou 4 innovations.

Il s'agit donc de dénicher « des pépites » proposant un potentiel intérêt pour les forces, d'identifier les technologies à forte valeur ajoutée susceptibles de pouvoir alimenter ce scénario.

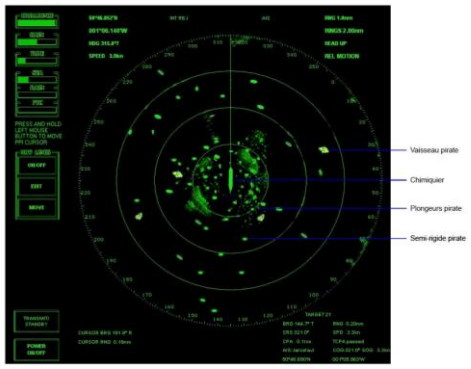
La recherche de solutions est volontairement étendue, afin d'avoir une flexibilité large pour l'élaboration du scénario détaillé. Les solutions, retenues ou non pour l'opération i-Naval, pourront faire l'objet d'échanges avec les clusters d'innovation navale Gimnote (Toulon) et Orion (Bretagne).

Pour information, le site physique retenu pour l'organisation de l'évènement est en cours de définition dans l'aire toulonnaise.

2. Contexte immersif

Le scénario opérationnel s'inspirera des travaux de la saison 0 « Les nouveaux pirates » et de la saison 1 « La sublime porte s'ouvre à nouveau » de la RED TEAM de l'Agence d'Innovation de Défense (AID).

Les nouveaux pirates



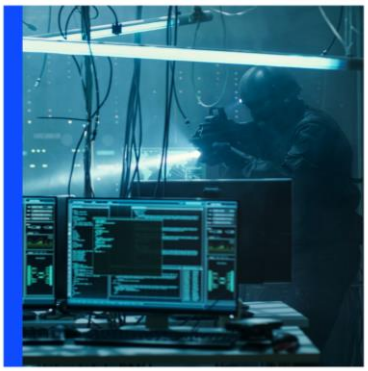
Deux scénarios, P-Nation et Barbaresques 3.0, viennent donner corps à la possibilité d'une menace stratégique de nouveaux pirates.

Le premier imagine la création d'une nouvelle nation pirate liée au changement climatique.

La seconde explore une faiblesse de la numérisation du monde : le hacking possible des implants neuronaux.

La sublime porte s'ouvre à nouveau

La course effrénée à l'armement hypervéloce et furtif a conduit à l'émergence du bouclier défensif (excluant l'être humain de la boucle et plaçant l'IA au cœur du dispositif), puis à l'hyperforteresse.



Le champ de bataille est marqué par un raccourcissement des distances et du temps, les nouvelles technologies démontrent une triple instantanéité : de l'action offensive d'abord, de la défense ensuite et de l'analyse et du traitement de la donnée.

Le rôle du soldat sera en formation permanente pour demeurer apte à gérer un environnement technologique dont il sera le pivot. Ultra-connecté, il intégrera des pare-feu et un camouflage cyber.

https://redteamdefense.org/

3. Séquences opérationnelles

Séquence 1 : Combat connecté sous-marin

La situation

Des navires de la Marine Nationale interviennent lors d'une situation de crise, au large d'un pays hostile. La situation se tend, la force navale doit à la fois se protéger et coordonner son action de combat.

L'analyse technique

L'action collaborative sous-marine vise à évaluer et analyser la situation opérationnelle en s'appuyant sur des informations issues de capteurs hétérogènes répartis sur des plates-formes de surface et sous-marines, habitées ou non. L'analyse doit être partagée au sein des plates-formes, dans un milieu étanche aux rayonnements électromagnétiques rendant difficiles la communication et le positionnement précis, et réduisant les capacités d'observation.

Les solutions techniques possibles (liste non exhaustive) :

- autonomie décisionnelle et classification par intelligence artificielle ;
- détection et identification de menaces sous-marines à longue distance ;
- réseaux de bouées et de drones ;
- fusion de données massives et multicapteurs ;
- aide à la décision ;
- communication acoustique ;
- imagerie à bas niveau de lumière, sonar, bathymétrie ;
- sondeur acoustique multifaisceaux (SMF) ;
- robotique sous-marine, engin autonome sous-marin (AUV).

Séquence 2 : Entrainement au combat des marins

La situation

Le maintien de la supériorité opérationnelle repose certes sur les technologies, mais également sur la préparation du personnel. Ainsi, il impose une résilience de l'équipage et des systèmes tant sur le plan individuel (connaissances métier et force morale, durcissement des matériels, etc.) que sur le plan collectif.

L'analyse technique de la situation

La résilience suppose :

- un entraînement aux différentes fonctions (opérationnelles et réaction face aux avaries) et sur des exercices à bord ;
- une capacité des systèmes, en particulier en espace confiné (gain de place, éclairage artificiel, etc.), à s'adapter aux différents utilisateurs.

Les solutions techniques possibles (liste non exhaustive) :

- simulateur-métier, 3D, réalité mixte et/ou augmentée, enseignement assisté par ordinateur ;
- intelligence des artefacts dans les scénarios d'entraînement (variétés de comportement des personnages non joueurs) ;
- simulation distribuée (*wargaming*) ;
- présentation et prise de l'information complexe (IHM innovantes) ;
- ergonomie des systèmes.

Séquence 3 : Réaction à un incident cyber

La situation

Des navires de la Marine Nationale interviennent lors d'une situation de crise, au large d'un pays hostile. La situation se tend, des tentatives d'agressions électromagnétiques et cyber sont détectées sur l'un des navires.

L'analyse technique

Les agressions électromagnétiques se caractérisent à la fois par du brouillage des capteurs (radars, guidage-navigation) et du leurrage (diffusion de fausses informations, notamment via l'AIS) ; l'objectif est détecter ces agressions et mettre en place les contre-contre-mesures appropriés.

Les attaques cyber ciblent les automates présents à bord du navire, notamment pour la conduite de la plate-forme : l'objectif est de les détecter et de maintenir le navire en conditions de sécurité. Les modes d'attaque cyber incluent la bombe logique (installée à quai ou par malveillance à bord) et la pénétration via les réseaux de communication ; un navire se caractérise par une architecture de télécommunication relativement ouverte vers les autres navires du groupe naval (en particulier, étrangers, dans le cas de coalition), et multi-niveaux (selon la classification des données traitées).

Les solutions techniques possibles (liste non exhaustive) :

- intelligence artificielle ;
- analyse comportementale ;
- communications sécurisées ;
- authentification ;
- service d'accès sécurisé hybride / multi-niveaux ;
- maintien en condition de sécurité (mise à jour, détection, qualification / attribution, remédiation) ;
- dispositifs de détection de brouillage et de leurrage GPS ou AIS.

Sont exclues *a priori* les actions menées par un SOC et/ou hors temps réel (veille sur la menace, développement de solutions de protection contre le brouillage et le leurrage, formation…).

Séquence 4 : Lutte contre la pollution[i]

La situation

Dans le cadre de l'action de l'Etat en mer, les navires de la Marine nationale doivent faire face à une pollution maritime.

L'analyse technique de la situation

La lutte contre la pollution suppose de pouvoir surveiller, détecter, identifier et traiter une pollution à large spectre (hydrocarbures, substances nocives, macro-déchets, etc.) sur une zone évolutive (extension des nappes, déplacement, conditions météorologiques, état de mer, en surface/profondeur, etc.).

Les solutions techniques possibles (liste non exhaustive) :

- (nano)-satellite d'observation (imagerie optique, radar) ;
- simulations numériques / algorithmes prédictifs ;
- équipements spécifiques d'isolement et/ou de collecte : barrages, rideaux de bulles, tapis roulant, écrémeurs, pompes, absorbants (à base de nano-structures magnétiques, bio-tissu), robot.

Séquence 5 : Lutte contre la piraterie et les trafics[i]

La situation

Dans le cadre de l'action de l'Etat en mer, les navires de la Marine nationale doivent lutter contre la piraterie et les trafics.

L'analyse technique de la situation

La sécurité maritime peut être compromise par les 7 menaces suivantes, définies par l'ONU : piraterie et vol à main armé contre les navires, actions terroristes impliquant le transport maritime/les installations « offshores » et autre intérêts maritimes, les trafics illicites d'armes et d'armes de destruction massive, les trafics illicites de drogues et de substances stupéfiantes, les trafics d'êtres humains par la mer, la pêche illégale non reportée no-régulée, les atteintes volontaires et illégales à l'environnement marin).

Les solutions techniques possibles (liste non exhaustive) :

- (nano)-satellite d'observation (imagerie optique, radar) ;
- autonomie décisionnelle et classement par intelligence artificielle ;
- effecteurs létaux et non létaux (projecteurs lumineux, canons sonores, fumigènes).

[i] Les missions opérationnelles d'action de l'Etat en mer, concernent : la sécurité maritime et le sauvetage en mer, la sûreté maritime et portuaire, la lutte contre les trafics illicites et contre les rejets illicites (pollutions volontaires), la lutte contre l'immigration illégale par voie maritime et la surveillance et contrôle des pêches. Elles sont assurées par : la Marine nationale, les garde-côtes, la Gendarmerie nationale, les Affaires maritimes, la Sécurité civile, la Douane et le cas échéant par des associations ou des sociétés privées à qui sont confiées des missions de service public (ex. Société nationale de sauvetage en mer).