« Exercice i-Naval 2023 »
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 mai et mi-juin 2023 à Toulon (Var) l'événement « Exercice i-Naval 2023 », 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). Il permettra d'alterner pitchs et séquences de démonstrations de technologies innovantes (démonstrations physiques ou projetées sur écrans géants). Il intègrera également un retour d'expérience de l'exercice interarmées « HEMEX Orion », déroulé fin février-début mars 2023.

Ainsi, pour cette édition, des innovations feront l'objet d'expérimentations opérationnelles sur le thème « combat naval littoral / côtier », dans le cadre de « HEMEX Orion ». En complément, les thèmes « cyberdéfense » et « entraînement et formation », déjà à l'honneur en 2021 et 2022, seront repris pour être approfondis.

Il s'agit donc d'identifier les technologies et projets :

- proposant un intérêt potentiel pour les forces ;
- susceptibles d'être intégrés dans les séquences d'expérimentation ou de démonstration.

Les solutions, retenues ou non pour « Exercice i-Naval 2023 », pourront faire l'objet d'échanges avec les clusters d'innovation navale Gimnote (Toulon) et Orion (Bretagne).

2) Séquences opérationnelles

Séquences 1 et 2 : Combat naval littoral / côtier

La situation

Des bâtiments de la Marine nationale sont au large d'une côte hostile et préparent un débarquement de forces spéciales.

Au cours du débarquement, l'ennemi résiste et fait usage de ses armes ; un blessé doit être évacué vers les bâtiments de soutien. Un appui feu est demandé.

L'analyse technique

Afin de limiter le risque pour le débarquement des forces spéciales, il s'agit dans un premier temps de faire du renseignement sur la zone de débarquement, d'évaluer et analyser la situation opérationnelle en utilisant les informations issues de capteurs hétérogènes répartis sur plusieurs plates-formes et de différentes natures. Ces informations permettent d'élaborer une tactique optimale pour le débarquement des forces, qui limite la prise de risque.

Dans un second temps, les forces spéciales progressent jusqu'à la côte.

Il s'agit d'assurer le sauvetage des blessés, en réalisant un télé-diagnostic et en définissant les chemins d'évacuation.

La réalisation de l'appui feu passe par l'utilisation d'informations issues de capteurs hétérogènes, répartis sur plusieurs plates-formes et de différentes natures, notamment pour la désignation de cibles.

Ces opérations nécessitent un réseau de communication opérationnel et sûr.

Les solutions techniques possibles (liste non exhaustive) :

- autonomie décisionnelle et classification par intelligence artificielle ;
- aide à la décision ;
- robotique sous-marine, engin autonome sous-marin (AUV) ;
- capteurs sous-marins (toute technologie), pour détection d'obstacles ou observation ;
- systèmes de communications multi-milieux ;
- embarcations de débarquement ;
- médecine de combat, télédiagnostic.

Séquence 3 : Entrainement et formation

Situation

Des navires de la Marine nationale interviennent lors d'une situation de crise, au large d'un pays hostile. L'équipage et les équipes d'assaut doivent se tenir prêt à une intervention.

L'analyse technique

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.

La résilience suppose :

– un entrainement aux différentes fonctions (opérationnelles et face aux avaries),

notamment pour faire face à un environnement spécifique (NRBC…) ;
- une capacité des systèmes à s'adapter aux différents utilisateurs.

Les objectifs de formation sont d'améliorer à la fois la performance individuelle dans la maîtrise des équipements, et la performance collective (notamment en situation d'urgence).

La représentativité et la gestion des données sont des enjeux importants, notamment en situation de combat.

Les solutions techniques possibles (liste non exhaustive) :

- simulateur métier, 3D, réalité mixte ou augmentée, métavers ;
- enseignement assisté par ordinateur ;
- intelligence des artefacts dans les scénarios d'entraînement (variétés de comportement des personnages non joueurs) ;
- simulation distribuée (*wargaming*) ;
- outils de simulation notamment le rejeu à partir de données réelles, le débriefing et la scénarisation des situations simulées ;
- système de gestion et de partage des data pour améliorer le réalisme des simulations.

Séquence 4 : Cyberdefense

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 de détecter ces agressions et de 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 et le système de direction de combat : 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) :

- blockchain ;
- cybersurveillance en temps réel ;
- 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 ;
- solutions de chiffrement (notamment sur support amovible) et chiffrement

post-quantique ;
- moyen de maitriser les empreintes numérique et électromagnétique d'une force navale (ex : surveillance des émissions des téléphones portables).