# Quels systèmes de combat pour les marines au XXI$^{e}$ siècle ?

Enseigne de Vaisseau de 2$^{ème}$ classe (R) Laurent Zeller

**CENTRE D'ENSEIGNEMENT SUPERIEUR DE LA MARINE - ETUDES**

Faute d'avoir été spécifiquement « équipé » par la nature, l'homme, pour coexister avec le milieu marin, ne peut avoir recours qu'à de piètres performances de natation, quand on les compare à celles des êtres que l'évolution a favorisés de ce point de vue. Sans l'aide de la technologie, il ne peut se déplacer, transporter des objets ou se battre bien longtemps. Son corps est rapidement épuisé par l'effort fourni pour se mouvoir et maintenir une température corporelle constante. En conséquence, notre capacité à maîtriser le milieu marin est directement tributaire du niveau de technologie que nous utilisons. De la pirogue à la frégate européenne multi-missions, les différences de niveau technologique expliquent en partie les rapports de forces entre les puissances maritimes.

En ce début de XXI$^{e}$ siècle, les technologies se développent et se renouvellent à un rythme jamais connu. Le développement des technologies de l'information est particulièrement frappant pour nos contemporains, certains l'ont même appelé *« la troisième révolution industrielle »*. Elle transforme en profondeur nos vies quotidiennes, en particulier dans les pays industrialisés. Le monde maritime est déjà touché par cette révolution comme en témoigne l'informatisation poussée des passerelles des navires. Cependant, la révolution informatique n'a pas fini de porter ses fruits. Les développements les plus importants auront lieu dans les dix ou vingt prochaines années.

Deux aspects des technologies de l'information auront un impact décisif sur la guerre maritime :

- La robotique qui permet aujourd'hui de concevoir des drones évoluant en surface, dans les airs et sous l'eau,
- Le développement des réseaux qui permet un partage de plus en plus rapide et de plus en plus complet des informations que possèdent les différents acteurs d'un théâtre d'opérations.

Bien que la guerre froide soit terminée depuis bientôt vingt ans, les flottes des puissances maritimes sont essentiellement dimensionnées et équipées avec du matériel conçu pour l'affrontement Est-Ouest en raison de la durée très longue des programmes d'équipements militaires. Les nouvelles technologies qui seront à la disposition des marines du monde entier d'ici quelques dizaines d'années s'articuleront dans un contexte stratégique multipolaire où les risques sont beaucoup plus diffus.

Comment ces nouvelles technologies vont-elles s'articuler avec le contexte géostratégique des vingt prochaines années ?

Au-delà du simple catalogue des nouvelles technologies que les puissances maritimes pourront utiliser d'ici quelques dizaines d'années, nous aimerions montrer ici l'intérêt de ces progrès pour les nouvelles missions qui incombent aux marines du monde entier. L'évolution du contexte géostratégique nous laisse en effet entrevoir que les priorités données à l'action navale sont en pleine mutation. On peut noter, parmi d'autres missions nouvelles, la lutte contre la piraterie, la défense de l'environnement et la lutte pour le contrôle de nouvelles zones stratégiques comme les routes arctiques que le réchauffement climatique dégage.

Nous examinerons d'abord l'un des aspects les plus médiatisés des progrès technologiques contemporains : les drones, en décrivant quelques-uns des prototypes ou démonstrateurs existants aujourd'hui. Nous verrons ensuite quels sont les progrès techniques à accomplir pour que les opérations militaires deviennent véritablement réseau-centré.

# I. Drones

## *A. Pourquoi les drones ?*

L'essor des drones est issu de la rencontre entre la possibilité de leur création et le besoin de véhicules automatisés par les forces armées. D'un côté, les formidables progrès accomplis dans le domaine de la robotique et celui de la miniaturisation de l'informatique autorisent aujourd'hui les ingénieurs à concevoir de nombreux types de drones aux capacités de mouvement et d'emport de plus en plus variés. De l'autre, la volonté de ne pas exposer inutilement des vies humaines et de pouvoir démultiplier rapidement sa force amène les puissances navales à en commander. Un drone sous-marin de neutralisation de mines, tel que le *Long-term Mine Reconnaissance System (LMRS)* de *Boeing*, évite d'exposer l'ensemble de l'équipage (une cinquantaine de marins) d'un chasseur de mine aux risques liés au déminage. Par ailleurs, lorsque cet équipement sera arrivé à maturité industrielle, ne serait-ce que pour des raisons de taille, il sera beaucoup plus facile d'en fabriquer en grande série et de les déployer à partir d'un grand nombre de navires. Chaque navire pourrait alors posséder sa propre capacité de lutte contre les mines. On peut distinguer trois types de drones en fonction du milieu dans lequel ils évoluent : aérien, surface, sous-marin. Nous nous limiterons ici aux drones susceptibles d'être utilisés par les marines, nous excluons donc les drones terrestres.

## *B. Les drones aériens*

### *1.* Le *Bell Eagle Eye*

Bien que les drones aériens (Unmanned Aerial Vehicle UAV) soient utilisés, depuis des années, par de nombreuses armées de par le monde et en particulier par les armées américaines et israéliennes (le *Mastiff* de *Tadiran Electronic Industries* effectuait des missions de reconnaissance pour Israël pendant la guerre du Liban en 1982), leur déploiement en milieu marin est plutôt récent. L'un des concurrents du programme de drone aérien maritime à décollage vertical fut le *Bell Eagle Ey*e. Dans leur programme de renouvellement de leurs matériels, les US Coast-Guards avaient, un temps, envisagé d'acheter de nombreux drones de ce type. Le démonstrateur fit son premier vol en 1998.

Il s'agit d'un drone à décollage et atterrissage vertical (VTOL Vertical Take-Off and Landing) utilisant une technologie de rotor basculant (tilt-rotor) à l'image du *V22 Osprey*. Cette technologie lui permet de ne pas sacrifier la vitesse maximum (360 km/h) à la capacité d'atterrir et de décoller verticalement. Celle-ci est essentielle, aussi bien pour les Coast Guards que pour la Navy, puisque cela veut dire que le drone doit être capable d'apponter et de décoller d'une plate-forme de navire.

Possédant une charge utile de 90 kg, il serait capable d'emporter de nombreux capteurs destinés à des missions de surveillance maritime.

La France cherche également à se doter d'un Drone VTOL Interarmées (DVI). *L'Eagle Eye* de *Bell* figure parmi les concurrents de cette étude de définition, dans une version où l'hélicoptériste américain fournit la cellule et intègre les systèmes embarqués définit par le gouvernement et développés par l'équipementier *Sagem*.

Par ailleurs, *Bell* a noué un partenariat avec *Rheinmetall AG* pour proposer une autre version de son *Eagle Eye* au gouvernement allemand.

### 2. D'autres drones

Début 2008, une revue parlementaire du programme « Deepwater », a mis au jour des retards importants dans le programme de développement de l'*Eagle Eye*. Les crédits initialement

attribués à ce programme par les Coast-Guards sont désormais gelés. Une solution commune avec l'U.S. Navy, qui faisait développer de son côté le *Fire Scout* de *Northrop-Grumman* et *Ryan Aeronautical of San Diego,* est privilégiée. Le *Fire Scout*, est fondé sur une architecture d'hélicoptère à rotor fixe plus classique. Il est multi-rôles avec une capacité d'emport d'armes. Cela signifie également que le partenariat avec *Sagem,* pour fournir à la DGA (Délégation Générale pour l'Armement) un DVI, est très fragilisé.

Parmi les derniers progrès accomplis sur le front de drones aériens destinés aux marines, des essais d'appontage sur une frégate ont été effectués pour la première fois en haute mer en octobre 2008. Le drone *CAMCOPTER S-100* de la société autrichienne *Schiebel* a apponté avec succès sur le *Montcalm* grâce au Système d'Appontage et de Décollage Automatique développé par DCNS, constitué d'un mat infrarouge. Celui-ci a permis au drone de se poser avec une précision de 30 cm afin qu'il puisse harponner la grille de la plate-forme hélicoptère.

### *C. Les drones de surface*

Plus marins encore que les drones aériens, les drones de surface sont déjà une réalité avec, par exemple, le *Spartan Scout*. C'est un drone de surface, développé par le *Naval Undersea Warfare Center* de Newport en collaboration avec *Radix Marine*, *Northrop-Grumman*, et *Raytheon*. Il a été conçu à partir d'une coque semi-rigide en deux versions : de 7 m et de 11 m.

Le *Spartan*, qui a fait l'objet d'une coopération entre les États-Unis, Singapour et la France, peut être équipé de différents modules. Une version armée, achetée par la garde-côtière de Singapour, autorise à approcher de près des navires suspects sans pour autant exposer des équipages à une action brusque et malveillante de ceux-ci. Elle permet d'assurer une surveillance des eaux territoriales à moindres frais. Une autre version, développée par la France, dispose d'un sonar trempé. Elle a été développée pour la lutte anti-sous-marine et pourrait être, dans certaines opérations, une alternative à l'emploi coûteux de l'hélicoptère. Enfin, un module a été développé, permettant d'identifier des gaz ou des substances toxiques dans une zone à risques pour l'homme.

### *D. Les drones sous-marins*

La prospective sur les drones sous-marins se développe fortement sous la double impulsion des marines et des industriels. Pour les marines, la première utilité d'un drone sous-marin est la lutte contre les mines. Le *Long Terme Mine Reconnaissance System* décrit en introduction, est le drone par excellence tel qu'il intéresse les marines.

Ces technologies sont déjà utilisées dans le civil. Elles sont extraordinairement utiles aux compagnies pétrolières qui doivent entretenir des pipelines sous-marins, ainsi qu'aux industriels garants de l'intégrité des câbles sous-marins, ou bien de tout autre équipement sous-marin.

Les défis techniques à relever pour les drones sous-marins sont encore plus importants que ceux rencontrés par les drones aériens et de surface. L'essentiel des difficultés réside dans les communications entre le drone et le monde extérieur, les ondes électromagnétiques traversant difficilement le milieu marin. Cela implique des contraintes sur la définition des missions, ainsi que sur la précision des centrales inertielles embarquées. En effet, le drone sous-marin, à moins de faire surface à intervalles réguliers, n'est pas capable d'entrer en contact avec les satellites de positionnement tel que le GPS[1].

[1] Il existe cependant des systèmes dit « GPS sous-marins », comme celui développé en France par la société ACSA, qui permettent d'obtenir un référencement absolu précis en utilisant des bouées dont la partie sous-marine est équipée d'un système acoustique qui positionne, en relatif, le drone par rapport à la bouée et une partie aérienne munie d'un récepteur GPS qui positionne la bouée en coordonnées absolue. La combinaison de ces deux référentiels donne la position en coordonnées absolues du drone sous-marin.

Exemples de drones sous-marins en cours de développement :

- Le *Long-term Mine Reconnaissance System (LMRS)* de *Boeing* : drone à longue endurance capable d'être mis en œuvre et récupéré à partir d'un sous-marin pour la reconnaissance en opération amphibie, la protection d'une force aéronavale ou le transit sûr dans une zone de danger « mines » ;
- La *Daurade* de la société ECA : drone prévu pour l'évaluation rapide de l'environnement (REA) afin de préparer des opérations de lutte sous la mer ;
- *L'AsterX* : drone de taille moyenne pour la surveillance sous-marine en domaine côtier. Il a été développé par l'*IFREMER* et fabriqué par *ISE Ltd (Vancouver) ;*
- *L'Alister,* drone de la société ECA, est un engin de lutte contre les mines, le soutien rapproché d'une force contre la menace des mines, la reconnaissance discrète de zone.

Les drones qu'ils soient aériens, de surface ou sous-marins, permettent de limiter les risques encourus par les marins et de démultiplier les capacités d'observation et d'action d'une marine. Toutefois pour atteindre ces buts au mieux, ces « capteurs déportés » doivent s'inscrire dans une technologie de partage de l'information plus globale rendue possible aujourd'hui par les progrès de l'informatique et des télécommunications. Prenons l'exemple d'un drone repérant une embarcation suspecte. Ne serait-il pas bénéfique que les informations qu'il capte sur celle-ci soient diffusées simultanément à tous les acteurs en ayant besoin, du commandement de l'opération à l'équipe d'intervention qui se prépare à l'abordage et aux aéronefs qui vont l'appuyer ? De même, cette équipe d'intervention aurait tout à gagner de pouvoir disposer d'informations sur l'embarcation provenant simultanément du drone, du bâtiment qui abrite le commandement de l'opération et des aéronefs présents au moment de l'abordage.

Ce type de communications implique une révolution technologique et organisationnelle très importante des forces armées et des marines en particulier : les Opérations Réseau-Centré (ORC)[2] .

# II. Opérations Réseau-Centré

## *A. Principes*

Le principe des ORC est la communication, par un réseau numérique, entre les différents acteurs du théâtre des opérations. L'objectif est de transformer un avantage, en termes d'informations, en avantage militaire opérationnel au travers d'un travail en réseau robuste entre les différents acteurs de l'opération.

Quatre hypothèses sont à l'origine du concept d'ORC :

- Une force armée équipée d'un réseau robuste améliore le partage de l'information en son sein ;
- Le partage de l'information améliore la qualité de l'information ainsi que la mise en commun de la connaissance d'une situation ;
- La mise en commun de la connaissance d'une situation permet la collaboration et l'autosynchronisation qui améliorent la durabilité et la vitesse du commandement ;
- À leur tour, celles-ci améliorent résolument l'efficacité opérationnelle.

[2] En anglais Network-Centric Opérations (NCO)

Les réflexions sur la guerre infocentrée sont nées de l'étude de cas pratiques d'entreprise qui utilisent les réseaux pour améliorer l'analyse de situation, contrôler précisément l'inventaire et la production tout en surveillant les relations client.

On distingue trois domaines :

Le domaine physique où les évènements ont lieu et où les capteurs et les individus peuvent les percevoir. Les données émanant de ce domaine sont ensuite transmises au moyen d'un domaine d'information. Enfin, ces données sont reçues et traitées par un domaine cognitif où elles sont évaluées et où la décision d'agir en fonction de celles-ci est prise.

On pourrait imaginer que les unités opérationnelles soient capables, sur le terrain, de retirer de l'information *ad hoc* (concept de pull) provenant des autres armées plutôt que de devoir compter sur les informations fournies par les autres services (push). En ce sens, on se rapprocherait plutôt de ce que nos contemporains connaissent dans Internet comme le peer-to-peer.

Dans les principes identifiés, la Net-Centric Data Strategy (NCDS, 2003) définit trois éléments clés :

- Les communautés d'intérêts ;
- Les standards de métadonnée ;
- Les services d'entreprise « Global Information Grid » ;

NCDS introduit sept objectifs aux données :

- Visible ;
- Accessible ;
- Gestion institutionnalisée des données ;
- Compréhensible ;
- Fiable ;
- Interopérable ;
- Répondant aux besoins des utilisateurs.

C'est le troisième des principes introduits par NCDS, que nous allons examiner maintenant

## *B. Global Information Grid*

### 1. Une initiative du Département de la Défense des États-Unis

Le Département de la Défense des États-Unis a décidé que la première réalisation concrète qui viendrait soutenir la mise en place d'ORC est la Global Information Grid (GIG, Grille d'Information Global). Au sein de la marine américaine, le concept d'ORC se traduit concrètement par un projet tel que le Cooperative Engagement Capability (CEC). Il vise à établir une vue aérienne de très haute qualité par le partage de données émanant de capteurs appartenant à diverses unités du champ de bataille : navires, avions d'observation, etc. Le CEC est considéré comme un précurseur de la GIG, qui se décline pour sa part dans toutes les armées.

### 2. Les objectifs de la GIG

L'ambition du GIG est d'être aux composantes du Département de la Défense, ce qu'Internet est aux particuliers. C'est-à-dire un réseau qui permet à ses multiples utilisateurs de tirer profit de la multiplicité des sources pour aller chercher l'information dont ils ont besoin au moment où ils en ont besoin. Toutefois, il ne s'agit pas uniquement d'un recueil d'information, il

s'agit également de pouvoir éventuellement prendre le contrôle à distance des capteurs ou de vecteurs automatiques. Un exemple parmi mille : un drone de reconnaissance pourrait prendre le contrôle d'un missile tiré par un avion, pour le guider jusqu'à la cible. L'aéronef, n'utilisant pas son radar, est donc moins susceptible d'être détecté par l'ennemi.

## 3. Producteurs et consommateurs de données

Le concept de partage d'information implémenté dans la GIG est un concept à la fois pluri-fournisseurs et pluri-demandeurs. En effet, un capteur, un vecteur ou bien une personne mettant à disposition des données sur la GIG, doit être en mesure de les fournir simultanément à de nombreux demandeurs d'informations. Symétriquement un capteur, un vecteur ou bien une personne demandant de l'information via la GIG doit être en mesure de recevoir de nombreuses sources d'informations simultanément.

Ces consommateurs de donnés, qu'on ait anticipé leur besoin ou non, doivent pouvoir voir, accéder et comprendre l'information présente sur la GIG à partir du moment où ils sont autorisés à la voir. Tout ceci afin de pouvoir trouver et récupérer l'information (find and pull) dont ils ont besoin en quasi-temps réel. Une manière de mettre ceci en œuvre est de mettre en place un système de publication et d'abonnements à des fils d'information, un peu à la manière des flux RSS communément utilisés sur Internet aujourd'hui.

## 4. Technologies de l'information utilisées

Les données sont transmises en utilisant l'IP (Internet Protocol) qui est une manière d'envoyer des données sous forme de paquets formatés. Grâce à cette technologie, le moyen de transmission (fibre optique, satellite, radio UHF, etc.) est transparent pour l'utilisateur. Peu importe que les informations qu'il demande ou bien que les ordres qu'il donne transitent par l'un ou l'autre de ces moyens.

Peu importe également qu'il appartienne à l'armée de terre et que les fusiliers-marins, à qui appartient le capteur de données, fassent partie de la marine. S'il est autorisé à les voir, il obtiendra les données. L'idée est de pouvoir répondre à tous les besoins en information, notamment ceux des forces déployées en opération.

Simultanément, il ne faut pas perdre de vue la nécessité d'être capable de répondre à de nouveaux besoins en terme de performance et de sécurité, émanant de progrès techniques ou opérationnels. Certains protocoles de transfert de haute performance ne sont pas compatibles avec la version actuelle de l'IP. À terme, l'idée est de développer des passerelles entre ces réseaux utilisant l'IP pour obtenir une compatibilité maximale.

## 5. Et en France ?

L'équivalent français de la GIG est la Bulle Opérationnelle Aéro-Terrestre (BOA). Un plan d'études amont a été lancé en 2006 sur ce concept. Comme son appellation l'indique, elle est nettement plus centrée sur l'opérationnel. De surcroît, elle est pilotée par l'armée de terre. Ce qui n'exclut pas forcément une intégration des autres armées, mais qui restreint tout de même l'ambition de ce concept par rapport à celui de la GIG.

## 6. Les enjeux de Sécurité

L'un des plus grands défis de la GIG est d'assurer une très robuste sécurité des données. En effet, la disponibilité simultanée d'autant de données pourrait être utilisée avec un profit immense par l'ennemi. Une brèche dans la sécurité permettrait potentiellement à la partie adverse d'avoir accès aux informations connues par les forces, à les manipuler, éventuellement à prendre le contrôle de leurs vecteurs. Il y a un équilibre difficile à trouver entre des forces déployées qui

doivent être capables d'accéder au maximum de données dans le minimum de temps, et simultanément de protéger ces données de leur exploitation par l'ennemi.

En conclusion, nous avons vu que la révolution technologique rendue, indispensable par l'avènement d'opérations réseau-centré, ne nécessite pas de révolution au niveau des capteurs, ou bien des vecteurs utilisés par les forces armées. Elle nécessite une révolution dans la manière dont la mise en réseau de ceux-ci est conçue. Par exemple, il suffit de combiner les images radar provenant d'un drone, d'un chasseur et une vue satellite (technologies existantes), pour former une image d'une précision et d'une richesse jamais vue jusqu'ici, à destination des unités déployées sur le terrain.

Tout ceci suppose que ces technologies, différentes dans leur fonctionnement et leurs standards, arrivent à communiquer entre elles. Ceci ne devient possible que par l'adoption de standards de métadonnées. Elle ne se fera pas sans une ouverture de l'architecture des systèmes d'armes afin qu'ils puissent communiquer entre eux. Cette architecture ouverte, une forme de nouvelle standardisation, appliquée au-delà du champ des communications, doit également permettre aux forces armées de se libérer des carcans des systèmes propriétaires. Elle doit enfin faciliter l'utilisation de solutions commerciales sur étagères (COTS Commercial Off The Shelf) dans la perspective d'une maîtrise des coûts et des délais des programmes d'armement.

Dans quelques dizaines d'années, de toute évidence, les marines militaires seront plus automatisées en faisant largement appel à des drones, plus réseau-centrée avec une gestion de l'information comparable à celle que l'on trouve sur Internet. Enfin, l'architecture des systèmes d'armes qu'elles utiliseront sera plus ouverte et fera davantage appel à des solutions sur étagère.