INTERNATIONAL > La politique européenne de surveillance maritime

DROIT > Or bleu et criminalité

TECHNIQUE > La sûreté, facteur de développement des ports

REVUE
de la gendarmerie nationale

REVUE TRIMESTRIELLE / MARS 2017 / N° 257 / PRIX 6 EUROS

SÛRETÉS
MARITIME ET AÉRIENNE

AVEC LA COLLABORATION DU CENTRE DE RECHERCHE DE L'ÉCOLE DES OFFICIERS DE LA GENDARMERIE NATIONALE

retour sur images NUMÉRO 256

© serpeblu-Fotoli

SMARTER SECURITY – UNE SÉCURITÉ INTELLIGENTE POUR LES TECHNOLOGIES DU FUTUR

La digitalisation du monde constitue une troisième révolution après l'invention de l'imprimerie et la révolution industrielle. La transformation qui en résultera doit reposer sur des bases de sécurité et de confiance. Outre des choix technologiques, l'évolution supposera une régulation, comme celle du commerce international ou des espaces maritimes. Les acteurs régaliens, associés aux acteurs privés, doivent orchestrer un consensus entre les obligations commerciales et le respect de l'intégrité de la personne.

RETROUVEZ EN PAGE 102 COMMENT CONCILIER LES IMPÉRATIFS ÉCONOMIQUES ET UNE SÛRETÉ DES PORTS

© HAROPA

Le commerce est le plus
grand de tous les intérêts politiques

Joseph Chamberlain – Discours de Birmingham – 13 novembre 1896

La sûreté des espaces maritimes et aéroportuaires dépend essentiellement d'une législation mondiale, européenne déclinée de manière similaire sur les territoires nationaux. L'importance vitale des échanges économiques maritimes et aériens impose une stratégie de sûreté qui permette d'accompagner ou d'anticiper l'évolution des menaces terroristes et criminelles.

Les économies mondiales sont distribuées autour de structures nodales constituées par les aéroports et les ports qui sont le cœur d'un réseau de distribution vers les zones de production et de consommation, via les voies ferrées, routières et les voies navigables.

La gendarmerie nationale, comme les acteurs régaliens, ne peut embrasser seule la totalité des flux matériels et humains de ces surfaces spécialisées ni réguler un transport multimodal. Une analyse du renseignement, une exploration scientifique des contenus, une collaboration active et loyale avec les autorités de tutelles des zones portuaires et aéroportuaires, ainsi qu'avec les opérateurs privés agréés, permettent des actions ciblées, centrées sur des prérogatives juridiques spécifiques. C'est une stratégie qui repose sur l'expertise de personnels spécialisés, susceptibles d'inscrire un facteur humain dans des processus de masse compatibles avec les exigences de la sécurité des transactions économiques qui est la base du commerce.

SOMMAIRE

NUMÉRO 257

DOSSIER

Sûretés aérienne et maritime

Communauté européenne - Vella

UNE COORDINATION EUROPEENNE A LA MESURE DES MENACES MARITIMES

Le caractère transnational des dangers et des menaces maritimes, le nombre et l'hétérogénéité des autorités ainsi que la disparité des politiques sectorielles menées au niveau national imposent d'instaurer une coordination européenne. Il s'agit essentiellement d'optimiser les ressources existantes, d'imposer des synergies et de briser des cloisonnements administratifs. L'intégration des politiques de surveillance et de sûreté maritimes de l'Union s'est déployée depuis 2007 autour de trois actions: le développement d'un environnement commun de partage d'information maritime (CISE) qui facilitera les échanges entre systèmes informatiques des différentes autorités nationales, civiles et militaires, l'adoption et la mise en œuvre de la stratégie européenne de sûreté maritime et la création d'un corps européen garde-frontières et garde-côtes. Dans ce cadre, le 14 septembre 2016, le Conseil a approuvé de manière définitive la création de cette unité internationale. Ce corps est composé des autorités nationales responsables des missions garde-côtes et des trois agences européennes compétentes: agence européenne de sécurité maritime, agence européenne de contrôle des pêches et agence européenne garde-frontières et garde-côtes (remplaçante de FRONTEX).

Les développements de la politique européenne de surveillance maritime

par **KARMENU VELLA**

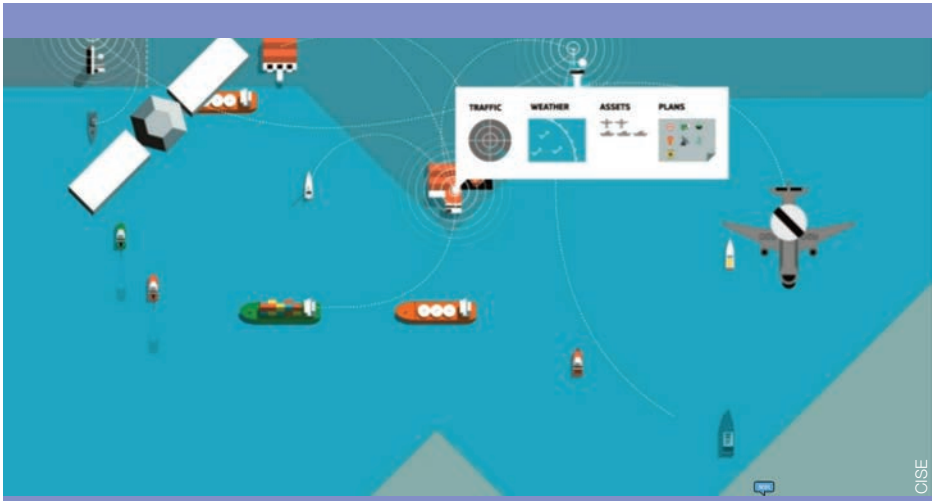
La surveillance maritime constitue une dimension incontournable de la politique maritime intégrée de l'Union européenne lancée en 2007[1]. La sécurité et la sûreté des espaces marins sont non seulement une précondition de toute politique maritime viable – qu'elle concerne le transport, la pêche, la protection de l'environnement, les énergies marines et les activités d'extraction - mais plus largement de la stabilité et de la prospérité de l'Union européenne.

KARMENU VELLA
Commissaire pour l'environnement, les affaires maritimes et la pêche
Commission européenne

Quelques chiffres suffisent pour illustrer à quel point nous dépendons d'espaces maritimes protégés et sûrs : L'économie maritime de l'UE génère 500 milliards d'euros de valeur ajoutée chaque année, 70 % des frontières de l'UE sont maritimes, 30 % de la flotte de commerce mondiale est contrôlée par des intérêts européens et 90 % du commerce extérieur mondial est acheminé par mer.

(1) Communication de la Commission au Parlement européen, au Conseil, Comité économique et social européen et au Comité des régions - Une politique maritime intégrée pour l'Union européenne COM(2007) 574 final

Si les États membres sont compétents pour mettre en œuvre les actions surveillance, le caractère transnational des dangers et des menaces maritimes appelle une coordination à l'échelle européenne. Elle est également rendue nécessaire par le nombre des autorités nationales et des politiques sectorielles impliquées dans la surveillance maritime: contrôle de la pêche, sécurité et sûreté de la navigation, protection de l'environnement et lutte contre les pollutions, maintien de l'ordre public et lutte contre les trafics, surveillance des



Les programmes permettent un partage d'information à partir de sources d'informations différentes (spationav, satelittes, avions, etc.).

frontières, douane, sans oublier les missions de défense. Dans l'Union, plus de 300 autorités nationales civiles et militaires interviennent quotidiennement dans ces différents domaines. Au regard de ces enjeux, la politique de sûreté et de surveillance maritime de l'Union a fortement progressé depuis 2007. Ce développement répond au fond à un impératif simple, de bon sens, qui vise à tirer le meilleur parti des moyens disponibles dans un contexte de menaces croissantes. Cet objectif est déjà pris en compte au plan national par nombre d'États membres qui disposent d'organisations visant à optimiser les synergies et surmonter les cloisonnements administratifs. La France dispose ainsi de longue date d'une organisation spécifique pour les missions relevant de l'Action de l'État en mer (AEM).

L'intégration des politiques de surveillance et de sûreté maritime de l'Union s'est déployée depuis 2007 autour de trois actions: le développement d'un environnement commun de partage d'information maritime (CISE), l'adoption et la mise en œuvre de la stratégie européenne de sûreté maritime et la création d'un corps européen garde-frontières et garde-côtes.

La mise en place d'un environnement commun pour le partage d'informations maritimes (CISE)

L'accès à l'information conditionne en grande partie l'efficacité des autorités nationales dans leurs missions de surveillance maritime. Prenant acte du compartimentage en "silos" des systèmes d'information au niveau national et européen, la Commission européenne et les États membres ont lancé en 2009 un

programme pour mettre en place un environnement commun de partage d'information (CISE)[2]. Ce cadre d'interopérabilité vise à faciliter les échanges entre systèmes informatiques des différentes autorités nationales, civiles et militaires. L'objectif poursuivi n'est pas d'aboutir à un partage illimité de l'information, ni de créer une base de données centralisée. Il s'agit de mettre à disposition des autorités intéressées une solution informatique décentralisée et sécurisée permettant l'échange de données d'un système national vers un autre système national, pour répondre à des nécessités opérationnelles précises.

(2) http://ec.europa.eu/maritimeaffairs/policy/integrated_maritime_surveillance_fr

Le développement de CISE a fait l'objet de trois projets de préfiguration menés entre 2009 et 2013 (BlueMassMed, Marsuno et CooperationProject) avec dans chaque cas une participation significative des autorités françaises. CISE est entré depuis 2014 en phase de déploiement pré-opérationnel. Un réseau test est développé par un consortium réunissant 50 autorités maritimes et institut de recherches issus de 12 États membres, dont la France. Ce projet bénéficie d'un financement européen dans le cadre du programme FP7 et d'un appui technique de la Commission européenne (Centre commun de recherche). Il aboutira en 2017 à la mise en place d'un premier réseau opérationnel d'échange d'information connectant les autorités nationales de 12 États membres, civiles et militaires. Ce réseau est ouvert à la participation de toute autorité publique et a vocation à être étendu.

La stratégie européenne de sûreté maritime

L'adoption de la stratégie européenne de sûreté maritime et de son plan d'action par le Conseil de l'Union, en 2014, constitue une avancée majeure vers une approche globale de l'action de l'Union et des États membres. Cette stratégie vise à assurer le plus haut niveau de protection des intérêts maritimes des États membres et de l'Union, en garantissant en particulier la liberté de navigation et la sûreté des espaces maritimes à l'échelle mondiale.

La stratégie consacre la nécessité de combiner et coordonner toutes les composantes de l'action des États membres et de l'Union qui intéressent la sûreté maritime, dans le domaine civil comme militaire :

– les politiques sectorielles internes des États membres et de l'Union dans les secteurs suivants: lutte contre la pêche illicite, non déclarée et non réglementée, sécurité et sûreté de la navigation, protection de l'environnement et lutte contre les pollutions, maintien de l'ordre public et lutte contre les trafics illicites, surveillance des frontières, missions

douanières, politique de recherche et d'innovation,

– la politique de l'Union européenne en matière de coopération et d'aide au développement en faveur des pays tiers,

– la politique étrangère et de sécurité commune,

– les politiques étrangères et de défense des États membres.

La stratégie est déclinée par un plan de 130 actions réparties en 5 domaines prioritaires d'action :

– la politique extérieure,

– l'échange d'information, comprenant notamment le programme CISE mentionné précédemment,

– le développement et la coordination des capacités,

– la protection des infrastructures critiques et la gestion de crise,

– la formation, la recherche et l'innovation.

La stratégie ne modifie pas la répartition des compétences entre les États membres et l'Union, pas plus qu'elle ne crée de dispositif décisionnel, organisationnel ou budgétaire nouveau. La mise en œuvre de la stratégie s'effectue à cadre constant en visant la meilleure mobilisation des outils existants. Elle constitue ainsi une responsabilité conjointe des États membres et des organes de l'Union: Conseil, Commission, Haut représentant pour la politique étrangère et les affaires de sécurité en particulier.

Un premier rapport de mise en œuvre a été présenté au Conseil par la Commission en juin 2016. Ce rapport est notamment établi sur la base des contributions fournies par les États membres. Compte tenu du nombre d'actions identifiées (130), la nécessité de définir des priorités est aujourd'hui reconnue comme un enjeu important pour déployer la stratégie de manière ciblée et efficace.

La création d'un corps Européen garde-frontières et garde-côtes

Dans son discours sur l'État de l'Union de septembre 2015 consacré principalement à la crise des migrants, le président de la Commission européenne Jean-Claude Juncker a annoncé que la Commission proposerait avant la fin de l'année « *des mesures ambitieuses en vue de mettre en place un corps européen de garde-frontières et de garde-côtes* ».

Le 14 septembre 2016, le Conseil a approuvé de manière définitive la création du corps européen de garde-frontières et de garde-côtes[3]. Ce corps est composé des autorités nationales responsables des missions garde-côtes[4] et des trois agences européennes compétentes: agence européenne de sécurité maritime, agence européenne de contrôle des pêches et agence européenne garde-

Le corps européen de garde-frontières et de garde-côtes sans empiéter sur les prérogatives nationales permettra une coordination des moyens pour la mise en oeuvre d'une stratégie européenne.

frontières et garde-côtes (remplaçant FRONTEX).

Le corps européen garde-frontières et garde-côtes prévoit notamment un renforcement de la coopération entre les agences européennes afin de mieux soutenir les autorités des États membres dans l'exercice de leurs missions. Les domaines de coopération sont les suivants:

– partage et analyse de l'information collectée dans les différents systèmes européens utilisés pour le suivi du trafic maritime (SafeSeaNet), la surveillance des frontières (EUROSUR) et le contrôle des pêches,

– mise à disposition de moyens de surveillance de pointe (drones, senseurs innovants),

– offre de formation et de programmes d'échanges de personnels,

– soutien aux États membres pour la coordination d'opérations de surveillance,

Perspectives

Amorcée en 2007, la politique de l'Union pour promouvoir une surveillance maritime intégrée a fortement progressé depuis. Elle vise à apporter une plus-value collective à un défi que rencontrent tous les États membres : faire face des risques et menaces multiples, interconnectés et souvent transnationaux avec des ressources limitées.

Cette approche intégrée de la surveillance maritime ne vise pas à faire table rase des politiques sectorielles existantes ni à modifier la répartition des compétences entre l'Union européenne et les États membres. Au contraire, elle s'appuie sur les politiques, les autorités et les procédures de décision en place au niveau national et européen avec pour objectif d'en tirer le meilleur parti. La dimension humaine, c'est-à-dire la capacité à surmonter les barrières administratives, culturelles et psychologiques constitue très probablement la clé du succès de cette approche globale de la surveillance maritime.

DOSSIER

Sûretés aérienne et maritime

L'analyse de sûreté du transport maritime

par CHRISTOPHE BÉGARD

Plus de 90 % du volume international des échanges commerciaux emprunte la voie maritime. Cette mondialisation s'est en grande partie confondue avec la maritimisation du monde[1] particulièrement vulnérable aux menaces et activités illicites. La gendarmerie maritime notamment par son dispositif de sûreté maritime et portuaire participe à l'action de l'État en mer. Outre le contrôle et la protection des acteurs principaux de l'économie bleue : les ports français et les navires en escales dans nos ports, elle a développé un outil, l'analyse de sûreté qui lui permet de détecter, de cibler les navires d'intérêt et ainsi d'orienter l'action de ses unités.

CHRISTOPHE BÉGARD
Chef d'escadron
Chef du bureau de la coordination des opérations, du renseignement et de la police judiciaire
Commandement de la gendarmerie maritime.

Une économie bleue particulièrement vulnérable aux menaces et activités illicites

(1) Cf. rapport d'information du Sénat n° 674 du 17 juillet 2012 - Maritimisation : la France face à la nouvelle géopolitique des océans.

Les échanges mondiaux favorisent l'expansion des activités illicites ou terroristes. Les espaces maritimes, leur immensité et le développement des activités offrent d'infinies opportunités de dissimulation. L'Office des Nations unies contre la drogue et le crime (ONUDC) estime que les commerces illicites représentent 7 % des exportations mondiales de marchandises. Ces dernières s'effectuant, pour l'essentiel, par voie maritime, on mesure ainsi l'importance de la corruption des flux.

Les échanges sont particulièrement dépendants de la sécurité des routes maritimes et des passages stratégiques. La sûreté du transport maritime a été affectée par la résurgence de la piraterie et du brigandage maritime, depuis le

début des années 1990, en particulier en Asie du Sud-Est, dans le golfe d'Aden et dans le golfe de Guinée. Le terrorisme maritime prend une nouvelle acuité du fait du développement de la menace djihadiste, de celle qui pèse sur le transport de passagers et d'une porosité plus grande avec d'autres pratiques illicites (piraterie, trafics d'armes, de stupéfiants ou de migrants, cyberattaques…). L'une des principales causes de développement des activités illégales réside dans la faiblesse de certains États et dans leur incapacité à contrôler leurs territoires terrestres et maritimes. La France possède le deuxième plus grand domaine maritime (ZEE) avec 11 millions de km² et 18 500 km de côtes. Le territoire national peut être ciblé depuis la mer. Les ports et leurs installations portuaires sont des interfaces mer-terre par excellence. La neutralisation de ces véritables points nodaux irriguant la France et l'Europe aurait des conséquences économiques significatives. C'est le cas des ports couvrant l'essentiel de nos importations en produits pétroliers ou de nos échanges commerciaux, en vrac ou conteneurisés. De plus, des installations à haut risque, comme les terminaux gaziers ou chimiquiers, sont des cibles potentielles au même titre que ceux recevant les navires de croisière ou les navires-rouliers à passagers. Plusieurs infrastructures critiques[2] sont également implantées le long du littoral métropolitain et ultramarin. La protection de tous ces sites incombe au préfet maritime et au préfet de département dans leurs zones de compétences.

(2) Bases navales, centrales nucléaires, sites SEVESO, centre spatial de Kourou, aéroports internationaux (Nice, Marseille, Ajaccio, Tahiti, La Réunion,

Une analyse de sûreté, pierre angulaire du dispositif de sûreté de la gendarmerie maritime

Dans la stratégie nationale de sûreté des espaces maritimes[3], le premier ministre rappelle que « *La France, forte de l'étendue de ses espaces maritimes métropolitain et ultramarin, doit faire face à des enjeux croissants pour y exercer sa souveraineté et en assurer la surveillance, contrôler les activités qui s'y déroulent et les protéger durablement au service de l'économie bleue.*

Dans un contexte géostratégique tendu, la sûreté de nos espaces et, plus largement la sûreté de la haute mer, constitue un défi majeur face à de nombreuses menaces et activités illicites : piraterie, terrorisme, attaques informatiques, trafics de tous ordres, pêche illégale, pollution… ».

(3) Déclinaison française de la stratégie de sûreté maritime de l'Union européenne.Martinique, Mayotte, Saint-Pierre-et-Miquelon…).

Les mesures du plan VIGIPIRATE et du code ISPS participent à la prévention. La protection des navires commence dans les ports, notamment lors des avitaillements et de l'embarquement des passagers ou des marchandises. Les Pelotons de sûreté maritime et portuaire (PMSP) y contribuent et leur déploiement dans les Ports de commerce d'intérêt majeur (PCIM) et les grands ports

militaires constituent le pivot de la réponse opérationnelle dans le cadre du continuum sécurité mer-terre et défense-sécurité intérieure[4].

(4) Grands ports d'intérêt majeur : Le Havre (2006), Port-de-Bouc (2009), Marseille (2010), Dunkerque (2017), Calais et Nantes-Saint-Nazaire (2018) ; Grands ports militaires : Cherbourg, Brest et Toulon.

Le contrôle au départ, en route ou à destination est privilégié selon le type de vecteur. Il repose principalement sur le ciblage ou le renseignement compte tenu du développement de nouveaux outils de détection et de suivi des activités maritimes, de l'amélioration du partage et de l'analyse du renseignement maritime. Le dispositif de sûreté maritime et portuaire développé depuis 10 ans par la gendarmerie maritime repose sur la priorité « ciblage/renseignement » au travers d'une analyse de sûreté en corrélation avec des capacités de sécurisation, de contrôle et d'intervention sur les navires en escale.

Chaque année, des dizaines de milliers de navires de commerce font escale dans les ports de commerce français (métropole et outre-mer). L'action de la gendarmerie maritime nécessite soit de protéger le navire pendant son escale (escorte de navire, patrouilles de surveillance…) soit de se préserver d'une unité qui peut servir de vecteur d'introduction sur le territoire national d'objets illicites, de personnes malintentionnées ou en situation irrégulière (surveillance discrète, contrôle de navire...).

Le contrôle de tous les navires n'étant pas réalisable et réaliste, la gendarmerie maritime effectue une analyse de sûreté (dite ciblage) de tous les navires en escale. Ce processus, qui s'apparente à un profilage de navires de commerce présentant un intérêt en matière de sûreté, repose sur une organisation dédiée.

Les informations nécessaires à l'analyse de sûreté

Les états contractants à la Convention SOLAS[5] peuvent exiger d'un navire ayant l'intention d'entrer dans un de leurs ports la fourniture de renseignements permettant de s'assurer que ce navire satisfait aux mesures spéciales pour renforcer la sûreté maritime (chapitre XI-2, règle 9). Le règlement européen 725/2004 dispose que les états membres de l'Union européenne ont obligation d'exiger des navires soumis au code ISPS la fourniture des renseignements de sûreté et d'analyser, dans la mesure nécessaire, les renseignements fournis. Ainsi, tout navire doit notifier son arrivée au moins 24 heures à l'avance ou, au plus tard, au départ du port précédent si la

(5) Safety Of Life At Sea

TERMINOLOGIE

La sûreté maritime englobe la prévention et la lutte contre tous actes illicites à l'encontre du navire, de son équipage et de ses passagers ou à l'encontre des installations portuaires. Quant à la sécurité maritime, elle désigne la prévention des risques accidentels ou naturels et la lutte contre les sinistres, quelle que soit leur origine, à bord des navires ou dans les ports.

durée du voyage est inférieure à ce délai (DE2002/59). Ce préavis d'escale entraîne de facto la constitution de l'escale dans le système portuaire. Le dossier d'escale est composé des formulaires suivants :

- FAL1 (Déclaration générale),
- FAL5 (Liste de l'équipage),
- FAL6 (Liste des passagers),
- FAL7 (Manifeste de marchandises dangereuses)
- Déclaration des déchets d'exploitation et des résidus de cargaison des navires (Waste)
- Déclaration de sûreté (ISPS)
- Déclaration maritime de santé (DMS).

En vue de simplifier la transmission des formalités déclaratives à l'entrée et à la sortie des ports des États membres, la directive européenne 2010/65 prescrit la dématérialisation de la transmission des données liées aux escales. Elle impose aux États membres la mise en place d'un guichet unique pour la transmission des formalités dans un format structuré (formulaires FAL de l'OMI) exploitable pour un traitement informatique. Le guichet unique portuaire (GUP) français, en cours de développement par le secrétariat d'État aux transports[6], devrait être opérationnel dans les prochains mois et sera un facilitateur pour le travail de ciblage et de criblage des administrations concernées (gendarmerie maritime, douane, police aux frontières).

(6) La France accuse un retard au regard d'une application initialement prévue au 1er juin 2015

LE CONSIGNATAIRE DE TRANSPORT ET L'AGENT MARITIME

Le consignataire est le mandataire salarié de l'armateur. Il agit au nom et pour le compte de son mandant, l'armateur, pour les besoins du navire et de ce qu'il transporte. Il effectue toutes les opérations que l'armateur exécuterait lui-même s'il était sur place ou auxquelles le capitaine pourrait procéder. Au départ, il réceptionne la marchandise et émet les connaissements ; à l'arrivée, il la livre au destinataire. Il pourvoit aux besoins normaux du navire et de l'expédition, prépare l'escale, assiste le navire pendant l'escale, gère tous les problèmes consécutifs à l'escale. Il assure la gestion des supports ou unités de transport multimodaux de la marchandise (conteneurs, remorques routières, remorques esclaves…) pour le compte de son armateur. Il reçoit tous actes judiciaires ou extra judiciaires destinés à l'armateur que le capitaine est habilité à recevoir et il accomplit toute autre mission confiée par l'armateur.
Le consignataire peut être également agent maritime. Pour cette fonction, il est notamment chargé de la négociation et la conclusion des contrats, de la gestion des finances, de la recherche de fret, de la mise en place d'une politique commerciale, de contacts avec la clientèle, de relations avec les autorités en charge des problèmes maritimes et ce, dans la zone qui le concerne. L'étendue de son pouvoir de représentation est déterminée par le contrat de mandat signé par l'armateur (agents portuaires, agents généraux, etc.).

Le processus d'analyse de sûreté

Ce dossier d'escale constitue la donnée de base de l'analyse réalisée par la gendarmerie maritime. À partir de ces données, l'analyste (le cibleur) suit un processus qui va lui permettre d'évaluer tous les navires en escale en fonction de critères définis par la gendarmerie maritime à partir des menaces qui pèsent sur le transport maritime :

	Analyse de sûreté de tous les navires en escale
CORGMAR CHERBOURG	Façade maritime Manche Mer du Nord
CORGMAR BREST	Façade maritime Atlantique
CORGMAR TOULON	Façade maritime Méditerranée
CRENSGMAR HOUILLES	Tous les ports en collaboration avec les CORGMAR et les PSMP + outre-mer

- le type de navire (porte-conteneurs, pétrolier, chimiquier, RO/RO, vraquier, navire à passagers…),

- la fonction du navire (long courrier, feedering, tramping…),

- le pavillon et l'armateur du navire,

- les ports de provenance et de destination du navire,

- l'interface du navire lors de son escale (port, zone de mouillage, installation portuaire),

- l'historique du navire (propriétaire, déficiences…),

- la fiabilité des documents transmis par le navire (validité, authenticité des documents)…

L'analyste crible le navire, l'équipage et les passagers dans les bases de données nationales, européennes ou internationales. Si nécessaire, une vérification des documents de la cargaison (connaissement[7], manifeste[8]) peut être effectuée.

Ainsi, sur la base des renseignements recueillis et des investigations effectuées, l'analyste peut identifier un navire, une ligne, un équipage, une cargaison… susceptible de nuire à la sûreté et informer en temps réel les autorités hiérarchiques (préfet terrestre et maritime) voire d'autres administrations (douane, centre de sécurité des navires, police aux frontières…).

(7) Contrat par lequel une compagnie de transports maritimes atteste qu'elle a reçu des marchandises à bord d'un bateau (avec en particulier mention de leur nature, nombre, poids, marque, le nom du transporteur et du destinataire, les lieux d'embarquement et de destination, le prix du transport) et par lequel elle s'engage à les remettre à leur destination, dans l'état où elle les a reçues, sous réserve de périls ou d'accidents en mer.

(8) Le manifeste est un document de transport qui récapitule la totalité des marchandises ou des passagers chargés dans une unité de transport pour un trajet donné. C'est un document de bord qui accompagne le vecteur tout au long du voyage, pour les différents contrôles administratifs ou douaniers.

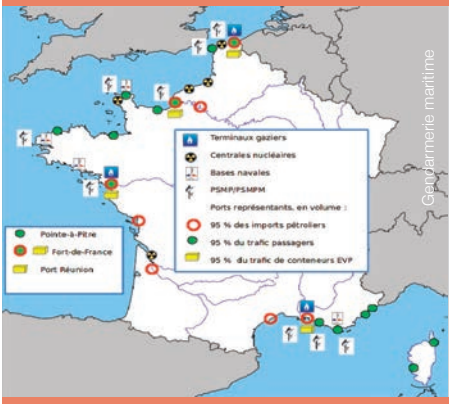
Les acteurs de l'analyse de sûreté

Initialement limitée aux ports de commerce d'implantation des pelotons de sûreté maritime et portuaire (civil et militaire)[9], l'analyse de sûreté est dorénavant réalisée par les gendarmes maritimes des Centres d'opérations et de renseignement de la gendarmerie maritime (CORGMAR)[10] et le Centre de renseignement de la gendarmerie maritime (CRENSGMAR).

La Cellule d'analyse de sûreté et d'évaluation des menaces (CEMAS) des CORGMAR assure le ciblage des navires de chaque façade maritime. Le centre de renseignement de la gendarmerie maritime analyse les navires en escale

(9) Le Havre, Marseille, Cherbourg, Brest et Toulon.

(10) Après une expérimentation menée en Méditerranée, les GEROM (groupe d'exploitation du renseignement opérationnel maritime) des groupements de gendarmerie maritime ont été transformés en CORGMAR (centre d'opérations et de renseignement de la gendarmerie maritime) le 1er avril 2016.



Carte des principales installations et activités littorales à protéger et positionnement des PSMP.

dans les ports d'outre-mer et anime au niveau national cette fonction pour le commandant de la gendarmerie maritime. Le centre de renseignement et les CEMAS travaillent en collaboration et échangent leurs informations avec les autres services de renseignement, de police, de la douane et de la défense….

Les outils utiles à l'analyse de sûreté

Pour réaliser cette mission, les analystes des CEMAS et du centre de renseignement disposent de nombreux outils :

- les logiciels portuaires de gestion des escales, à terme le guichet unique portuaire (GUP) ;
- le système SPATIONAV V2, système de surveillance en temps réel des approches maritimes ;
- IMDate, système intégré de surveillance maritime de l'agence européenne de sécurité maritime (EMSA),
- LLOYD's, base de données des navires de la société de classification maritime britannique,
- EQUASIS, base de données regroupant des informations concernant la sécurité des navires,
- AIS marine trafic, vessel finder[11]…
- Bases de données judiciaires, administratives et documentaires nationales, européennes et internationales.

L'analyse de sûreté, outil d'orientation de l'action de la gendarmerie maritime

(11) Logiciel gratuit de suivi des navires par leurs coordonnées AIS

(12) Peloton de Sûreté Maritime et Portuaire

Cette analyse de sûreté permet aux échelons de commandement d'orienter l'action des unités de gendarmerie maritime. Pour chaque navire d'intérêt et selon la menace (terrorisme, trafic illicite, clandestins…), un dossier d'analyse de sûreté identifie les actions de sécurisation et de contrôle à mener par les unités : surveillance discrète, contrôle élémentaire, contrôle approfondi, visite de coque, emploi des équipes cynophiles, de référents fraude documentaire mais aussi dispositif d'escorte de navire, d'équipe de protection des navires à passagers… Le CORG constitue également le centre opérationnel permettant de déclencher les capacités d'intervention de la gendarmerie maritime.

Des capacités de sécurisation

L'action des PSMP[12], unique en Europe,

est reconnue aujourd'hui par le monde maritime et les autorités d'emploi, compte tenu de leur expertise (technicités détenues, formation et entraînement des militaires) et du spectre des missions militaires et civiles réalisées : équipes cynophiles explosifs, armes et munitions, équipes subaquatiques, capacités Reconedex et de fouille des navires. Ces unités disposent de moyens spécifiques et adaptés afin de réaliser leur contrat opérationnel. Trois nouvelles unités seront créées en 2017 et 2018 pour renforcer la sûreté des ports de Dunkerque, Calais et Nantes-Saint-Nazaire.

Les PSMP participent, seuls ou avec d'autres services de l'État (douane, police aux frontières, centre de sécurité des navires…), à la sécurisation des ports par des patrouilles maritimes et terrestres, des navires à passagers à l'embarquement et au débarquement, au blanchiment de quai lors d'escale de navires sensibles, à la sensibilisation des acteurs du transport maritime à la menace terroriste et à la radicalisation. Depuis le 1er août, dans le cadre du renforcement de la sûreté du transport à passagers, les PSMP participent, avec le concours de la marine, à la sécurisation en mer des navires à passagers par l'embarquement d'équipes de protection des navires à passagers (EPNAP) des compagnies françaises ayant passé une convention avec l'État français (représenté par la marine nationale). La sélection des navires à passagers qui embarquent une EPNAP est décidée par le préfet maritime sur proposition du groupement de gendarmerie maritime (CORGMAR/CEMAS).

Des capacités de contrôle

Si les contrôles élémentaires peuvent être réalisés par toutes les unités de gendarmerie maritime, les contrôles approfondis dits fouilles de sûreté, ne sont réalisés que par les PSMP qui sont formés et équipés. Chaque contrôle est précédé de l'envoi par le CORGMAR (CEMAS) d'un dossier d'analyse de sûreté. À l'issue du contrôle, les renseignements obtenus sont centralisés au niveau des CORGMAR et partagés avec les services de renseignement mais aussi les autres services de l'État chargés des contrôles des navires voire des partenaires étrangers dans le cadre d'une coopération policière internationale et européenne. Ainsi, dans le cadre du réseau Aquapol (coopération policière européenne liée au milieu maritime et fluviale), les priorités d'action des pays participants visent le renforcement de la

CODE ISPS

« International Ship and Port facility Security » - Code de sûreté des navires et des installations portuaires annexé à la Convention pour la sauvegarde de la vie humaine en mer (SOLAS) renforcé par le règlement (CE) n ° 725/2004 et, pour les ports, la directive 2005/65 (CE). Décidée par le Premier ministre, la mise en oeuvre des mesures repose sur les opérateurs privés, l'État (en qualité d'autorité de sûreté maritime et portuaire et de point de contact pour l'OMI), ses représentants locaux et les administrations compétentes. Ces mesures visent à prévenir les menaces et en limiter les impacts.

sûreté et la lutte contre la radicalisation dans les ports et des marins de commerce.

Des capacités d'intervention

Les PSMP, compte tenu de leur implantation, sont des éléments d'intervention de proximité capables de s'engager et de se projeter dans un court délai pour répondre à un incident de sûreté dans un port ou sur un navire. Pour faire face à l'évolution des modes d'action des terroristes, notamment à une tuerie de masse sur un navire à passagers dans un port ou à proximité immédiate de la côte, la gendarmerie maritime a développé le concept de PSMP Espadon, se rapprochant du concept des PSIG Sabre[13] de la gendarmerie nationale. Les PSMP agissent par une action des primo-engagés ou de primo-intervenants, sur ordre du commandant de groupement (CORGMAR), en subsidiarité et dans l'attente de l'arrivée d'unités spécialisées en contre-terrorisme maritime (GIGN et commandos marine).

(13) Les PSIG renforcés, dits Sabre, s'intègrent dans le cadre du Plan et de la doctrine spécifique d'intervention développée par la gendarmerie pour faire face à tout type de crise. Ils sont disposés dans les zones les plus exposées aux troubles graves à l'ordre public, en cohérence avec l'implantation des autres unités d'intervention, les brigades territoriales, mais aussi les unités d'intervention spécialisée.

(14) Stratégie de sûreté maritime de l'Union européenne, 11205/14 du 24 juin 2014.

« *L'UE dépend de l'ouverture, de la protection et de la sûreté des mers et des océans pour son développement économique, ses transports, sa sécurité énergétique, ainsi que pour garantir le libre-échange, le tourisme et le bon état écologique de l'environnement marin* »[14]. La gendarmerie maritime contribue au niveau national et européen à renforcer la sûreté du transport maritime grâce à son dispositif maritime et portuaire. L'analyse de sûreté permet aux échelons de commandement d'orienter la réponse opérationnelle face aux menaces qui pèsent ou qui viennent des navires en escale. Des défis sont identifiés et constituent des objectifs à moyen et long terme pour la gendarmerie maritime : les cybermenaces, le big data pour améliorer les capacités d'analyse de sûreté, la coopération entre les services chargés de la sûreté des ports (identification des bonnes pratiques, standards communs de contrôle…).

L'AUTEUR

Christophe BÉGARD, chef d'escadron, occupe les fonctions de chef du bureau de la coordination des opérations, du renseignement et de la police judiciaire au commandement de la gendarmerie maritime. Il est également le référent sûreté maritime et portuaire de la gendarmerie maritime. Antérieurement, il a été adjoint au chef de la section Schengen Élargissement de l'Union européenne et programmes européens de 2002 à 2006 à la DGGN, puis il a commandé et conduit l'expérimentation du 1er peloton de sûreté maritime et portuaire, au Havre de 2006 à 2008. De 2008 à 2013, il prend le commandement et crée la compagnie de gendarmerie maritime de Marseille avec pour mission principale de créer les PSMP du port de Marseille (Port-de-Bouc en 2009 et Marseille-Joliette en 2010). Au niveau européen, il préside depuis 2016, le groupe régional Atlantique et mer du Nord du réseau Aquapol (réseau des polices et gendarmeries maritimes européennes).

La mer, eldorado des cybercriminels ?

par **FLORIAN MANET**

En 2011, un rapport de l'ENISA[1] dénonçait le déficit de prise en compte de la cybersécurité par les gens de mer en affirmant que « *la sensibilité à la problématique (de cybersécurité) varie de faible à inexistant* ». Depuis, une prise de conscience réelle des dangers de la marétique[2] répond davantage aux enjeux d'une activité en plein développement au sein d'une économie globalisée.

Un espace de liberté vulnérable

La technologie assure, en effet, une navigation en dépit des éléments naturels et prévient aussi les risques de collision ou de talonnage dans des routes maritimes surchargées. Humble par nature, le marin sait aussi la malveillance dont il peut être la victime à la mer. Certes, le pirate des mers demeure une réalité contemporaine mais il ne doit pas pour autant évacuer le cyberpirate qui constitue - à n'en pas douter - la menace prégnante aujourd'hui. La démocratisation de la cyber-malveillance introduit une stratégie du faible au fort renversée : des cyberpirates, investissant quelques centaines d'euros, sont en mesure de causer des préjudices s'élevant à plusieurs dizaines de millions d'euros et de provoquer une désorganisation des flux commerciaux internationaux dans le contexte de la mondialisation économique.

La faible perception de la cyber-menace apparaît paradoxale au vu de l'interconnexion internationale qui

FLORIAN MANET

Lieutenant-colonel de gendarmerie, commandant la section de recherches de la gendarmerie maritime.

(1) L'ENISA ou European Union Agency for Network and Information Security. Voir https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1

(2) La marétique, contraction entre maritime et numérique, désigne l'ensemble des systèmes d'information et de traitement de données relatifs aux activités maritimes et portuaires.

caractérise l'écosystème maritime étendu de la sphère portuaire et de l'omniprésence de la technologie au sein de l'univers professionnel dans lequel évolue un marin. L'univers technologique maritime s'est, notamment, construit au fil du temps, en se fondant sur la croyance en une absolue sécurité apportée par la technologie sans fil[3], conçue pour œuvrer dans un circuit fermé, et sur la multiplication des SCADA[4] qui a réduit corrélativement les équipages à bord des navires[5]. Ainsi, des systèmes d'information interopérables et interconnectés au sein du bord, comme avec d'autres navires en mer ou encore avec les installations portuaires ont envahi les passerelles comme les salles des machines. De plus, la complexité croissante des multiples systèmes d'information a rendu l'équipage dépendant de techniciens intervenant à distance depuis la terre, accroissant de fait les vulnérabilités. À titre d'illustration, en matière de navigation maritime, apparaissent actuellement des bouées de balisage de nature virtuelle qui exploitent la technologie AIS. Elles produisent alors un écho virtuel similaire à celui d'un AIS sur les écrans ECDIS[6] des passerelles, permettant, par exemple, de baliser un haut-fond. Économiquement très intéressantes, elles demandent des frais réduits de maintenance sauf s'ils résultent d'une opération malveillante.

(3) En passerelle se trouvent de multiples systèmes qui s'appuient sur la technologie VHF tel que l'Automatic Identification System (ou AIS) ou, en milieu portuaire, les technologies Portable Pilot Unit ou PPU. Il s'agit de systèmes de positionnement de type local.

(4) Le SCADA (Supervisory Control and Data Acquisition) est un système de télégestion à grande échelle permettant de traiter en temps réel un grand nombre de télémesures et de contrôler à distance des installations techniques. Les systèmes SCADA ne sont pas spécifiques au domaine maritime et équipent de nombreuses infrastructures critiques.

(5) Le porte conteneurs CMA CGM Bougainville dispose de 27 membres d'équipage pour 400 mètres de longueur et près de 17 000 boites.

(6) ECDIS ou Electronic Charts Display Information System est un système de visualisation des cartes électroniques et d'information qui permet de visualiser la position d'un mobile sur la représentation d'une carte à l'écran. Son usage peut permettre de se passer de la carte papier.

LES CHIFFRES CLÉS DE LA MARITIMISATION

90 % du commerce extérieur européen emprunte les mers
90 % de la population mondiale vit à moins de 100 kilomètres des côtes
90 % des fonds marins ne sont pas exploités
27 % de la production mondiale d'hydrocarbure est issue d'un gisement off-shore
150 millions de dollars : le prix du porte conteneur CMA CGM BOUGAINVILLE d'une capacité de 17 700 EVP[8]
350 kilomètres, c'est l'équivalent ferroviaire du fret transporté par un porte conteneurs
40 jours de navigation relient les ports de Chine au Havre

Des enjeux fondamentaux pour l'humanité

Les cyber-menaces maritimes prennent place dans un contexte de maritimisation d'une économie mondialisée et globalisée. Plus que jamais, la puissance économique passe par la mer qui

s'impose par des avantages concurrentiels indiscutables (coût du transport, bilan carbone, intermodalité,..). Mieux encore, la terre accroît sa dépendance au potentiel extraordinaire des richesses que la mer renferme (réserve alimentaire, énergétique..). De fait, les flux commerciaux internationaux empruntent de véritables autoroutes de la mer qui relient des hubs logistiques interconnectés et intermodaux, favorisés, en cela, par une incessante course au gigantisme en matière de construction navale. Au-delà des seuls aspects économiques, les cyber-menaces maritimes exercent une pression environnementale et redessinent des équilibres géopolitiques[7] pourtant établis.

(7) Le spectre d'un cyber blocus maritime n'est pas à écarter.

(8) EVP ou équivalent vingt pieds est une mesure internationale de conteneurs.

Un écosystème complexe générant une grande variété de cibles

Concrètement, les cyber-menaces peuvent se traduire par la perte de contrôle de la propulsion ou de la navigation, ou encore celle d'informations commerciales stratégiques. Exploitant les vulnérabilités présentes dans la chaîne maritime et portuaire, particulièrement interconnectée, des cybercriminels disposent d'une très large variété de cibles : le vecteur maritime lui-même, sa navigation, l'équipage (négligences professionnelles et communications personnelles) et le fret transporté (par exemple les balises de géolocalisations de certains containers sensibles) sans négliger, par ailleurs, l'écosystème maritime (points fixes terrestres – ports par leurs portiques de levage automatisés et connectés, les sémaphores, les phares et balises, - énergie maritime renouvelable, exploitation de la mer...).

De fait, le cyberespace maritime désigne simultanément un théâtre des opérations, qui expose immédiatement et malgré eux, les gens de mer à des groupes criminels bien souvent organisés et internationaux, mais également un vecteur qui permet aux cybercriminels d'exprimer leur revendication ou leur avidité.

Un chiffre noir

La réalité de la cyber délinquance affectant le milieu maritime est d'autant plus difficile à estimer que les victimes peinent à porter plainte par crainte d'un risque d'atteinte à leur image, par un sentiment d'impuissance à obtenir une réparation du préjudice ou simplement par honte. Ce chiffre noir n'aide pas à améliorer la prise en compte de ce risque particulier même si les assureurs maritimes proposent désormais des garanties dans leur contrat.

Les cybercriminels sont de natures très diverses: états étrangers, « hacktivistes », groupes criminels, mouvements terroristes ou concurrents. Mais tous sont

animés d'un même but : obtenir du pouvoir ou de l'argent. L'environnement maritime leur offre une caisse de résonance sans commune mesure.

Une révolution dans le risk assessment maritime

Les cyber-menaces constituent véritablement une révolution dans l'évaluation des risques par les gens de mer. Traditionnellement, les risques encourus au cours d'une navigation résultaient principalement de conditions de mer ou météorologiques défavorables, d'avaries mécaniques et de collisions, volontaires ou non, avec d'autres navires ou enfin, d'actes de piraterie.

Aujourd'hui, le cyber impose une menace terrestre permanente exercée sur la navigation alors même que le navire évolue au milieu des océans, loin des côtes. L'action cyber-malveillante peut être, en effet, déclenchée à distance depuis la terre ou bien encore intégrée dans les systèmes d'information lors d'une escale avant de se concrétiser ensuite à la mer selon les plans criminels. Les escales sont véritablement identifiées comme des points de faiblesses de la *supply chain*[9] de nos économies.

(9) Le supply chain management est la gestion de l'ensemble des maillons (achats, approvisionnement, transport, manutention, etc.) qui constituent la chaîne logistique d'approvisionnement.

L'impact de ces cyber-menaces sur nos sociétés est à la mesure du gigantisme de la construction navale contemporaine. Il n'est guère utile d'insister davantage sur les effets produits par un dérèglement malveillant d'un SCADA à bord d'un porte-conteneurs d'une capacité de 20 000 EVP (conteneurs) ou d'un navire à passagers possédant à son bord près de 8000 personnes et renfermant plusieurs tonnes d'hydrocarbure et d'hydrauliques. À la différence des transports guidés[10] qui permettent de localiser à coup sûr l'événement et ses conséquences concrètes, la navigation maritime offre d'innombrables possibilités, ce qui accroît, par conséquent, la complexité de la gestion de crise de tels agissements criminels.

(10) Les transports guidés rassemblent les modes de transport type ferroviaire. En 2008, un hacker était parvenu à faire dérailler un tramway exploité à Lodz en Pologne. Des virus paralysent régulièrement des rames de train et de métro à travers le monde.

(11) Un livre blanc sur la cybercriminalité maritime est en cours de rédaction au sein de l'organisation maritime internationale.

(12) Loi n° 2013 – 1168 du 18/12/2013 relative à la programmation militaire pour les années 2014-2019 (Article 22 définit des disposition spécifiques à la sécurité des systèmes d'information).

Des initiatives nationales à coordonner

Sous l'égide de l'Organisation maritime internationale, les acteurs du monde maritime se sont emparés du sujet[11]. Ainsi, un livre blanc sur la cyber sécurité synthétisant les travaux de cinq associations d'armateurs a été notamment rédigé en collaboration avec l'association internationale des assureurs maritimes (IUMI).

Une prise de conscience est aussi observée dans de nombreuses nations.

Au-delà d'une réglementation[12] appropriée, une organisation nationale française dédiée est d'ores et déjà mise sur pied. L'amiral Coustillières, officier général cyber, issu de la Marine nationale, a des attributions transverses à tout l'état-major des armées, au sein de « l'EMA Cyber ». Les structures mises en place par le gouvernement s'appuient, en matière maritime, sur l'expertise combinée du CALID[13] et de la gendarmerie maritime. La cybersécurité est alors développée sous un double angle. Tout d'abord, un volet technique se développe au travers notamment de la recherche, à l'image des centres de recherches de l'école navale ou de l'école nationale supérieure maritime comme au sein d'entreprises. Ensuite, une action à destination du management est menée simultanément au sein des organisations maritimes. À ce titre, la marine nationale intègre systématiquement les cyber-menaces dans le contrôle de la

(13) Le CALID ou Centre d'analyse de Lutte Informatique Défensive est placé sous les ordres de l'OG CYBER.

(14) Le COMINFORM rassemble les praticiens et les experts de la cyber sécurité au sein de la marine nationale.

(15) Ces rencontres parlementaires cyber sécurité et milieu maritime ont été organisées pour la première fois le 12 février 2015.

UNE MENACE CYBERNÉTIQUE MARITIME RÉELLE

- des recherches menées dans une université texane ont illustré la vulnérabilité du système de navigation maritime embarquée : le cap d'un navire peut être changé à l'insu du bord en interférant le signal GPS de telle sorte que les instruments de navigation prennent pour référence une position erronée du navire,
- des hackers ont pénétré, en 2011, les systèmes d'information d'un grand port nord européen en charge de la gestion des conteneurs dans le but de soustraire au contrôle douaniers des conteneurs chargés de produits stupéfiants,
- des attaques type déni de service portées sur les systèmes d'information portuaires comme des tentatives d'intrusion via des réseaux sans fil,
- des pirates somaliens ont eu recours, en 2011, aux services de hackers pour obtenir des informations relatives aux navires dans le golfe d'Aden ainsi qu'à leur cargaisons. Cela a donné lieu à au moins un acte avéré de piraterie,
- un hacker a perturbé, en 2014, le réglage de l'assiette d'une plate-forme pétrolière exploitée au large de l'Afrique, entraînant sa fermeture temporaire, une éolienne alimentant en énergie l'île d'Ouessant a été piratée en 2015.
– escroqueries aux achats frauduleux de billets (croisières) par carte bancaire sur Internet. On peut prendre en référence les opérations coordonnées d'Europol pour lutter contre de tels escroqueries dans le domaine des billets d'avion (gendarmerie des transports aériens), qui génèrent des millions d'euros de préjudice...

D'autres exemples dignes d'intérêt :

https://www.blackhat.com/docs/asia-14/materials/Balduzzi/Asia-14-Balduzzi-AIS-Exposed-Understanding-Vulnerabilities-And-Attacks.pdf

https://www.blackhat.com/docs/us-14/materials/us-14-Santamarta-SATCOM-Terminals-Hacking-By-Air-Sea-And-Land-WP.pdf

http://www.blackhatworld.com/seo/bypass-high-internet-rates-on-cruise-ships.555415/

Gendarmerie maritime

La section de recherches de la gendarmerie maritime bénéficie de l'expertise de l'institution dont la maîtrise des technologies numériques est confortée par des partenariats avec les grands opérateurs privés et publics.

capacité opérationnelle de ses bâtiments tout comme elle anime un séminaire annuel[14]. A l'image des rencontres parlementaires[15] annuelles, la mobilisation des gens de mer[16] se traduit par un fort partenariat public-privé fondé sur des échanges de bonnes pratiques et des actions de sensibilisation sous l'égide de l'ANSSI.

(16) À l'image des groupes de travail existant au sein du GICAN (Groupement des Industries de Construction et Activités Navales) et du Cluster maritime français.

(17) Le C3N assure trois missions : Il effectue des investigations judiciaires, anime le renseignement criminel et donne un appui opérationnel aux 2000 enquêteurs spécialisés du réseau décentralisé « Cybergend ». Le C3N offre une capacité unique en France de rapprochement et identification des auteurs/victimes apparaissant sur des contenus pédopornographiques (CNAIP).

Demain, cap sur la cybersécurité maritime?

La sûreté du monde maritime exige une impulsion forte de la part des acteurs régionaux, nationaux et internationaux, de manière à motiver voire à contraindre des parties prenantes souvent timides sur le sujet mais légitimement préoccupées par des objectifs commerciaux au vu des engagements financiers colossaux déjà consentis. Une dynamique internationale contraignante est fondamentale afin de limiter les effets d'une concurrence déloyale au sein d'échanges globalisés. Régi par de multiples conventions internationales, le droit maritime pourrait

produire un texte normatif spécifique ou inclure, par exemple, un volet cyber-sécurité dans la convention SOLAS[18] ?

(18) La convention SOLAS ou Safety of Life At See ou convention internationale sur la sauvegarde de la vie humaine en mer a été adoptée en 1974. Elle définit des normes en matière de sécurité et de sûreté qui s'imposent aux armateurs et qui font l'objet d'inspection par l'état du pavillon.

Dans cet effort collectif, il s'agit aussi de promouvoir une meilleure cohérence entre armateurs, constructeurs navals, fournisseurs de solutions et équipages de manière à concevoir des environnements maritimes cyber-secure. Cette démarche peut naturellement s'enrichir des compétences et expériences développées par la gendarmerie maritime directement confrontée à la cybercriminalité et point de contact avec les structures spécialisées du ministère de l'Intérieur.

Enfin, la démarche de cyber sécurité maritime repose avant toute chose sur les épaules de l'homme d'équipage. Ce dernier représente à la fois le maillon faible, un cheval de Troie viral qui s'ignore ou non, et le maillon fort sur qui repose tous les espoirs de la résilience maritime. Il est celui qui, par son esprit critique et ses compétences, détecte les anomalies observées entre la perception du réel et les données offertes par la machine. Développer des réflexes de « cyberhygiène », cloisonnant, par exemple, le VLAN[19] dit professionnel et celui dédié au « welfare », sécurisant le réseau wifi du bord, définissant rigoureusement les droits d'accès, administrateurs comme utilisateurs. Dans ce contexte, la désignation au sein du bord un officier

(19) VLAN ou virtual local area network.

LA CELLULE D'INVESTIGATIONS NUMÉRIQUES MARITIMES DE LA SECTION DE RECHERCHES DE LA GENDARMERIE MARITIME

Dotée de capacités judiciaires, la gendarmerie maritime constitue la 5ème force de la Marine nationale. Forte de plus de 1000 militaires, elle s'appuie sur un maillage littoral, métropolitain comme ultramarin, qui lui permet d'apporter une réponse adaptée aux enjeux de sûreté maritime et portuaire en complémentarité des autres acteurs de l'action de l'état en mer.
Elle constitue un acteur clé de la lutte contre la cyber-malveillance maritime au travers de la cellule d'investigations numériques maritimes de la section de recherches de la gendarmerie maritime. Ses enquêteurs « nouvelles technologies » (NTECH) animent un réseau de correspondants nouvelles technologies (C-NTECH) présents au sein de toutes les unités des groupements de gendarmerie maritime. Ils possèdent des capacités à la fois légales et techniques comme légales pour conduire des cyber-patrouilles, pour exploiter tous supports numériques, relever des infractions à la loi pénale en matière de cyber. Développant une proximité avec les gens de mer, cette cellule d'investigations judiciaires travaille en lien étroit avec le CALID et le C3N (centre de lutte contre les criminalités numériques)[17]

cyber formé pourrait constituer un premier pas symbolique d'une prise en compte effective par la profession des cyber-risques.

Le chantier d'une cybermarétique secure est immense. Néanmoins, les gens de mer ont déjà connu au cours des siècles d'autres révolutions fondamentales dans leur profession. Tenace et responsable, le marin possède assurément les ressorts nécessaires pour créer de nouveaux modes de fonctionnement afin de garantir une navigation sécurisée.

L'AUTEUR

Florian MANET, Lieutenant-colonel de gendarmerie, commande la section de recherches de la gendarmerie maritime. Fortement impliqué dans la sûreté des transports, il a occupé les fonctions de conseiller gendarmerie du secrétaire général de la SNCF de 2011 à 2015. Ces fonctions particulières ont confronté cet officier à l'ensemble des problématiques sûreté affectant un opérateur d'importance vitale, agissant dans un cadre européen et international.
A ce titre, il a, notamment, animé, au sein du Club des Dirigeants de Sûreté d'Entreprises, un groupe de travail inter-entreprises associant les forces de l'ordre, dédié à la lutte contre les vols de métaux.

Le Cluster maritime français et cybersécurité

entretien avec FRÉDÉRIC MONCANY DE SAINT-AIGNAN

réalisé par FLORIAN MANET, commandant la section de recherches de la gendarmerie maritime

Q

Qu'est ce que le Cluster Maritime Français ?

Le Cluster est une organisation qui rassemble les acteurs du secteur maritime, de l'industrie aux services, des organismes de formation, des associations, des collectivités... ainsi que la marine nationale. Il crée des synergies entre les acteurs maritimes afin que toute l'économie puisse bénéficier des capacités d'innovations et des opportunités de business qu'offrent les activités en mer.

Comment l'activité maritime est-elle affectée par la révolution numérique ?

FRÉDÉRIC MONCANY DE SAINT-AIGNAN

Président du Cluster Maritime Français

La révolution numérique touche tous les secteurs de l'économie, le maritime n'est pas épargné. L'homme qui part en mer s'appuie désormais sur de nouvelles technologies. La liste est longue, le marin d'aujourd'hui est de plus en plus dépendant du numérique. Il doit donc placer sa confiance dans des systèmes qui ne le trahiront pas. Pour cela, la sécurité numérique des outils qu'il utilise est une priorité.

Au-delà du navigant, cela concerne toute une sphère économique connectée : les installations, la gestion des transports maritimes, de la logistique (*supply chain*), les constructions navales, les énergies marines, la surveillance maritime, les complexes *oil&gas*, métiers de « services »…

La sécurité numérique devient un enjeu fort pour une majorité d'entreprises françaises bien que la prise de conscience soit encore récente. Vecteur de la mondialisation, le secteur maritime transporte 90 % des marchandises. Il est donc vital

Sirpa-gendarmerie

Le cluster crée des synergies entre les acteurs maritimes afin que toute l'économie puisse bénéficier des capacités d'innovations et des opportunités de business qu'offrent les activités en mer.

pour notre monde globalisé... Il ne s'agit pas ici de lister les vulnérabilités des opérateurs maritimes, mais de souligner l'urgente nécessité de prendre les mesures adéquates pour protéger et défendre les SI[1], les infrastructures réseaux et les SCADA[2].

(1) Systèmes d'Information

(2) Supervisory Control And Data Acquisition) SCADA est un système de télégestion permettant de traiter en temps réel des télémesures et de contrôler à distance des installations techniques.

Quelles sont vos priorités en matière de cybersécurité maritime ?

Je voudrais en citer trois :

Décider d'une véritable stratégie au plus haut niveau des entreprises et l'appliquer à tous les échelons

Après avoir fixé les règles de sécurité, d'hygiène informatique et défini les objectifs en matière de politique numérique, les décisions qui seront prises devraient faire l'objet d'une sensibilisation élargie à tout le personnel. Le facteur humain est l'une des clefs de cette stratégie de sécurité numérique. Si l'homme est le principal

facteur de risque, il est également celui par qui des solutions d'améliorations sont recherchées.

La mise en place d'une véritable stratégie numérique au sein des entreprises du maritime est une décision de management du plus haut niveau. Aussi, il n'est pas anodin de constater que les CDO[3] ont depuis peu leur place au comité exécutif des entreprises.

(3) Chief Digital Officer : Directeur de la Stratégie Digitale.

(4) Autorité nationale en matière de sécurité et de défense des systèmes d'information.

Dynamiser une gouvernance nationale et internationale

L'ANSSI[4], dans le cadre de sa mission d'autorité nationale en matière de sécurité et de défense des systèmes d'information, apporte naturellement son expertise et son assistance technique aux acteurs maritime, notamment au profit des opérateurs d'importance vitale (OIV) .

Il faut parler de gouvernance à deux autres strates: le niveau européen, au travers de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA[5]), mise en place par la Commission européenne, mais aussi au niveau international où l'Organisation maritime internationale (OMI) a récemment exhorté ses membres à proposer à la prochaine session du Comité de la sécurité maritime (MSC) des recommandations sur la cybersécurité maritime.

(5) Elle a produit un rapport en 2011 intitulé « Cyber Security Aspects in the Maritime Sector ».

Anticiper les changements :

Pour prévoir les cybermenaces, il faut déjà procéder à un état des lieux, un audit des infrastructures, des systèmes d'informations (embarqués ou à terre), des modules de contrôle, bref de tout ce qui compose une architecture informatique au sein d'une entreprise. Lorsqu'il s'agit de construction à échelle industrielle, avec des programmes longs parfois alors que l'informatique évolue sans cesse, ne devrait-on pas penser à travailler en amont, c'est à dire développer des produits qui dès le départ intègrent une sécurité numérique intrinsèque. Pour anticiper les changements et les cyberattaques, la *security by design*, terme désormais retenu, doit être une priorité des concepteurs. Plus encore, lorsque l'on commence à parler de navires autonomes, d'intelligence artificielle…

Alors que le Conseil Interministériel de la Mer du 22 octobre 2015 a approuvé la feuille de route cybersécurité maritime et a mandaté l'ANSSI et la DAM[6] pour la conduire, en associant le Secrétariat général de la mer dans le

(6) Direction des Affaires Maritimes

cadre du suivi des actions de la stratégie nationale de sûreté des espaces maritimes, le Cluster maritime français anime un groupe de travail « cybersécurité maritime » qui rassemble tous les acteurs maritimes concernés.

C'est dès à présent qu'il nous faut réfléchir et travailler de concert entre État, industriels, utilisateurs et organisations professionnelles pour une véritable stratégie maritime française de la sécurité numérique.

L'AUTEUR

Officier de la marine marchande, Frédéric MONCANY de SAINT-AIGNAN préside le Cluster Maritime Français depuis décembre 2014. Il est très fortement investi dans la maritimisation de notre société via des engagements associatifs, des cercles de réflexion comme le « laboratoire de la Blue Society » ou encore au sein de nombreuses instances comme le Conseil Supérieur de la Marine Marchande ou le Conseil Exécutif d'Armateurs de France. En parallèle de ses fonctions au Cluster maritime français, il est Senior Vice-Président de l'Association Internationale des Pilotes Maritimes et siège à ce titre à l'Organisation maritime Internationale.
Il est également Capitaine de Frégate de Réserve (RCit) de la Marine nationale.

Big data et sécurité maritime, une réalité

par **STÉPHANE CLAISSE**

Le trafic maritime et la vie subaquatique génèrent une multitude d'informations qui, via la définition d'algorithmes spécifiques, doivent favoriser la compréhension de cet écosystème, l'aide à la décision et la prédiction d'événements. Pour cela, il faut déterminer la pertinence des modes de stockage, d'analyse et d'appariement des données au sein d'un Big Data maritime.

Des centaines de capteurs déployés par les centres de recherche en climatologie sur des bouées transmettent chaque jour des informations sur la qualité de l'eau, sa salinité, sa température, etc. et permettent de prédire les événements climatiques de manière de plus en plus précise. Des hydrophones enregistrent les bruits dans les mers et océans et détectent les activités sous-marines.

STÉPHANE CLAISSE

Directeur Adjoint du Pôle Mer Méditerranée
Ingénieur en Chef de 2e Classe des Etudes et Techniques d'Armement

Porté par le CNRS, le projet MEUST, au large de Toulon, développe des moyens particuliers pour détecter les neutrinos des antipodes qui interagissent dans la croûte terrestre et produisent des particules chargées, les « muons », qui pénètrent dans la mer depuis le fond en émettant un flash de lumière bleutée enregistrés par des capteurs répartis sur un réseau au fond de la mer.

Ces dispositifs installés de manière permanente permettent d'obtenir des données en continu et en temps réel. Cette possibilité ouvre des opportunités sans précédent aux sciences environnementales pour, par exemple, étudier l'évolution du climat et de la circulation océanique, la faune des abysses, la biodiversité, la

géodynamique du bassin Ligure, les risques sismiques et les tsunamis. Ainsi, on peut suivre la consommation d'oxygène sur toute la colonne d'eau avec le dispositif « IODA », écouter les mammifères marins et étudier leurs comportements et le suivi de leurs populations, observer de manière non intrusive des organismes profonds bioluminescents, étudier les relations entre formation d'eau profonde et phénomènes climatiques, détecter des tsunamis et les tremblements de terre…

Toutes ces informations sont stockées dans des entrepôts de données, situés parfois en France, corrélées, fusionnées, traitées, optimisées pour générer de nouvelles informations qui deviennent parfois pertinentes dans un autre contexte que celui pour lequel elles ont été réalisées. C'est ainsi qu'on arrive désormais à identifier le meilleur endroit pour installer des éoliennes, afin de maximiser la production d'énergie tout en réduisant les coûts…

Et la sécurité dans tout cela ?

Les nouveaux satellites reçoivent depuis quelque temps les données AIS[1] des navires et sont maintenant capables d'identifier par radar, optique ou optronique, les objets évoluant en mer. La miniaturisation et l'optimisation énergétique font que l'on peut désormais imaginer de nouvelles constellations de satellites, comme STELLA MARINA de THALES ALENIA SPACE, qui rassembleront et transmettront une masse importante de données recueillies sur des zones étendues.

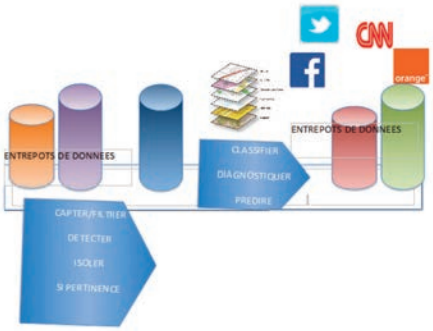
Il ne faut pas oublier que la ZEE française[2] est la seconde, après celle des États-Unis et qu'une surveillance de cette zone implique la mise en place de nouveaux moyens. Les navires de commerce sont de plus en plus équipés de senseurs performants leur permettant d'optimiser leur course et d'utiliser au mieux les courants marins et la météo.

Ils communiquent déjà entre eux pour remonter des alertes. On peut citer le système REPCET, développé par CHRISAR, qui permet d'alerter sur la présence de mammifères marins sur une zone trafic maritime. Utiliser les navires de commerce comme source de données, tout comme les autres sources ouvertes (OSINT), permettra de recueillir de l'information dont la pertinence n'apparaîtra peut-être pas immédiatement mais qui prendra du sens après corrélation avec une nouvelle information.

(1) « Automatic Identification System » signifie système automatique d'identification des navires. Développés dès les années 2000, les transpondeurs AIS de type « Classe A » ont été rendus obligatoires en 2002 pour tous les navires de transport de passagers et les navires de commerce supérieurs à 300 tonneaux. Associé à une station terrestre, l'AIS permet aux autorités portuaires et aux organismes de sauvetage d'assister le service de trafic des navires (VTS : Vessel Traffic Service) en réduisant les risques de collision dans leurs zones de couverture.

(2) Une zone économique exclusive (ZEE) est, d'après le droit de la mer, un espace maritime sur lequel un État côtier exerce des droits souverains en matière d'exploration et d'usage des ressources

Un Big Data maritime efficient impose un stockage sécurisé des données associé à des outils d'analyse pertinents.



Une prédiction efficace repose sur un volume de données pertinent et de capteurs bien identifiés.

Des entrepôts de données pour assurer leur avant même d'imaginer pouvoir les traiter.

Le laboratoire de l'OTAN (CRME à La Spezia), travaille sur le BIG DATA maritime depuis longtemps. Il stocke les informations AIS transmises par les navires depuis 2007. Près de 250 messages sont enregistrés chaque seconde, sur un serveur, qui détient à lui seul quelques pétaoctets de mouvements de navires. Ces informations vont bientôt atteindre l'exaoctet soit 1000 pétaoctets dans quelques années.

Ainsi, il suffit d'un simple SIG (Système d'Information Géographique) puissant pour afficher les données et immédiatement constater que les flottes de pêche étrangères délimitent parfaitement la ZEE française dans le pacifique et s'agglutinent à la limite de la ZEE.

En effet, certains pêcheurs du pacifique utilisent des DCP (dispositifs de concentration de poisson) dérivant pour attirer les bancs de thons, et avant même que le DCP ne rentre dans la ZEE, ils organisent le seinage des bancs de poissons qui sont capturés très facilement et en très grosse quantité.

Certains navires non-collaboratifs sont difficilement détectables car ils n'ont pas d'AIS à bord et sont trop petits et parfois rapides pour être détectés par un radar ; Il convient donc dans ce cas de trouver d'autres moyens de détection : bruit, présence de téléphones satellites ou GSM à bord, sillage, image infrarouge, etc.

L'explosion des moyens d'échanges de données, de communication, des objets connectés nous ouvre de nouvelles pistes pour pouvoir trouver, au sein du Big Data, les données pertinentes, soit homogènes donc fusionables ou hétérogènes autorisant uniquement la corrélation et l'analyse de vraisemblance. Le retour d'‘expérience des spécialistes du traitement des données du CRME est simple : on constate une divergence des analyses et des résultats si les données en excès ne sont pas filtrées correctement. Il convient dans tous les cas de savoir où exactement se trouve le capteur, pour identifier s'il est d'intérêt ou non.

Dans le cadre du futur développement à Toulon, du Sealab Innovation Center, un centre d'innovation collaborative axée sur la sécurité et l'environnement, nous avons pour ambition de créer un *Maritime Situation Awareness Center*, afin de fabriquer les entrepôts de données de la *Maritime Cooperative Operational Picture*.

Ensuite, l'approche à privilégier, pour analyser les données consiste à suivre les étapes de ce schéma : il est important de prédire afin d'anticiper plutôt que de réagir (souvent trop tard !).

Heureusement, les modèles cinématiques des navires sont assez bien connus et cela permet une prédiction des mouvements futurs. La trace et la trajectoire passée permettent un calcul assez simple de la position et de la vitesse future. Pour cela, une combinaison des données AIS, radars dans un contexte côtier, satellites en haute mer, les données météorologiques et océanographiques permettent d'anticiper les mouvements « normaux » de plusieurs heures et d'isoler les anomalies dans le trafic maritime. L'analyse se fonde naturellement sur des bases de données existantes, sur les enregistrements en temps réel et sur des algorithmes de prédictions. En fait l'expérience est un facteur prédominant qu'il faut tenter de modéliser.

Le problème peut devenir très compliqué lorsque ces données de nature hétérogènes ne permettent qu'une analyse contextuelle. Elle conduit à des incertitudes et, de fait, à des solutions qui peuvent diverger.

Le problème de la prédiction peut s'avérer extrêmement difficile mathématiquement car elle peut diverger selon l'approche . On parle de solutions

NP Non Polynomiale. En d'autres termes, chaque solution génère de nouvelles possibilités de résultats et très rapidement on fait face à une « explosion » d'hypothèses. Les scientifiques appellent cela un problème NP exponentiel où l'on perd la réponse dans une masse de solutions.

Comment éviter ce phénomène ? Ce n'est pas le nombre de capteurs qui compte mais leur positionnement ! La combinaison de données hétérogènes ne permet pas de remonter à l'original si le placement des capteurs n'est pas parfaitement connu.

On voit qu'il est important de ne pas confondre (au sens propre de fondre) mais d'associer. Cela prend tout son sens lorsqu'on associe des données satellites, radars, AIS, etc. C'est aujourd'hui une constatation internationale : il faut un nombre suffisant de capteurs et… pas plus ! C'est le revers de la médaille du BIG DATA.

En conclusion, une chaîne fonctionnelle se conçoit et se mesure pour le futur utilisateur avec des objectifs :

• La prédiction à court et long terme des voies maritimes : la météorologie et les courants marins jouent autant un rôle majeur que les marchés financiers dans le cas des bateaux de commerce.

• La reconnaissance des événements en ligne en prenant en compte le « bruit » intrinsèque dans les données voire les imperfections inhérentes aux capteurs.

• L'intégration des données hors ligne maintenues dans les bases de données avec les données réelles en ligne.

Les enjeux sont encore nombreux sur le plan opérationnel : efficacité des calculs en temps réel, diminuer les incertitudes de prédiction et conforter une aide à la décision lorsque les cibles sont multiples à un moment donné !

Enfin les données issues de l'OSINT jouent désormais un rôle très important dans ces analyses : en effet, le moindre tweet posté d'un navire côtier peut donner une information à corréler avec les analyses de comportement et de risques. Les téléphones portables se connectent seuls aux réseaux et trahissent parfois leurs utilisateurs : trianguler un GSM à partir d'un réseau d'antennes relais côtières n'est plus interdit par la CNIL, Orange vient même de lancer un service

professionnel dédié à cette activité. Le BIG DATA est maintenant au centre des affaires maritimes. Il offre une chance unique et inespérée de sécuriser et de protéger les échanges en organisant cette foultitude de données. Il ouvre une nouvelle façon d'analyser des objets en mouvement ou non (au sens large) dans un contexte multi-échelle et spatio-temporel. Le BIG DATA est en fait devenu un outil, il faut maintenant travailler sur les stratégies de décision.

L'AUTEUR

Stéphane CLAISSE, 45 ans, Directeur Adjoint du Pôle Mer Méditerranée, Pôle de compétitivité à vocation mondiale sur la Mer et ses industries.

Diplômé de L'ENSTA Bretagne et de l'INPG de Grenoble, Ingénieur en Chef de 2e Classe des Études et Techniques d'Armement, détaché auprès de DCNS, il a fait sa carrière au sein de DCNS et des ses filiales avec Thales, et a participé notamment à de nombreux projets pour la Défense (Horizon, FREMM), mais a aussi été en charge de projets français ou européens de sécurité maritime (FUI SISMARIS, FP7 I2C, FP7 PERSEUS).

Il est en charge du domaine Sécurité et Sûreté Maritime au sein du Pôle Mer Méditerranée, qui constitue le cluster le plus actif dans le domaine de la sécurité en PACA et Occitanie, avec plus de 400 membres (Grands Groupes, ETI, PME et académiques)

SPATIONAV,
un système de surveillance

par HUBERT SANSOT

La gendarmerie maritime est depuis 2016 partie prenante de l'opération SPATIONAV, un système de surveillance des approches maritimes françaises né de l'organisation particulière de la France dans le domaine de l'action de l'État en mer, dont la maîtrise d'ouvrage est assurée par la Direction générale de l'Armement (DGA).

La surveillance des côtes françaises

La surveillance des côtes françaises est une longue tradition liée à l'histoire de la France et à l'étendue de son littoral. Dès la Révolution était créé le fameux chemin de douaniers qui longe le littoral. En 1806, Napoléon Ier est en conflit avec la Grande-Bretagne. Pour éviter une invasion et lutter contre la contrebande, le sémaphore est créé pour surveiller la mer et rendre compte par signaux optiques avec une plus grande rapidité.

HUBERT SANSOT

Ingénieur en chef des études et techniques de l'armement
Direction générale de l'armement

Après la chute de l'Empire, les sémaphores tombent en désuétude mais sont réactivés en 1862. Confiée à la Marine nationale, la chaîne de sémaphores française s'étoffe alors pour couvrir quasiment la totalité des côtes, chaque site étant choisi pour des raisons stratégiques ou de portée optique sur la mer. C'est ainsi que l'on trouve logiquement très souvent un sémaphore à proximité des phares les plus emblématiques. Aujourd'hui, 59 sémaphores sont présents et sont armés pour la plupart d'une dizaine de guetteurs se relayant H24 pour assurer leur mission.

En 1968, sont créés les CROSS, les Centres Régionaux Opérationnels de Surveillance et de Sauvetage, qui

Marine nationale

SPATIONAV au sémaphore de Carteret.

dépendent aujourd'hui de la Direction des Affaires maritimes (DAM). Chargés de la sécurité en mer, ils sont créés à la même période que le rail d'Ouessant en lien avec l'augmentation très forte du trafic maritime en Manche. Actuellement au nombre de 6, ils travaillent avec les sémaphores au sein de l'action de l'État en mer. L'environnement, le terrorisme, l'immigration clandestine ont fait prendre conscience de l'importance de la chaîne sémaphorique et en particulier, en 2001, lorsque les plages de Saint-Raphaël assistent au premier débarquement massif de migrants sur les côtes françaises (cargo *East Sea* avec 910 Kurdes à bord). Un deuxième cas d'afflux massif venant de la mer interviendra en Corse quelques années plus tard. Cette nouvelle donnée s'impose à l'administration française qui réagit rapidement.

L'action de l'État en mer

L'Action de l'État en mer (AEM) est une organisation française spécifique. Chaque administration participe selon ses caractéristiques et ses moyens sous une autorité administrative unique (le préfet maritime en métropole, le délégué du gouvernement pour l'action de l'État en mer assisté du commandant de zone maritime outre-mer). Cette organisation a l'avantage de coordonner toutes les administrations, sans pour autant disposer d'un budget propre.

La mise en évidence de failles de détection dans les approches maritimes décide le Secrétariat général de la Mer, service sous l'autorité du Premier ministre en charge de la coordination de la politique maritime de la France, à mettre en œuvre un système de surveillance efficace.

En 2001, la Marine nationale émet une première expression de besoin pour le système SPATIONAV à la DGA. Celle-ci est chargée en particulier de l'acquisition des matériels militaires pour le ministère de la Défense et fournit pour l'occasion son expérience en gestion de projet et son expertise des systèmes d'information opérationnels et de combat. Pour SPATIONAV, la DGA assure ainsi la cohérence du besoin entre les différentes

administrations, acquiert le système et assume la responsabilité technique du déploiement en coordonnant les activités des organismes chargés du réseau ou des infrastructures, et des organismes de soutien.

SPATIONAV

Sur un mode incrémental, une première version V0 de SPATIONAV a été notifiée à l'industrie en 2002 pour disposer rapidement sur la façade méditerranéenne d'un premier système d'information afin de synthétiser la capacité de surveillance des radars préexistants. Chaque sémaphore de Méditerranée, mis en réseau, retransmettait ensuite ses informations à l'autorité militaire de Toulon.

La version V1 de SPATIONAV a été lancée mi-2005 afin d'améliorer l'ergonomie du système, d'ajouter des capteurs de données AIS[1] émises par les navires et de disposer d'une synthèse nationale de l'ensemble des situations des approches maritimes de la France (Méditerranée, Manche, Mer du Nord et Atlantique) ainsi que d'équiper plusieurs autres administrations de postes d'exploitation (Douanes et CROSS).

(1) AIS : le navire émet des rapports comportant des données de position et des caractéristiques clefs. Ce matériel est imposé pour les navires de plus de 20 mètres pour des raisons de sécurité, anti collision notamment.

La version V2 de SPATIONAV a été lancée en 2011 afin de rénover les radars antérieurs au lancement du système et de compléter la couverture par des capteurs complémentaires (radars, capteur des données AIS émises par les navires, goniomètres…). Elle doit présenter aux préfets maritimes et à tous les centres de coordination et de surveillance des frontières extérieures la situation des approches maritimes dans une fréquence proche du temps réel. Enfin elle permet un échange de données avec l'ensemble des systèmes équivalents à travers l'Europe. Son déploiement s'est achevé en 2016 pour la France métropolitaine.

Aujourd'hui SPATIONAV V2 est un système complet couvrant l'ensemble des côtes françaises regroupant 75 radars, 36 stations AIS, 62 goniomètres et 2 caméras thermiques. Ces capteurs fonctionnent en réseaux et sont situés sur les sémaphores, sur des sites isolés, sur les CROSS et sur 8 Falcon 50 de la Marine nationale.

Chaque navire naviguant à proximité des côtes est donc ainsi détecté et enregistré. Il fait également l'objet d'une fiche navire renseignée automatiquement, à partir notamment des données AIS reçues et des informations radar. Elle est complétée manuellement par les opérateurs des CROSS ou par les guetteurs sémaphoriques qui interrogent par radio systématiquement les navires d'importance approchant des côtes. Toutes ces données brutes des capteurs sont traitées en local puis regroupées et corrélées sur deux sites centraux pour la

façade Manche/Mer du Nord - Atlantique et la façade Méditerranée. L'été, ce sont environ 8 000 pistes qui ont été détectées et traitées en temps réel le long des côtes françaises. Ces données agrégées sont retransmises en temps réel aux sites capteurs qui disposent de deux vues : leur situation locale et une situation complète des approches maritimes de leur façade.

L'ensemble est agrégé pour fournir la situation nationale. Ces deux niveaux d'information, national ou par façade, sont distribués à des sites d'exploitation ne disposant pas de capteurs : 6 CROSS, 4 sites de la douane (COD, DNRED), 9 sites de la gendarmerie maritime, 4 centres de commandement et opérationnels de la marine nationale (COM, État-major des opérations de la marine), ainsi que le Centre opérationnel de la fonction garde-côtes (COFGC).

SPATIONAV permet aussi de fournir des données en dehors du réseau du ministère de la Défense, en temps différé. Ainsi SPATIONAV transfère l'ensemble des données des AIS aux Affaires Maritimes, avant qu'elles ne soient transférées à des systèmes européens. Il communique également ses pistes à un système de commandement de la Douane. Dans le cadre d'un champ de coopération qui débute, SPATIONAV dispose d'une capacité d'échanges avec tous les systèmes européens *via* des normes standardisées et ouvertes.

Le soutien financier européen

Depuis 2001, les différents incréments de SPATIONAV sont portés pour l'essentiel par le budget de la Défense, les autres administrations finançant principalement les matériels ou des modifications qui leur sont spécifiques. La surveillance maritime reste un dispositif à bas coût, chaque capteur est repris de technologies civiles largement répandues. Le logiciel SPATIONAV est développé par une PME française, leader mondial dans le domaine de la surveillance maritime.

SPATIONAV s'inscrit dans le cadre d'EUROSUR, projet européen de surveillance des frontières maritimes. Il bénéficie à ce titre du soutien de fonds européens. Sans ce soutien indispensable, le système SPATIONAV n'aurait pas vu le jour.

Une efficacité opérationnelle immédiate avec de nouvelles possibilités d'action

Depuis 2003, le phénomène migratoire s'appuyant sur de gros navires abordant les côtes n'est plus réapparu en France. Déployé depuis 2013 en Méditerranée à la place de la version précédente, et équipé de radar détectant mieux les petites embarcations, SPATIONAV V2 a permis de bloquer de nouveaux phénomènes.

En 2014, un guetteur sémaphorique observe une trace extrêmement rapide et fugace sur le système. Quelques jours

plus tard, les guetteurs et leur hiérarchie sont de veille de nuit et un *speed boat* est intercepté. Aucun navire de ce type ne cherchera plus à intervenir dans la zone, préférant donc refluer vers l'Espagne.

En 2016, un sémaphore de la Manche observe une faible trace radar, les îles anglo-normandes sont à quelques nautiques. L'embarcation se dirige vers la Grande Bretagne et ses autorités sont prévenues. Une lutte contre les passeurs commence en Manche et SPATIONAV V2 en est l'outil principal. Des filières sont démantelées avant qu'elles ne montent en puissance à partir des Pays-Bas ou de la Belgique.

L'année 2016 marque surtout un changement radical dans le mode fonctionnement du fait de la mise à disposition de SPATIONAV à un nombre très important d'organismes exploitant le système à distance, sans capteur propre. Ce sont désormais les capacités avancées du système qui peuvent être utilisées à grande échelle.

Sur requête, il est possible de rejouer une situation datant de plusieurs mois et donc de fournir des indications précises valant présomption de preuve.

Sur renseignement, un organisme peut définir précisément l'arrivée d'un navire suspect et organiser son accueil à un port, une plage, voire guider une embarcation chargée d'une intervention.

D'ores et déjà, le système permet à chaque utilisateur de créer des zones et des alertes. Ainsi la simple fonction de filtre permet de n'avoir que les navires d'intérêt sur l'écran. Immédiatement, on peut constater que la moitié du trafic maritime dans les eaux territoriales françaises est le fait de navires n'émettant pas d'AIS donc le plus souvent des navires légers de moins de 20 mètres.

Sur des critères simples de vitesse, un opérateur peut mettre en place une alerte sur l'ensemble d'une façade fonctionnant en temps réel. Il peut recevoir immédiatement une alerte lorsqu'un navire au large des côtes a une vitesse nulle ou anormalement basse laissant imaginer des transbordements ou des mises à l'eau. Sur un critère de vitesse maximale, il est possible d'avoir une alerte globale de la présence de speed boat. Enfin, il est possible de détecter immédiatement les comportements suspects, tels que le franchissement de nuit des eaux territoriales pour certains types de navires ou le départ de la côte.

DGA

SPATIONAV vue.

Perspectives

Comme on a pu le voir, le système SPATIONAV est déjà un outil de coopération interadministrations qui a bénéficié de manière déterminante du soutien des fonds européens. Il s'ouvre actuellement un champ d'utilisation nouveau avec la possibilité de coopérations internationales en connectant le système SPATIONAV avec les systèmes des autres nations. Le système continuera pour sa part à évoluer sous la responsabilité technique de la Direction générale de l'Armement pour répondre au besoin des différentes administrations participant à l'action de l'État en mer et anticiper la menace.

Sociétés privées de sûreté
maritime et partenariats opérationnels

par THIERRY HOUETTE

Les premières années du XXIe siècle sont le siège de très nombreux conflits et actes asymétriques : terrorisme, piraterie, trafics en tous genres. La maritimisation de l'économie mondiale et la faible capacité des États à surveiller et intervenir en mer favorisent l'épanouissement des actes délictueux et criminels. Pour faire face à cette situation, les opérateurs publics et privés doivent travailler ensemble. Cet article donne la vision d'un groupe de PME spécialisé dans la sûreté maritime.

La sûreté maritime et son application en Afrique

THIERRY HOUETTE
Directeur du groupe de sécurité marine, Prorisk International

Une histoire ancienne

La sûreté représente l'opposition constituée contre les actes ou les intentions malveillantes. Elle est distincte de la sécurité qui traite des situations accidentelles et de leurs conséquences. La sûreté se confronte à un agresseur souvent inconnu, aux intentions et aux modes opératoires imaginés par anticipation et dont les motivations sont souvent supposées mais non vérifiées. C'est la raison pour laquelle la sûreté a toujours été un besoin. Elle appuie son action sur le renseignement pour prévenir la menace et sur la dissuasion pour éloigner l'agresseur.

Une nécessité réveillée par l'attentat du 11 septembre 2001

Le 11 septembre 2001, l'irruption d'un terrorisme radical a rendu nécessaire le renforcement de la sûreté. Le monde maritime n'a pas échappé à ce besoin. Dès juillet 2004, le code ISPS[1]

(1) International Ship and Port Facility Security (ISPS), « Code international pour la sûreté des navires et des installations portuaires ». Il a été adopté le 12 décembre 2002 par la résolution 2 de la Conférence des gouvernements contractants à la Convention internationale pour la sauvegarde de la vie humaine en mer (Solas) de 1974.

Des infrastructures hétérogènes et liées à une prolifération d'activités économiques peu maîtrisées.

a défini une organisation et la mise en application des procédures de protection des ports internationaux et des navires de commerce contre les actes de terrorisme, les trafics illicites, les vols, les malveillances et l'immigration clandestine. Ce renforcement sécuritaire a engendré une profonde modification doctrinale en impliquant les opérateurs et les usagers des ports : La surveillance, le contrôle des accès et des aires de travail relèvent désormais de leur responsabilité, l'intervention restant régalienne.

L'application du code ISPS a été bénéfique pour l'activité portuaire et a augmenté la sécurité des agents qui y travaillent. En clôturant les ports et en établissant des autorisations d'accès la circulation a été facilitée et l'encombrement des aires de travail fortement réduit, générant ainsi un gain de productivité et parallèlement une réduction des risques d'accident. Ainsi, en une dizaine d'années, certains ports africains ont évolué radicalement en substituant aux traditionnels et pittoresques marchés locaux des terminaux performants où la circulation reste rigoureusement limitée au strict nécessaire.

Un besoin confirmé par la montée de la piraterie

L'avènement des pirates somaliens a provoqué la deuxième secousse sécuritaire avec la prise du Ponant en 2008 et les nombreuses attaques qui suivirent. Leurs abordages musclés, leurs prises d'otages et leur incroyable rayon d'action ont étonné le monde entier. L'augmentation des primes d'assurance a perturbé le business et les marines militaires se sont déployées pour

dissuader et intervenir. A bord des navires de commerce, les « Best Management Practices »[2], validées par l'Organisation Maritime Internationale, ont mis en place des mesures et des procédures visant à empêcher la montée à bord de pirates. Le cas échéant, elles organisent le regroupement de l'équipage dans un espace sécurisé, la citadelle, en attendant l'arrivée de forces de secours.

(2) Best management pratices for protection against somalia based piracy / Suggested Planning and perational Practices for Ship Operators and Masters of Ships Transiting the High Risk Area http://www.mschoa.org/docs/public-documents/bmp4-low-res_sept_5_2011.pdf?sfvrsn=0

(3) EPPN : entreprise privée de protection des navires.

L'immensité des océans et le grand nombre de navires de commerce empruntant chaque jour les routes maritimes n'ont pas permis aux seules forces internationales d'éradiquer la piraterie. La protection de chaque navire par une équipe armée privée (EPPN)[3] s'est petit à petit imposée comme une solution d'autoprotection efficace et bon marché.

Le cadre juridique du navire est complexe : droit de l'État du pavillon, droit de l'État côtier et droit international se chevauchent ou se substituent selon l'éloignement du navire vis-à-vis de la terre. La piraterie s'exerce exclusivement en haute mer selon le droit international (convention de Montégo Bay). Elle est souvent confondue avec le brigandage à main armée en zone côtière. Comme le droit du pavillon du navire s'applique pleinement en haute mer, chaque Etat a souhaité encadrer l'action des EPPN dans le strict cadre de la légitime défense.

Les premiers pays autorisèrent l'activité des EPPN dès 2009. La France adopta pour ses navires une loi en juillet 2014, applicable fin 2015. Certes tardive, la réglementation française reste cependant la seule à encadrer clairement cette activité. La France est surtout la seule à engager sa responsabilité en délivrant, à chaque agent, une carte professionnelle obligatoire attestant de sa qualification et de sa bonne moralité.

Une nécessité vitale pour l'économie mondiale « maritimisée »

La maritimisation de l'économie mondiale provoquera probablement la troisième secousse sécuritaire. En Afrique, les ports représentent les portes d'accès aux marchés internationaux. Comme beaucoup de pays manquent d'infrastructures routières et ferroviaires performantes pour acheminer les marchandises dans tout leur territoire, une migration des populations s'opère des campagnes vers les villes littorales et principalement vers les ports où le travail se fait rare. L'accueil de cet afflux n'est pas maîtrisé par manque de moyens et d'infrastructures. La surpopulation entraîne la pollution des eaux côtières qui appauvrit la pêche artisanale traditionnelle. Ainsi, l'inactivité d'une partie de la population augmente et les désœuvrés sont attirés par les nouvelles

Le soutien comporte la formation de personnels qualifiés qui puissent mettre en œuvre des mesures de protection.

activités illicites et lucratives liées à la mer : trafics illicites, brigandage, piraterie, etc.

Les États côtiers manquant d'organisation pour conduire et coordonner leur action en mer, les initiatives criminelles et délictueuses s'épanouissent et bafouent leurs droits dans leur Zone économique exclusive (ZEE) souvent en toute impunité. Ces enjeux de maîtrise de l'espace maritime deviennent aujourd'hui majeurs pour la survie à terme de la plupart des États.

En France, le concept d'Action de l'État en mer (AEM), né à la fin des années soixante-dix, mutualise les ressources nécessaires pour la surveillance et l'intervention des moyens étatiques. Il s'est développé autour de la marine nationale qui possède les moyens hauturiers[4] bien que les missions de l'AEM soient civiles. D'autres pays ont opté pour des services dédiés de gardes-côtes. La majorité des pays francophones du Golfe de Guinée ont choisi le modèle français. Trouver un bon équilibre permettant aux services d'assumer leurs missions en mer tout en optimisant l'emploi des moyens de surveillance et d'intervention en mer constitue un exercice délicat pouvant prêter à des alternatives doctrinales et opérationnelles.

(4) On parle de navigation hauturière lorsque le navire navigue en haute mer (hors de vue de terre) et de navigation côtière (ou cabotage, mais ce terme est restreint à l'activité exercée) lorsqu'il navigue en vue des côtes.

Un besoin de solutions globales et adaptées reposant sur 3 pôles d'excellence.

Pour être pertinente et efficace, une réponse globale aux questions sécuritaires s'impose. La problématique pourrait se décliner au travers de cette question : comment, face à des menaces maritimes multiformes, agir efficacement, sans délai mais dans la durée et la permanence, avec peu de moyens matériels et des équipes peu expérimentées et insuffisamment formées ?

La coopération internationale apporte sa réponse mais les moyens financiers des

contributeurs tendent à diminuer. Les sociétés privées font également des propositions utiles et performantes. C'est dans ce cadre que la Holding française GROUPE PRORISK s'implique fortement avec pour ambition d'apporter une réponse globale aux problématiques de maîtrise des espaces maritimes et des activités économiques qui s'y déroulent. Sa vision vise à asseoir, dans le cadre d'un partenariat public-privé, une relation avec les états pour renforcer leur efficacité et harmoniser leur organisation au plan national ou au niveau d'une sous-région. Elle comprend une ingénierie susceptible de protéger et d'assurer un développement durable des activités industrielles, touristiques, de la pêche et de l'aquaculture dans le respect de l'environnement. Dans cet esprit, le groupe accompagne les industriels et les acteurs publics et privés du monde maritime et portuaire pour la définition, la mise en place et la mise en œuvre de leur politique et de leurs obligations en matière de sûreté.

La crédibilité et l'efficacité des propositions reposent sur la maîtrise de trois pôles d'excellence : l'ingénierie-conseil, la formation et le soutien opérationnel. Ils constituent les ingrédients indispensables à l'élaboration et la mise en place de la sûreté maritime.

L'ingénierie-conseil contribue à l'identification des menaces, à l'évaluation des risques et à la rédaction de plans de sûreté mais également à la définition des moyens pour réduire les risques et la rédaction des cahiers des charges afférents.

L'application du code ISPS, sous la pression des garde-côtes US, pousse les ports à améliorer leur performance sécuritaire. Cependant, on constate souvent une faiblesse de l'organisation mise en place et l'absence d'une réglementation applicative nationale. Cette situation peut être génératrice de corruption et d'abus de pouvoir au détriment de la sûreté et de la sécurité.

Lorsqu'elle s'adresse à un État, l'ingénierie-conseil apporte une assistance pour la définition et la rédaction des corpus réglementaires et des procédures organisant l'AEM. La définition de l'organisation des services étatiques, de leurs missions et des moyens qui leur sont alloués constitue une condition *sine qua non* pour que l'AEM existe.

La formation est le moteur de la réussite car sans compétences on ne peut escompter des résultats probants. Le milieu maritime reconnaît 3 niveaux de responsabilités : opérateur, contremaître et cadre. En matière de formation et de sûreté, l'offre, bien qu'insuffisante, évolue positivement comme l'atteste la création de l'Institut de sécurité maritime interrégional (ISMI) à Abidjan, relevant de l'OMAOC[5] et soutenu par la France, les

Groupe Prorisk

L'ingénierie-conseil est la pierre angulaire d'une régulation des transactions économiques au sein d'ensembles portuaires nouveaux souffrant d'une réglementation insuffisante.

(5) Organisation Maritime de l'Afrique de l'Ouest et du Centre - http://www.omaoc.org/FR/statjuridique.php

USA et l'Union européenne. L'insuffisance évoquée relève d'un manque de structures adaptées mais également de la difficulté liée au coût du déplacement des élèves d'un pays vers l'un des rares centres de formation. La coopération internationale met en place des séminaires ou des stages de formation, en particulier pour ce qui relève de la sûreté maritime élargie à certains domaines de l'AEM, mais les programmes de coopération sont limités dans le temps et dans l'espace alors que les besoins s'inscrivent dans la durée et touchent tous les pays côtiers.

Tenant compte de ces difficultés, GROUPE PRORISK a développé une gamme de formations destinée aux agents de tous les services d'un État dès lors qu'ils sont impliqués dans l'AEM.

Le soutien opérationnel est humain et matériel. Il vise à mettre à disposition d'un client des moyens pouvant contribuer à la bonne marche d'un service ou à la réalisation de tout ou partie d'une mission. Si la coopération internationale

et principalement militaire agit depuis longtemps dans ce domaine, la diminution des budgets et la réduction des effectifs militaires tendent à minorer cet effort. L'opportunité d'un partenariat public-privé est évidente au regard des énormes besoins des acteurs. Dans ce contexte, une offre privée permet la mise à disposition des acteurs locaux, pour des durées à convenir, des assistants opérationnels. Leur mission peut être de participer à la mise en ordre de marche des systèmes et centres opérationnels en apportant leur expertise et leur expérience et d'assurer l'entraînement des opérateurs. L'expertise de sociétés privées, comme le groupe Prorisk, dans le cadre de sa palette de métiers, autorise la proposition de renforts en termes de vecteurs pour améliorer la couverture et la fréquence de la surveillance des espaces maritimes. Les moyens déployés peuvent être mutualisés entre plusieurs pays. Les coûts opérationnels sont ainsi lissés et la maintenance et l'entretien n'incombent pas à l'utilisateur.

Élaborer une réponse globale française dans le cadre de partenariat public privé

Comme nous l'avons évoqué, la solution à la problématique de la sûreté maritime ne peut être qu'une réponse globale. Or, selon que l'on est prestataire ou demandeur de services, étatique ou privé, les intérêts divergent. En premier lieu, il convient de faire converger ces intérêts vers la réponse aux attentes du client. Aujourd'hui, c'est dans le montage de la proposition vers le client que des améliorations sont nécessaires et possibles.

Possibles car il s'agit de mettre en ordre de bataille l'ensemble les acteurs français souhaitant intervenir au profit d'un pays étranger pour la sûreté maritime. Pour cela, il conviendrait de créer ou désigner une autorité en charge d'analyser des besoins, de coordonner et de répartir la participation des sociétés privées et des services étatiques tout en vérifiant la cohérence et la recevabilité de la solution globale ainsi élaborée. Le Secrétariat général pour la mer (SGMER) joue un rôle de coordination interministérielle pour l'AEM français. Un élargissement de ses prérogatives au pilotage de programmes maritimes internationaux pourrait satisfaire cette ambition. Chaque société partenaire serait alors responsable de l'exécution de sa part de marché mais resterait soumise au suivi collégial d'un comité de pilotage sous la responsabilité de cet SGMER export.

Nécessaires car une PME n'est pas de taille pour traiter avec un État alors qu'elle peut être porteuse d'une partie de la solution globale attendue. Dans le cadre d'un partenariat public-privé français, elle devrait pouvoir proposer ses solutions. Dans le contexte intérieur de menace terroriste, une implication des acteurs privés allégerait la charge des forces de

sécurité. Dans le cadre des marchés export de la sûreté maritime, cette démarche est « gagnante-gagnante » pour les services étatiques et les sociétés privées françaises. Elle offre la cohérence et le réalisme qui sont indispensables pour remporter des marchés où des concurrents, peut-être moins pertinents, sont très offensifs. Dans cette logique, qui mériterait d'être poussée plus loin, Laurent Fabius, ministre des affaires étrangères, avait ouvert une voie en souhaitant favoriser l'ouverture des marchés à l'étranger aux PME grâce à l'assistance des missions économiques à l'étranger.

L'AUTEUR

Les 25 ans passés dans la Marine Nationale par le capitaine de vaisseau (R) Thierry Houette, ont été essentiellement partagés entre des embarquements et commandements opérationnels et des responsabilités en État-major. Revenu à la vie civile en 2002 , il devient ingénieur d'affaires pour une société High-Tech œuvrant dans l'imagerie acoustique des fonds marins. En 2005, il créé la société Marine Management et Services et s'associe dans la société KSI, organisme de sûreté maritime et portuaire habilité par l'administration française et centre de formation agréé. Il fonde, en 2010, Prorisk International, entreprise spécialisée dans la protection des navires transitant en zone à risque de piraterie. En 2013 il regroupe l'ensemble de ses activités au sein de la société holding Groupe Prorisk traitant de la sûreté et de la maîtrise et sauvegarde des espaces maritimes.

Grands aéroports,
réorganisation des services de l'État

Entretien avec PHILIPPE RIFFAUT

réalisé par le lieutenant-colonel Hugues Hornbeck

Monsieur le Préfet, dans le cadre de la menace terroriste, comment se sont réorganisés les services de l'état qui sont sous votre autorité ?

Le préfet délégué a un rôle central en matière de coordination interministérielle sur les aéroports de Paris-Charles de Gaulle et de Paris-Le Bourget. Cette fonction, unique en France et rappelée par la circulaire interministérielle du 3 octobre 2007, en fait le garant d'un positionnement cohérent des services de l'État intervenant dans la sûreté et la sécurité aéroportuaire. Ayant pris mes fonctions en décembre 2014 et ayant vécu les événements de janvier 2015, j'ai pris immédiatement la mesure du risque terroriste sur les sites qui relevaient de ma responsabilité. Il a été l'occasion de repenser l'intégration et la coordination des services de l'État. Le concept de « police d'agglomération de la métropole parisienne » a consacré l'intégration de la plate-forme aéroportuaire dans le dispositif des services de la Préfecture de police de Paris. La DOPC (Direction de l'ordre public et de la circulation) va prendre en compte la circulation routière sur l'aéroport (200 km de réseau routier) ainsi que l'ordre public en dehors des aérogares. La DSPAP (Direction de la sécurité publique de l'agglomération parisienne) va quant à elle assurer les missions de sécurité publique et de police judiciaire dans le secteur hôtelier de la plate-forme, dans le centre commercial Aéroville de même que sur l'aéroport du Bourget. Ainsi, la PAF pourra se consacrer à son cœur de métier : le contrôle aux frontières et la sécurité et l'ordre publics dans les aérogares.

PHILIPPE RIFFAUT

Préfet, délégué à la sécurité et à la sûreté des plates-formes aéroportuaires

J'ai également ilancé les nécessaires travaux de réflexion et de conception des plans spécifiques d'intervention. Ils tiennent compte de l'évolution de la menace et intègrent cette nouvelle configuration des forces en présence (n'oublions pas le dispositif Sentinelle). Ils visent à apporter une réponse rapide, adaptée et garantissant une acquisition de la réalité des faits et une cohérence dans la direction des opérations. Ces plans sont maintenant opérationnels.

La dimension du renseignement a-t-elle été intégrée dans le dispositif ?

Le recueil du renseignement, la capacité de son traitement et de son exploitation sont les bases d'une action efficace et adaptée à une menace. La création d'un service du renseignement dédié

à nos aéroports relève de cette stratégie. En effet, j'ai rapidement été amené à faire le constat de l'insuffisance de la dimension « renseignement » sur l'aéroport. Le portrait que l'on avait de la plate-forme dans les domaines du communautarisme ou du social, par exemple, relevait de l'empirique et des constats qui avaient été dressés du temps des RG. Aussi ai-je proposé au ministre, qui a soutenu la démarche, la constitution sur la plate-forme d'une antenne du renseignement territorial dédiée aux aéroports de Paris CDG et Le Bourget. Cette unité, implantée depuis le mois de septembre, constituée de fonctionnaires de la DRPP, de gendarmes de la GTA, de policiers de la PAF et très bientôt de fonctionnaires de la douane, travaille en étroite collaboration avec les services du renseignement territorial et la DGSI.

Quelles sont les mesures techniques qui ont été mises en œuvre pour limiter le risque d'attentats sur les surfaces aéroportuaires ?

Les mesures qui sont mises en œuvre ressortent des acteurs régaliens et privés qui forment une « communauté aéroportuaire ». Elles sont de deux ordres. La première mesure concerne un quadrillage des surfaces par le déploiement efficient d'une ressource humaine spécialisée. La seconde repose sur la mise en œuvre de moyens techniques qui permettent de cerner les flux des personnes et du fret. Le dispositif de sécurité intègre, dans le cadre de l'opération « Sentinelle », le renfort d'une compagnie de 122 militaires. Ils assurent leur mission en pleine complémentarité avec les policiers par des missions de patrouilles permanentes dans les aérogares et sur les surfaces périmétriques de la plate-forme. Les policiers, qui disposent de nouveaux équipements (fusils d'assaut, protections balistiques et casques), bénéficient d'une formation continue en matière de réponse rapide face au risque terroriste. Il faut ajouter à ce dispositif la composante « piste » assurée par la gendarmerie des transports aériens et un PSIG sabre, dédié à la plate-forme, composé de militaires de la gendarmerie spécialement formés et dotés d'un équipement adapté : fusils d'assaut, casques et visières balistiques, gilets pare-balles et boucliers résistant à des munitions d'armes automatiques. S'intègre à ce dispositif le renforcement décidé par la direction de l'aéroport de mesures de sûreté par les opérateurs de sûreté et le déploiement de patrouilles régulières, y compris cynophiles, dans les aérogares.

Les moyens techniques concernent essentiellement un important système de vidéosurveillance par caméras, fonctionnant dans le cadre juridique du respect des droits personnels. Un dispositif LAPI de lecture automatique de plaques minéralogiques complète cette architecture. Une réflexion est menée pour renforcer ce dispositif à l'aide de drones spécialisés. Par ailleurs, les tests d'équipements automatiques performants de passage à la frontière, reposant sur la technologie de la reconnaissance faciale, seront installés au printemps afin de trouver un compromis entre la sûreté et la fluidité des flux commerciaux.

Pour terminer, je veux préciser que la sûreté aéroportuaire résulte de la cohérence de l'action des forces de sécurité, de services de l'État et des acteurs privés qui sont résolument engagés dans la lutte contre le risque terroriste. Elle comporte des processus appliqués sans faille, revisités par un retour d'expérience dans le cadre d'une concertation de toutes les parties prenantes. Cette vigilance de tous les instants repose également sur l'organisation du recueil des informations et renseignements susceptibles d'être exploités par les services spécialisés de l'État.

La GTA est l'expression d'une expertise en matière de sûreté aéroportuaire

entretien avec FRANCIS FORMELL

réalisé par Philippe Durand, rédacteur en chef de la revue

Dans un contexte de menace terroriste sur les plates-formes aéroportuaires, quelle est la place de la Gendarmerie des transports aériens (GTA)?

Les missions principales de la GTA sont la sûreté, la police judiciaire, l'intervention et le renseignement. Elles placent naturellement la GTA comme un des acteurs majeurs contribuant à la protection de l'aviation civile et du transport aérien. L'évolution des missions liée à l'émergence de nouvelles menaces impose une présence accrue sur le terrain et le renforcement de notre capacité à recueillir du renseignement, notamment les signaux faibles de radicalisation.

FRANCIS FORMELL

Colonel de gendarmerie commandant la gendarmerie des transports aériens

Le secteur aérien, revêtant une grande sensibilité dans un contexte de menace terroriste, nécessite la mise en œuvre de processus de haut niveau pour assurer, dans un milieu interministériel, la sûreté des plates-formes aéroportuaires.

Disposant de militaires spécialement formés, la GTA est compétente pour vérifier la mise en œuvre effective des mesures de sûreté sur l'ensemble de sa zone de compétence, principalement le « côté piste » des aéroports.

Par ailleurs, nous avons recruté récemment un ancien personnel du Groupe d'intervention de la gendarmerie nationale (GIGN), chargé d'animer l'intervention professionnelle au sein de notre formation. Il permettra à l'ensemble des unités d'améliorer leur réaction face à un évènement potentiellement de haute intensité.

Comment s'articule le dispositif de la GTA dans le cadre de ses missions sur les plates-formes aéroportuaires ?

Formation spécialisée de la Gendarmerie nationale, la GTA est placée pour emploi

La GTA exerce des missions spécifiques de sûreté à l'intérieur des zones « côté piste » notamment par un contrôle des titres de circulation aéroportuaire.

auprès du directeur général de l'Aviation Civile. Forte de 1038 personnels en métropole, elle est organisée selon une structure classique de la gendarmerie en s'appuyant sur un état-major, 2 groupements et 9 compagnies. Ses 31 brigades (BGTA) couvrent les plus grands aéroports français sur lesquels les militaires accomplissent l'ensemble des missions dévolues à la gendarmerie nationale. La capacité judiciaire de ces unités de terrain est renforcée par une section de recherche à compétence nationale et 2 brigades de recherches épousant la compétence territoriale des groupements.

Pour assurer sa mission spécifique de sûreté, la GTA s'est dotée d'une structure complète, le « réseau sûreté », calquée sur le modèle des chaînes judiciaire et de renseignement. En plus des brigades qui agissent chaque jour pour assurer la sécurité des mouvements aériens, 6 Pelotons de surveillance et d'intervention (PSIGTA) complètent ce dispositif sur les aéroports.

À ce sujet, je souhaite souligner le « glissement » réussi de nos PSIG parisiens en PSIG Sabre. Ces gendarmes spécialisés, immédiatement mobilisables, sont en mesure de se projeter rapidement sur le lieu d'une crise en attendant la venue d'unités hautement spécialisées comme le GIGN. Primo-intervenants, ils ont pour mission de fixer les terroristes et de les neutraliser par le feu selon la situation. Ces unités ont vu leur dotation en matériel significativement renforcée et adaptée à leurs missions (pack balistique, armement spécifique composé notamment de fusils HKG36 et d'aides à la visée). Spécialistes du milieu aéroportuaire, elles sont soumises à un entraînement particulier et confrontées à des mises en situation

réalistes. Au sein de ces unités, 7 binômes d'observateurs contre-tireurs, dotés de fusils de précision de type TIKKA T3 et ULTIMA RATIO, sont notamment chargés de neutraliser tout auteur d'une tentative d'agression sur les dirigeants de l'État français ou des pays étrangers. Formés par le GIGN, ils sont présents pour couvrir tout événement sensible bien qu'ils restent « invisibles » au commun des usagers.

Des équipes cynophiles, spécialisées en matière de recherche d'explosifs, évoluent sur les plates-formes aéroportuaires. Après leur formation initiale, les chiens bénéficient d'entraînements spécifiques qui permettent d'optimiser leur évolution en zone « côté piste », malgré le bruit et les odeurs spécifiques à ce milieu particulier. Ces unités peuvent par ailleurs être engagées sur d'autres missions, notamment en soutien des équipes de déminage de la sécurité civile.

Sur le plan judiciaire, la Section de recherches de la gendarmerie des transports aériens (SRGTA) a su développer une forte capacité d'expertise. Dans le domaine de la lutte contre la criminalité, les enquêtes les plus sensibles, concernant les produits stupéfiants et les vols de fret, ont permis la saisie de plusieurs millions d'euros d'avoirs criminels. Par ailleurs, dotée de matériels spécifiques et projetables, la SRGTA reste une référence dans le domaine des enquêtes judiciaires lors des accidents aériens (Rio-Paris, Germanwings…). Cette unité sait s'appuyer sur des experts de haut niveau dont certains sont intégrés au sein des réserves de la gendarmerie.

La GTA a ainsi complété son dispositif en faisant appel à une réserve opérationnelle d'environ 200 personnels. Anciens de l'arme ou issus de préparations militaires gendarmerie, ils sont employés sur l'ensemble des aéroports en fonction des besoins des unités et de l'activité. Enfin, elle a renforcé son dispositif par une réserve citoyenne composée de volontaires issus de la société civile, agréés par l'autorité militaire en raison de leur expérience et de leurs compétences.

La gestion du renseignement est essentielle pour asseoir une action. Quels sont vos moyens en la matière ?

Le renseignement est au cœur des préoccupations du commandement de la GTA. Nous nous appuyons pour réaliser cette mission sur l'ensemble de nos unités. Chaque militaire de la GTA se comporte comme un capteur actif du renseignement dans l'exécution de sa mission. La chaîne de renseignement, activée sur l'ensemble des unités, est animée par un Centre de renseignement opérationnel armé H24 (CRO GTA). Sa compétence est parfaitement identifiée et reconnue de l'ensemble des acteurs intervenant autour de l'aviation civile.

À ce titre, la GTA est aussi pleinement intégrée dans le dispositif de lutte contre la radicalisation. Son action dans ce domaine s'est renforcée depuis les attentats perpétrés sur le territoire.

Ainsi, la GTA s'inscrit dans le dispositif conçu au sein du ministère de l'Intérieur et assure par son positionnement la continuité du maillage territorial. Elle

partage les renseignements collectés sur sa zone de compétence avec les autres services en charge du renseignement et participe aux Groupes d'évaluation départementaux (GED).

Au mois de juillet 2016, l'aéroport de Paris-Charles-de-Gaulle a été doté d'une Antenne du renseignement territorial (ART) rattachée à la Direction du renseignement de la préfecture de police de Paris (DRPP). Forte d'une trentaine de personnels, elle est composée de policiers de la DRPP et de 2 gendarmes de la GTA.

Par ailleurs, l'action de lutte contre la radicalisation sur les aéroports de province sera aussi renforcée. Neuf nouvelles antennes seront créées sur les grands aéroports où la GTA participera à hauteur de deux militaires (BEAUVAIS, ORLY, NANTES, BALE-MULHOUSE, NICE, LYON, MARSEILLE, TOULOUSE et BORDEAUX).

Enfin la GTA expérimente un outil de détection des comportements atypiques visant à identifier aussi précocement que possible toute intention d'action illicite, notamment terroriste.

Cette expertise est-elle partagée ?

Notre expertise est reconnue par la Direction de la coopération internationale (DCI) et la DGAC qui nous sollicitent pour de nombreuses missions à l'étranger afin de comparer nos pratiques avec nos partenaires à l'international et de mettre en avant notre savoir-faire. À cette occasion, nous participons aussi à des groupes de travail et à des séminaires internationaux.

Suite à notre adhésion en 2010 au réseau AIRPOL, nous pouvons disposer de points de contact utiles dans chaque pays membre mais également recenser les phénomènes délictueux et les bonnes pratiques ainsi que les initiatives constructives. Il est également possible d'organiser des actions communes.

Par ailleurs, nous œuvrons dans un contexte interministériel, sous l'égide du Secrétariat général de la défense et de la sécurité nationale, avec l'Armée de l'air et nos partenaires américains et britanniques, à la prise en compte des vulnérabilités des aéroports en France et à l'étranger, face aux « Man-portable air-defense systems » (MANPADS). Nous sommes également engagés sur des missions d'évaluation d'aéroports étrangers ayant des liaisons directes avec le territoire national. Les déficiences éventuellement constatées peuvent alors donner lieu à des décisions interministérielles imposant des mesures de sûreté supplémentaires.

L'AUTEUR

Colonel de gendarmerie, Francis Formell commande la gendarmerie des transports aériens depuis le premier novembre 2016. Saint-Cyrien, après des débuts en gendarmerie mobile, il œuvre 11 ans comme pilote d'hélicoptère au sein des formations aériennes de la gendarmerie. Il servira ensuite en finances et ressources humaines au sein de la DGGN avant de commander pendant 3 ans le groupement de gendarmerie départementale de Seine-et-Marne. Il est breveté de l'école de guerre, possède un Executive MBA HEC et a été auditeur de l'INHESJ et de l'IHEE.

Les enjeux
de la sûreté aéroportuaire

par **EMMANUELLE SANSOT**

La sûreté aéroportuaire est le produit d'une combinaison de mesures ainsi que de moyens humains et matériels concourant à la protection de l'aviation civile contre les actes d'intervention illicite[1]. Ces actes recouvrent des scénarios multiples incluant non seulement l'aéronef et les passagers, mais également l'aéroport et les personnes au sol, ainsi que les installations aéronautiques.

(1) OACI (2011) Annexe 17 à la Convention relative à l'aviation civile internationale, 9e édition, (amendements 1-14), p. 1-3

EMMANUELLE SANSOT

Chef d'escadron, chef du Bureau Emploi Sûreté État-major de la gendarmerie des transports aériens

Face à une menace évolutive et polymorphe, il apparaît nécessaire d'adopter une démarche globale, tant sur le plan de l'analyse du risque que dans les réponses apportées par les autorités, afin de contrer un phénomène terroriste qui prend ses racines bien en amont de l'aéroport.

La distinction entre la sécurité et la sûreté aérienne

Symbole de liberté, vecteur du commerce international, le transport aérien a été rapidement marqué par des préoccupations sécuritaires afin de prévenir les accidents. Cela a entraîné la mise en place d'un ensemble de dispositions établies par l'Organisation de l'aviation civile internationale (OACI), institution spécialisée dépendant des Nations Unies, dans divers domaines (conception des aéronefs, infrastructures, contrôle aérien...).

Au fur et à mesure, la sécurité s'est retrouvée concurrencée par des considérations liées à la sûreté aéroportuaire, marquant ainsi la nette

Le risque terroriste oblige à durcir tous les processus de sûreté régulant les flux des passagers, du fret et des personnels travaillant sur les plateformes.

distinction entre ces deux termes [2]. L'aviation civile internationale a toujours constitué une cible privilégiée pour les groupes terroristes et la criminalité organisée. En effet, le nombre conséquent de victimes potentielles, l'impact médiatique et économique, ainsi que l'atteinte au symbole étatique représentent un attrait indéniable pour toute action malveillante. L'OACI a alors adopté un ensemble de normes et de recommandations réunies au sein de l'annexe 17 à la Convention relative à l'aviation civile internationale.

(2) Demettre, Lucie (2010) De sécurité en sûreté : où en est l'espace aéroportuaire ? http://cafe-geo.net/wp-content/uploads/securite-espace-aeroportuaire.pdf

L'évolution de la menace : de la piraterie aérienne au terrorisme international

Cette menace a évolué de façon incontestable au fil des décennies, modifiant profondément la notion d'acte d'intervention illicite[3].

(3) Dupont-Elleray, Michel (2005) Géopolitique du terrorisme aérien : de l'évolution de la menace à la diversité de la riposte, Stratégique 1/2005 (N° 85), pp. 109-122. https://www.cairn.info/revue-strategique-2005-1-page-109.htm

Les actes de piraterie aérienne classique, avec des détournements d'aéronefs et des prises d'otages spectaculaires, parfois tragiques, ont atteint leur paroxysme dans les années 70 et apparaissent alors comme le reflet des relations internationales. Ainsi, en septembre 1970 (« skyjack sunday »), des

terroristes du FPLP (Front Populaire pour la Libération de la Palestine) détournent quatre avions de ligne de la BOAC, Swissair, TWA et de la Pan Am afin d'obtenir la libération de prisonniers palestiniens. Une tentative similaire sur un cinquième vol de la compagnie El Al sera déjouée. Après avoir évacué les otages, les pirates de l'air font exploser trois de ces aéronefs devant la presse internationale.

En 1985, le détournement d'un avion de la TWA fut particulièrement marquant de par sa durée (17 jours, au cours desquels l'aéronef enchaîna des allers-retours entre Alger et Beyrouth). En parallèle, une nouvelle forme de menace apparaît dès les années 70. L'aéronef, pris pour cible, est détruit par des explosifs introduits à bord, occasionnant un nombre important de victimes. L'attentat du vol Pan Am 103, survenu en décembre 1988 au cours d'une liaison Londres-New York, reste emblématique. L'aéronef explose au-dessus du village de Lockerbie (Écosse), entraînant ainsi la mort de 270 personnes.

L'apparition de kamikazes fait évoluer la menace de façon dramatique et la sûreté aérienne devient indissociable de la notion de terrorisme. Les attentats du 11 septembre 2001 ont ainsi marqué un profond tournant dans la conception de la protection de l'aviation civile, en choquant durablement les esprits. En effet, l'aéronef est devenu une arme susceptible de causer la mort de milliers de victimes, à travers un acte soigneusement planifié. Face à l'apparition de cette nouvelle menace, la communauté internationale a intensifié les moyens humains et techniques consacrés à la protection de l'aviation civile.

Ainsi, les fondements de la sûreté aéroportuaire actuelle découlent des attentats du 11 septembre 2001, avec l'instauration de règles communautaires visant à protéger l'aviation civile contre les actes d'intervention illicite. Ces mesures de sûreté, harmonisées au niveau européen, se rapportent en particulier aux passagers, aux personnels, aux bagages, au fret et au courrier, à l'aéronef et aux installations aéroportuaires[4]. Elles ont profondément modifié le transport aérien, le milieu aéroportuaire devenant progressivement un espace ultra contrôlé.

(4) Thomas, Marc (2016) Transports aériens : sûreté de l'aviation civile. [en ligne] In : Fiches techniques sur l'Union européenne. http://www.europarl.europa.eu/ftu/pdf/fr/FTU_5.6.8.pdf

Le transport aérien face à des vulnérabilités multiples

Les attentats de septembre 2001 ont également révélé au grand jour la menace du djihadisme international, entraînant une lutte antiterroriste à grande échelle. Preuve de la capacité de ces réseaux à adapter leurs modes d'action, l'état de la menace évolue et impose de développer une forte capacité d'anticipation.

Des dispositions spécifiques ont ainsi été instaurées suite aux tentatives d'attentats déjouées utilisant des explosifs liquides

contre des vols assurant des liaisons transatlantiques en 2006. De même, après les tentatives d'octobre 2010, mettant en jeu des imprimantes piégées en provenance du Yémen et à destination des États-Unis, une législation spécifique au fret aérien provenant de pays tiers et à destination de l'Union européenne a été adoptée (législation ACC3 - *air cargo third country carrier*)[5].

(5) Site internet du Ministère de l'Environnement, de l'Énergie et de la Mer, Information relative à la législation européenne en matière de sûreté du fret des vols entrants. [en ligne] mis à jour le 21 janvier 2014. http://www.developpement-durable.gouv.fr/Information-relative-a-la.html

Au niveau international, des pays dits sensibles

Compte tenu de leur contexte géopolitique instable, certaines escales présentent un niveau de menace particulièrement élevé. Les pays engagés dans la lutte contre l'État islamique (EI) constituent une cible privilégiée. Ainsi, le 31 octobre 2015, le crash dans le Sinaï de l'Airbus A321 reliant la station balnéaire de Charm el-Cheikh (Égypte) à Saint-Pétersbourg (Russie), avec 224 personnes à bord, a immédiatement été revendiqué par Daech. L'hypothèse de l'attentat est reconnue officiellement par les autorités russes, qui évoquent le déclenchement d'une bombe artisanale pendant le vol[6]. Pour parer à la menace, la France s'est dotée en 2015 d'un arsenal juridique lui permettant de renforcer la sûreté des « vols entrants ». Ainsi, en cas de menace pour la sécurité nationale, elle peut imposer aux compagnies aériennes desservant le territoire national au départ d'aérodromes étrangers des mesures de sûreté supplémentaires concernant - entre autres - les passagers, les bagages, le fret, la fouille et la protection des aéronefs[7]. En cas de non-respect, des mesures restrictives d'exploitation peuvent notamment être imposées.

(6) Mandraud, Isabelle (2015) Crash dans le Sinaï : Poutine admet un attentat et promet de « punir » les responsables, http://www.lemonde.fr/international/article/2015/11/17/crash-dans-le-sinai-poutine-admet-la-piste-de-l-attentat-et-promet-de-punir-les-responsables_4811717_3210.html

(7) Décret n° 2015-383 du 3 avril 2015, Legifrance https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030439272&dateTexte=20160721

(8) Shapiro, Andrew J. (2012) Addressing the Challenge of MANPADS Proliferation. [en ligne] In : Stimson Center, Washington, DC, 2 février 2012. http://www.state.gov/t/pm/rls/rm/183097.htm

(9) Rapport final du Groupe d'experts sur la Libye créé par la résolution 1973 (2011) du Conseil de sécurité, 19 février 2014, p. 95. http://www.un.org/ga/search/view_doc.asp?symbol=S/2014/106&referer=http://foreignaffairsreview.co.uk/2015/10/manpads/&Lang=F

Les systèmes portatifs de défense antiaérienne ou MANPADS (*man-portable air defense systems*) représentent également une menace contre l'aviation civile. En particulier, sous Kadhafi, la Libye a acquis un stock de ces armes estimé à environ 20 000 unités. La chute du régime a engendré un risque majeur de prolifération non seulement pour la région mais également pour l'ensemble de la communauté internationale[8]. L'évaluation précise du volume d'armes ayant disparu reste indéterminée, un des principaux facteurs étant la difficulté à estimer ce stock au moment de l'effondrement du régime.Un rapport d'un groupe d'experts

de l'ONU en date du 19 février 2014 confirme ce transfert de MANPADS vers des groupes terroristes[9].

La menace pesant sur le « côté ville » des aéroports, reflet des modes opératoires actuels de Daech

Le « côté ville » constitue une cible privilégiée pour des groupes terroristes : accessibilité, nombre important de victimes potentielles, alliés à une symbolique internationale. Ainsi, deux attentats récents particulièrement meurtriers ont visé des terminaux de passagers. Le 22 mars 2016, des kamikazes ont provoqué une double explosion dans le hall des départs de l'aéroport de Bruxelles-Zaventem, en Belgique. Une heure plus tard, cet attentat-suicide a été suivi d'une troisième explosion dans la station de métro Maelbeek. Une trentaine de personnes sont décédées, et plus de 300 blessés sont recensés. Le 28 juin 2016, un nouvel attentat-suicide a frappé l'aéroport international Atatürk d'Istanbul, tuant au moins une quarantaine de personnes et faisant plus de 200 blessés. Trois assaillants ont mitraillé des passagers et des policiers en faction, avant d'actionner leurs explosifs.

Les déroulés de ces événements illustrent les modes opératoires actuellement développés par l'État islamique, avec une sélection prioritaire de cibles vulnérables susceptibles d'engendrer de nombreuses victimes. Les profils des terroristes sont caractérisés par une pleine acceptation de la mort et la volonté de mourir en héros. Si la stratégie générale reste définie au niveau central, les aspects tactiques semblent laissés à l'appréciation de leaders locaux afin d'adapter leur action, augmentant ainsi la difficulté à les détecter en amont. Pour autant, les scénarios d'actes d'individus isolés ne peuvent être écartés et constituent une réelle menace[10].

(10) Changes in modus operandi of Islamic State terrorist attacks, Review held by experts from Member States and Europol on 29 November and 1 December 2015 https://www.europol.europa.eu/sites/default/files/publications/changes_in_modus_operandi_of_is_in_terrorist_attacks.pdf

Le facteur humain … l'enjeu de la recherche du renseignement

Alors que les technologies se développent en permanence, l'humain se retrouve paradoxalement placé au cœur des dispositifs actuels de sûreté.

« La complicité interne » constitue une vulnérabilité particulièrement difficile à maîtriser pour le transport aérien, que ce soit par le biais d'individus radicalisés voire d'agents qui seraient victimes de menaces pesant sur leurs proches. Il est donc nécessaire que les personnels chargés de certaines missions de sûreté et/ou ayant accès à des secteurs sensibles (aéronef, bagages, fret…) fassent l'objet de vérifications d'antécédents de façon régulière afin de s'assurer que leur comportement est effectivement compatible avec les fonctions exercées.

Au niveau national, ces obligations sont notamment matérialisées par la nécessité de détenir une habilitation afin d'avoir accès, en particulier, aux zones de sûreté à accès réglementé des aérodromes ainsi qu'au fret sécurisé. Délivrée pour une durée maximale de trois ans, cette habilitation requiert la réalisation préalable d'une enquête administrative[11].

(11) Code des transports, article L6342-3, Legifrance [en ligne] version en vigueur au 3 mars 2012. https://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000023075738&cidTexte=LEGITEXT000023086525

Par ailleurs, les agents mettant en œuvre les opérations d'inspection filtrage des personnes, des objets qu'elles transportent, des bagages et des véhicules doivent avoir été préalablement agréés par le préfet et le procureur de la République, ce « double agrément » étant également précédé d'une enquête administrative[12].

(12) Code des transports, article L6342-4, Legifrance [en ligne]. https://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000025423812&cidTexte=LEGITEXT000023086525>

Mais les modes d'action actuels des terroristes visent à déjouer les services de renseignement et les phénomènes de radicalisation sont susceptibles d'être très rapides. Le rapport réalisé au nom de la commission d'enquête sur la surveillance des filières et des individus djihadistes, en date du 2 juin 2015, montre bien toute la complexité de ce phénomène, rendant fondamental le travail coordonné des services de renseignements.

Il y est ainsi précisé que « *plus de la moitié des personnes parties vers la zone irako-syrienne étaient inconnues des services* [13] » et qu'« *il est particulièrement difficile d'évaluer la dangerosité des djihadistes de retour sur notre territoire, notamment parce que certains peuvent avoir des stratégies de dissimulation*[14]» .

(13) Rapport fait au nom de la commission d'enquête sur la surveillance des filières et des individus djihadistes (n°2828), 2 juin 2015, pp. 23, 26 et 47. http://www.assemblee-nationale.fr/14/pdf/rap-enq/r2828.pdf

(14) CF. Note 13

(15) CF. Note 13

S'il apparaît complexe de déterminer un profil type de terroriste djihadiste, des indicateurs visibles de basculement sont généralement détectables avec « *un certain nombre d'indices liés à l'apparence, au comportement ou encore au discours des intéressés*[15] ».

La détection de ces signaux atypiques et leur traitement constituent un réel enjeu en termes de prévention du terrorisme face à cette menace protéiforme.

La douane, un acteur majeur de la sûreté aéroportuaire

Entretien avec XAVIER PASCUAL

réalisé par Philippe Durand, rédacteur en chef de la revue

La protection du territoire national et des citoyens constitue l'une des missions essentielles de l'administration des douanes et droits indirects. Dans le contexte de l'année 2016, la douane est par nature un acteur majeur de la sécurisation des flux de marchandises. En aéroport, la douane est souvent connue pour sa mission de contrôle des bagages à l'arrivée des voyageurs. Elle assure parallèlement la sécurisation du fret à l'exportation et plus généralement la sûreté des marchandises transportées par voie aérienne.

XAVIER PASCUAL

Directeur des services douaniers
Adjoint au directeur régional des douanes de Roissy Voyageurs

Deuxième force de l'État en termes d'effectifs implantés sur l'aéroport de Roissy Charles de Gaulle après la direction de la Police aux frontières, les 1300 douaniers de Roissy veillent 24h/24 et 7j/7 sur les marchandises qui arrivent ou quittent l'aéroport.

Quel est le rôle de la douane en matière de sûreté aérienne ?

Au cœur des flux commerciaux internationaux et de la régulation des échanges, l'administration des douanes joue un rôle essentiel en matière de sûreté aérienne, aux côtés des autres services de l'État.

Sur un aéroport international comme celui de Roissy Charles de Gaulle, les services de l'État mettent en œuvre les mesures de sûreté selon la clé de répartition suivante : la police aux frontières (PAF) supervise l'inspection des passagers et de leurs bagages « cabine », la Gendarmerie des transports aériens (GTA) celui des bagages de soute et la douane supervise quant à elle la sécurisation du fret à l'exportation.

La sécurisation du fret est complémentaire des mesures de sûreté appliquées aux passagers et à leurs bagages de soute.

Forte d'une expérience en matière de sûreté / sécurité dans le cadre du dispositif communautaire ICS[1], la douane échange quotidiennement avec les professionnels de la logistique (transitaires, handlers…) et connaît la typologie du fret transporté ce qui lui permet d'enrichir en permanence ses bases de données pour accroître son expertise. À l'instar de ce dispositif mis en œuvre à l'importation, la douane assure également la sûreté du fret à l'exportation afin de sécuriser toute marchandise montant à bord d'un aéronef. Sur un vol long-courrier, ce sont près de 30 tonnes de fret qui sont embarquées en soute sous les pieds des passagers. Il est donc fondamental que ce fret soit correctement sécurisé et que des contrôles de sécurisation soient effectués puisque la sûreté d'un aéronef recouvre tous les types de chargements. Il serait en effet inutile de mettre en place des procédures de sûreté strictes pour les passagers et leurs bagages si parallèlement le fret transporté dans le même avion n'était pas soumis à des procédures de sûreté tout aussi strictes. Sur les aéroports franciliens, les mesures de sûreté aérienne à l'exportation sont mises en œuvre au quotidien par des sociétés privées de sûreté sous la tutelle de l'administration des douanes. Sur la plate-forme de Roissy Charles de Gaulle, cela représente plus de 5 000 emplois. La douane assure ainsi la supervision et le contrôle de la mise en œuvre de ces mesures de sûreté.

(1) Dispositif Import Control System décliné sur le territoire communautaire depuis 2009.

Quels sont les enjeux en termes de sûreté sur un aéroport international ?

Roissy étant le premier aéroport de fret transporté en Europe et le 9e aéroport au niveau mondial, la sûreté du fret constitue une mission de premier ordre pour les douaniers de la circonscription. Avec 139 compagnies aériennes desservant 319 villes, l'aéroport Roissy Charles de Gaulle est connecté au monde entier et constitue ainsi la première frontière douanière de France.

Dans un souci de réduction des coûts de transport, les compagnies aériennes profitent des capacités de stockage importantes des avions passagers et des nombreuses opportunités de connexions proposées par le hub de Roissy pour transporter du fret. Ainsi, près de 60 % du fret aérien voyage actuellement dans les soutes des avions passagers. Par ailleurs, de par sa situation géographique, l'aéroport de Roissy Charles de Gaulle propose chaque semaine 20 800 opportunités de correspondance en moins

de 2h, situation de choix qui démultiplie les opportunités de chargement pour les logisticiens. Sur un aéroport international, les enjeux en termes de sûreté sont donc particulièrement élevés en raison de la volumétrie des échanges et de la multiplicité des pays d'origine et de destination.

La douane assure donc la sûreté du fret sur les flux import et export ?

Souvent dénommée « Police des marchandises », la douane est en charge du contrôle des marchandises et ce à plusieurs titres : d'un point de vue fiscal, avec la mission historique de perception des droits et taxes à l'importation mais aussi en référence avec la lutte contre les grands trafics avec les saisies de stupéfiants, cigarettes, espèces protégées, flux illicites de capitaux ou encore par la vérification de la conformité des marchandises aux normes nationales et européennes. La douane contrôle ainsi la circulation des marchandises à l'importation, à l'exportation et en transit.

En raison de la volumétrie des échanges mondiaux et du contexte international, la douane a ajouté une forte dimension sûreté-sécurité à son action de contrôle des marchandises. Depuis la mise en place du programme européen ICS évoqué ci-dessus, toutes les compagnies aériennes doivent transmettre à l'administration des douanes, quatre heures avant l'arrivée d'un vol long-courrier ou au plus tard au décollage de l'avion pour les vols courts-courriers, les informations concernant le fret transporté à bord des aéronefs. Sur la base de 27 données, la douane réalise alors une analyse de risque sûreté/sécurité des envois pour cibler, avant l'arrivée du vol, les marchandises potentiellement dangereuses qu'elle va contrôler de manière plus approfondie. La douane de Roissy héberge pour cela l'une des 3 cellules de « levée de doute » implantées sur le territoire national, avec les cellules du Havre et Marseille. La cellule de Roissy est chargée d'analyser la nature et le niveau de risque rattachés aux marchandises expédiées par voie aérienne sur le territoire de l'Union européenne lorsque la France est le premier point d'entrée dans l'UE. La douane de Roissy est par conséquent le

DES CONTRÔLES DE SÛRETÉ AUSSI SUR LES VOLS À L'ARRIVÉE

Depuis 2015, les autorités françaises peuvent imposer aux compagnies aériennes desservant la France au départ d'aéroports étrangers la réalisation de mesures de sûreté supplémentaires. Ces mesures sont déterminées au cas par cas, suite à une analyse de la menace.
De telles dispositions s'appliquent à ce jour aux vols au départ de la Tunisie, du Sénégal et du Mali dont les dispositifs de sécurisation du fret aérien au départ sont jugés insuffisants. Des inspections-filtrages supplémentaires sont réalisées au départ avec un contrôle à l'arrivée permettant de s'assurer de la bonne réalisation de ces mesures supplémentaires au travers d'un document de traçabilité. Une répartition des vols et des compagnies par administration a été effectuée. La douane contribue aux côtés de la GTA et de la PAF à la réalisation de cette mission.

Douanes

La douane joue ainsi un rôle central dans la sécurisation du fret aérien à l'importation en métropole et dans les DOM

point d'entrée national des « déclarations sommaires d'entrée » (ENS) pour tout le transport aérien français, soit plus de 6 millions d'ENS traités par an. Elle joue ainsi un rôle central dans la sécurisation du fret aérien à l'importation en métropole et dans les DOM.

Par ailleurs, les entreprises du monde aérien abordent déjà les questions de sûreté avec la douane, dans le cadre du label européen d'Opérateur économique agréé (OEA). Il s'agit d'une certification délivrée à l'issue d'un audit douanier des process internes à l'entreprise, qui comporte un volet douane et un volet sûreté-sécurité. Enfin, la douane assure la conduite en douane et la prise en charge des marchandises à l'importation, à l'exportation ou en transit. Concrètement, cela signifie que toutes marchandises circulant dans la zone sous douane, des soutes de l'avion aux magasins sous douane sont sous la surveillance générale de la douane. Il ne peut être procédé à l'ouverture des envois sans son accord préalable.

Concrètement, avez-vous des spécialistes de la sûreté ?

Oui, nous avons constitué à Roissy un « Pôle Sûreté » spécialement dédié à la sûreté du fret qui comprend une brigade de surveillance extérieure spécialisée (BSES) et une cellule administrative. Leur rôle est double : inspecter les entreprises qui demandent ou détiennent un agrément d'agent habilité et effectuer des contrôles inopinés auprès de tous les acteurs du fret.

Vos agents suivent-ils des formations spécifiques ?

Oui, tous nos agents ont acquis une double qualification auprès de l'école

nationale de l'aviation civile (ENAC) :

- « contrôleur fret » (SURAD), qui constitue la formation de base ;

- « inspecteur fret » (SURSIF), qui constitue la formation avancée au cours de laquelle la réglementation sur la sûreté du fret aérien est présentée de façon détaillée. Elle permet alors de réaliser des inspections d'agents habilités, de rédiger des rapports et de mener des contrôles qualités sur ces rapports.

Des formations continues sont également organisées régulièrement, environ deux fois par an, sur des points thématiques précis ou dans le but d'effectuer des retours d'expérience.

Par ailleurs, les cadres suivent la formation généraliste SURET qui donne une vision plus large et plus stratégique des enjeux de sûreté aérienne.

Pouvez-vous nous décrire schématiquement comment fonctionne la sûreté du fret aérien ?

Une compagnie aérienne ne peut charger à bord d'un avion que du fret qu'elle a sécurisé elle-même, ou qui lui a été remis par un « agent habilité » à sécuriser le fret qu'il traite. Le statut « d'agent habilité » est donc à la base de la sûreté du fret aérien. Il s'agit essentiellement de transitaires ou de gestionnaires de magasins sous douane. À Roissy, comme à Orly ou au Bourget, c'est la douane qui audite les entreprises qui souhaitent obtenir ce statut sachant que l'habilitation délivrée par la DGAC est valable 5 ans.

Que contiennent les rapports d'inspection ?

Les candidats au statut « d'agent habilité » élaborent un programme de sûreté. La DGAC vérifie qu'il est conforme aux textes en vigueur puis elle confie à la douane la mission d'inspection. Il s'agit pour la douane d'effectuer un audit de l'entreprise, pour vérifier si la pratique logistique est en adéquation avec le programme de sûreté.

L'inspection comporte l'examen de plusieurs points de contrôle, liés aux exigences réglementaires, à savoir :

- l'organisation interne et la définition des rôles et responsabilités de chacun ;

- les vérifications documentaires effectuées par l'entreprise lorsqu'elle réceptionne du fret ;

- les modalités d'inspection-filtrage ;

- le programme de formation des agents de sûreté ;

- les équipements de détection disponibles.

Les sous-traitants sont nombreux dans la chaîne logistique du fret en général et dans celle de la sécurisation en particulier. Cette multiplicité d'intervenants complique le travail de recherche et de traçabilité des opérations de sécurisation qui est essentielle pour déterminer les responsabilités de chacun. L'expertise de notre brigade spécialisée permet d'optimiser et de multiplier nos contrôles.

Les inspecteurs sûreté du fret rédigent un rapport d'inspection qui reprend les

thématiques évoquées ci-dessus point par point et attribue des niveaux de conformité sur une échelle de 1 à 4, allant de la conformité des mesures de sûreté avec la réglementation jusqu'à la constatation de graves déficiences avec un impact majeur sur la sûreté de l'aviation civile. Actuellement, la douane de Roissy a en portefeuille 72 agents habilités.

Effectuez-vous d'autres contrôles en dehors de ces inspections des agents habilités ?

Oui, la douane réalise quotidiennement des contrôles inopinés, portant sur tous les points de la réglementation sûreté. Des équipes de douaniers circulent dans les entrepôts de fret et se déplacent sur les pistes, jusqu'en pied d'avion. Elles vérifient que les marchandises qui vont être chargées à bord des avions ont bien été sécurisées et qu'elles l'ont été selon les bonnes techniques.

Elles s'assurent de la conformité entre la nature de l'expédition et le moyen d'inspection-filtrage mis en œuvre. Ainsi par exemple, le fret opaque ne peut être inspecté par rayon X, il nécessite le recours à une autre technique, telle que l'odorologie canine. Elles vérifient enfin que les personnels en charge de la sécurisation sont à jour de leurs formations et habilitations, y compris des TCA. Dans certains cas, des vérifications plus poussées sont effectuées, notamment pour le fret considéré « à haut risque ». Sont considérés comme « à haut risque » le fret endommagé, partiellement altéré ou le fret en provenance de certains pays présentant un risque élevé en matière de sûreté.

Au final, ce sont plusieurs milliers de contrôles inopinés qui sont menés chaque année et qui contribuent à une surveillance générale et quotidienne de l'activité des sociétés privées de sûreté.

En cas de découverte d'anomalies, un procès-verbal de constat de manquement aux règles de la sûreté aérienne est dressé et transmis à l'autorité préfectorale pour les suites requises. Le procès-verbal est alors présenté en commission de sûreté, en présence de l'opérateur. Cette commission est présidée par la DGAC et comporte des représentants de la GTA, de la PAF et de la douane. Si la commission confirme le manquement, elle propose une sanction au préfet délégué à la sécurité et à la sûreté de l'aéroport, qui statue en dernier ressort. Les sanctions maximales sont de 750 euros pour une personne physique et 7 500 euros pour une personne morale.

L'AUTEUR

Diplômé de l'Institut d'études politiques de Bordeaux, Xavier Pascual a intégré l'administration des douanes et droits indirects en 1998. Il a occupé des fonctions au niveau central et déconcentré.
Il est actuellement chef du pôle d'orientation des contrôles à la direction régionale Roissy Voyageurs et notamment chargé du pilotage du Pôle Sûreté.

La multi-biométrie : l'avenir du contrôle aux frontières

par LUC TOMBAL

Le secteur du contrôle aux frontières bénéficie aujourd'hui de nouvelles technologies biométriques qui ont connu des évolutions remarquables. Des systèmes « à la volée » et non intrusifs modifient la perception que les voyageurs ont de la biométrie.

Le déploiement de ces technologies a déjà commencé dans des aéroports ultramodernes, comme ceux des Émirats arabes unis. Il s'agit d'une première étape menant vers une sécurité frontalière à 360° qui se caractérise par une interconnexion entre toutes les frontières aériennes, maritimes et terrestres. Autrefois futuriste, le concept de « e-Border » (frontière électronique), ou encore de frontière intelligente, devient aujourd'hui une réalité qui apporte de nombreux avantages à toutes les parties prenantes.

LUC TOMBAL

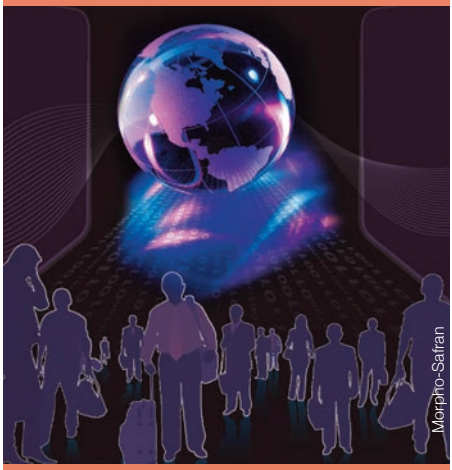
Directeur Stratégie et Développement de Marché,
Division Sécurité
Safran Identity & Security

Coup d'œil sur les frontières de demain

Dans les aéroports de demain, les passagers ne verront pas les installations de sécurité. Les points de contrôle aux frontières terrestres seront directement connectés aux ports et aéroports. Les instances gouvernementales sauront précisément qui a pénétré sur leur territoire national. Quant aux garde-frontières, ils travailleront en toute confiance. Les voyageurs ne seront plus stressés par la lourdeur des contrôles. Cet aperçu des frontières de demain n'est pas une vision utopique. Des éléments essentiels sont prêts et n'attendent plus que d'être assemblés pour le bénéfice de tous.

Biométrie « à la volée » : la révolution des contrôles frontaliers

L'image de la biométrie est en pleine évolution, surtout en ce qui concerne les



Les dernières technologies à distance disponibles pour la capture d'empreintes digitales (MorphoWave) et la capture d'iris (Iris At a Distance) permettent aux autorités de sécuriser l'espace aéroportuaire.

empreintes digitales. Autrefois, les autorités policières relevaient uniquement les empreintes digitales des individus considérés comme suspects, et pour le public, il s'agissait d'un moyen d'investigation policière. La toute première technique de saisie d'empreintes digitales, qui consistait à prendre les empreintes dactylaires d'un individu par la pression sur une feuille de papier de doigts préalablement trempés dans l'encre, était particulièrement invasive. Même si cette technique a été peu à peu remplacée par des capteurs optiques avec contact entre la main et le dispositif, le processus garde une connotation négative aux yeux de l'opinion publique. Malgré tout, les autorités du monde entier ont vite compris les avantages que la biométrie pouvait apporter aux contrôles frontaliers (la quasi-certitude sur l'identité permet d'authentifier des individus qui entrent dans un pays) et ont commencé à prélever les données biométriques des voyageurs. Des systèmes ont tout d'abord été déployés dans des aéroports où l'infrastructure informatique existait déjà. Toutefois, le processus est long et les contacts physiques liés à la saisie des empreintes digitales soulèvent encore des questions d'ordre hygiénique ou culturel.

L'émergence de technologies sans contact avant-gardistes rend la biométrie très intéressante pour le contrôle aux frontières : en offrant de bien meilleures conditions aux utilisateurs, les nouveaux systèmes permettent aux autorités frontalières de relever les données biométriques de chaque personne rapidement et sans occasionner de gêne. Par exemple, la solution « Iris At a Distance » (IAD), combinant la capture d'iris et celle du visage, peut relever les empreintes d'iris à une distance d'un mètre en une seconde. MorphoWave™ est un autre exemple. Cette solution de contrôle d'accès biométrique capture et identifie quatre empreintes digitales en un seul passage de la main. Elle applique une technologie brevetée véritablement sans contact qui non seulement acquiert avec une très grande précision les données dactyloscopiques, mais surmonte également les problèmes qui touchent les systèmes classiques avec contact (humidité ou sécheresse des doigts et empreintes résiduelles). Grâce à ces

systèmes, les voyageurs acceptent plus volontiers les contrôles de sécurité qui peuvent être incorporés dans les aéroports pour faciliter le processus d'identification des passagers. La rapidité du système représente un autre avantage clé, les points de contrôle frontaliers étant très souvent encombrés et les douaniers étant soumis à de fortes contraintes de temps.

La multi-biométrie est la clé de voûte de ces dispositifs

En matière de sécurité, il s'agit d'identifier avec certitude la personne qui franchit la frontière et de déterminer très rapidement si elle est y est autorisée. Un humain sans assistance technologique ne peut maintenir à lui seul ce degré de certitude et de rapidité d'identification. Les autorités frontalières doivent être équipées d'outils appropriés pour pouvoir anticiper et se concentrer sur l'identification de comportements suspects qui déclencheront des recherches plus poussées.

Seule la biométrie est véritablement efficace ici car chaque individu possède ses propres caractéristiques physiques. La multi-biométrie offre des résultats encore meilleurs car la combinaison du traitement du visage (un passeport comporte toujours la photo du visage de son détenteur), des empreintes digitales et des iris offre une précision quasi parfaite.

Le cas des Émirats arabes unis

Récemment, les Émirats arabes unis ont lancé un ambitieux projet de gestion des frontières par multi-biométrie. Le système « e-Border » est la suite logique du projet pilote qui a été conduit par Safran Identity & Security dans l'aéroport international d'Abu Dhabi en 2012.

Il répond aux besoins des Émirats arabes unis en matière de contrôle frontalier. Situé au carrefour de l'Asie et de l'Europe, le pays attire de nombreuses personnes en provenance des nations voisines. Les immigrants représentent 85% de la population. La sécurisation des frontières, et donc du territoire national, est ainsi une question vitale. Aujourd'hui, les Émirats arabes unis utilisent principalement la biométrie de reconnaissance d'iris pour identifier leurs citoyens. Ce système est très pratique, car aux Émirats arabes unis de nombreuses femmes ont le visage voilé. Le pays possède aussi un système

d'identification automatique d'empreintes digitales (AFIS, *Automated Fingerprints Identification System*) et un système de reconnaissance faciale.

Le nouveau système, qui utilise les trois types de données biométriques, est l'un des plus précis au monde. Installé dans cinq grands aéroports des Émirats arabes unis, il gère les arrivées et les départs de tous les voyageurs. À terme, il intégrera 96 *e-Gates* (portes automatiques de passage des frontières) et 94 *e-Counters* (comptoirs électroniques d'immigration). Le système multi-biométrique des Émirats arabes unis est un programme unique, pour plusieurs raisons. Il combine plusieurs solutions biométriques, il est le premier projet à intégrer une nouvelle technologie « à la volée » pour les iris et les empreintes digitales, et il est l'un des premiers systèmes du genre au monde à être utilisé pour les entrées comme pour les sorties.

Vers une intégration des frontières aériennes, maritimes et terrestres

L'histoire ne s'arrête pas là. En réalité, elle ne fait que commencer et prouve que la multi-biométrie est la solution idéale pour une gestion efficace des frontières. Son utilisation initiale dans des aéroports est totalement logique : la plupart des aéroports, au moins internationaux, sont en effet équipés de l'infrastructure informatique adéquate. Le déploiement ne doit pas s'arrêter aux aéroports qui ne constituent qu'un des composants d'un système de contrôle aux frontières. Nous pouvons considérer les aéroports comme des plates-formes d'essai direct pour un système plus large qui intégrerait également les points de contrôle aux frontières terrestres et maritimes.

Des avantages pour toutes les parties prenantes

La future gestion des frontières par multi-biométrie apporte des avantages à toutes les parties prenantes : les gouvernements, soucieux d'assurer la sécurité du territoire national ; les autorités en charge de l'immigration, qui gèrent les contrôles à des frontières de plus en plus fréquentées ; les opérateurs de transport, toujours en quête de nouveaux clients ; ou tout simplement les voyageurs, qui veulent rejoindre leur destination sans souci.

L'AUTEUR

Luc Tombal est ingénieur en informatique et en mathématiques appliquées. Il commence sa carrière professionnelle dans les services du Premier ministre français, où il met en œuvre des systèmes informatiques dans le domaine du renseignement. Il rejoint ensuite Safran Identity & Security (I&S), leader mondial dans le domaine des solutions biométriques. Durant 15 ans, Il y occupe diverses fonctions dans la mise en œuvre de systèmes de sécurité : architecture, développements de produit, intégration, et déploiement. En 2011, il prend en charge au niveau mondial les activités d'avant-vente de la société pour la fourniture de solutions gouvernementales. En janvier 2014, il est nommé directeur de la « Business Unit Contrôle des frontières / Transport / Infrastructures critiques » de la division Sécurité de Safran I&S. Depuis le 1er septembre 2015, il occupe les fonctions de directeur Stratégie et Développement des Marchés de la division Sécurité.

La formation, un contributeur important de la sûreté aéroportuaire

par **CHARLOTTE BRUNET-RICCHI**

Le gestionnaire d'aéroport détermine un programme de sûreté qui est décliné par les opérateurs. Ces derniers profitent de l'expérience et des services de centres de formation de sociétés privées qui assurent, au profit des personnels, des processus pédagogiques spécifiques pour permettre une mise en œuvre cohérente de ces directives. Liens très étroits avec les sociétés opératrices de sûreté, veille réglementaire, formations certifiées et en adéquation avec les règles des métiers sont les ingrédients d'une reconnaissance par les pouvoirs publics et les opérateurs des zones aéroportuaires. Cette aptitude sera abordée par un balayage du contexte réglementaire puis par un aperçu des formations dispensées.

CHARLOTTE BRUNET-RICCHI

Directrice du centre de formation HUB SAFE

Un lien étroit avec les sociétés de sûreté

Pour pouvoir répondre à la réalité opérationnelle du terrain, il est nécessaire d'entretenir des liens très étroits avec les sociétés opératrices de sûreté dans les aéroports. Pour un centre de formation, il s'agit non seulement d'assurer une veille réglementaire rigoureuse en termes de formation, tâche facilitée par l'implication de l'ENAC[1] et son système de diffusion de l'information auprès des instructeurs, mais aussi d'appliquer au niveau local la réglementation nationale.

(1) ENAC : École Nationale de l'Aviation Civile

C'est sur ce dernier point que les échanges avec les sociétés de sûreté sont indispensables. En effet, le gestionnaire d'aéroport décline la réglementation nationale dans son

Une formation exigeante et sélective à la mesure des enjeux de sûreté.

programme de sûreté reprise dans les consignes d'exploitation de la société de sûreté. L'accès du centre de formation à ces consignes ainsi qu'aux résultats des « contrôles qualité » effectués en interne permet d'une part aux instructeurs d'être en parfaite cohérence avec les pratiques du terrain, et d'autre part de pouvoir être pédagogiquement plus efficaces. C'est pourquoi nombre de sociétés opératrices de sûreté possèdent leur propre centre de formation.

La sûreté n'est pas réservée aux professionnels

En dehors des agents de sûreté aéroportuaire, toutes les personnes exerçant leur activité côté piste (en ZSAR[2] ou PCZSAR[3]) sont formées à la sûreté. Une formation est commune à tous et permet de faire une demande de Titre de circulation aéroportuaire. Par ailleurs, des formations spécifiques sont obligatoires pour les personnels d'assistance en escale et des compagnies aériennes, pour les personnes qui effectuent des fouilles de sûreté d'aéronefs ou mettent en œuvre leur protection, mais également pour celles qui effectuent la concordance entre passagers et bagages, des contrôles sur les approvisionnements de bords, le fret, le courrier,… La sûreté est donc l'affaire de tous.

(2) ZSAR : Zone de Sûreté à Accès Réglementé

(3) PCZAR : Partie Critique Zone de Sûreté à Accès Réglementé

Par qui les agents de sûreté sont-ils formés ?

Il est bien entendu nécessaire que l'organisme de formation soit déclaré à la DIRECCTE[4] et enregistré comme dispensateur de formation. Il doit également remplir les obligations légales émanant du ministère de tutelle des organismes de formation, à savoir le ministère du Travail. Entre autres, il faut effectuer un bilan pédagogique et financier annuel et bien entendu respecter le cadre légal de la formation professionnelle continue.

(4) Les directions régionales des entreprises, de la concurrence, de la consommation, du travail et de l'emploi (DIRECCTE ou DIECCTE dans les régions et départements d'outre-mer) sont des services déconcentrés de l'Etat. Dans chaque région (hors Outre-mer français qui fait l'objet de dispositions juridiques spécifiques), elles ont remplacé, entre 2009 et 2011, huit services dont notamment les directions régionales et départementales du travail, de l'emploi et de la formation professionnelle.

(5) CNAPS : Conseil National des Activités privées de sécurité

À partir du 1er juillet 2017, les organismes dispensant des formations de sûreté aéroportuaire devront être certifiés par le CNAPS[5] (Arrêté du 1er juillet 2016 relatif à la certification des organismes de

formation aux activités privées de sécurité et aux activités de recherches privées). Cette certification vise pour les autorités à s'assurer que les compétences nécessaires à la transmission des savoirs dans le domaine sont présentes dans l'organisme, de même que les outils et méthodes de traçabilité.

Dans une certaine mesure, la question des compétences est déjà validée par l'ENAC et la DGAC[6], puisque les instructeurs sûreté de l'aviation civile sont certifiés par la DGAC depuis janvier 2013.

(6) DGAC : Direction Générale de l'Aviation Civile

Par ailleurs, l'ENAC édite des modules de formation pour toutes les formations sûreté. Ces modules sont mis à jour régulièrement par l'ENAC en fonction des modifications de la réglementation. Les centres de formation sont quant à eux tenus de s'assurer que les modules mis à jour sont bien diffusés durant les sessions d'apprentissage. En outre, chaque organisme peut développer son propre support de formation qui doit au préalable être approuvé par la DGAC avant diffusion en session.

Quelles formations pour les agents de sûreté aéroportuaire ?

La formation des agents de sûreté se compose de quatre volets.

La formation initiale.

Celle-ci permet aux agents d'acquérir les compétences et les savoirs nécessaires pour assurer les missions d'agent de sûreté aéroportuaire. Cette formation est composée d'une partie sécurité, commune à la formation des agents de prévention et de sécurité et d'une partie sûreté aéroportuaire.

La première d'une durée de 41 heures est sanctionnée par un examen établi par l'ADEF en lien avec la CPNEFP Sécurité. Il s'agit de connaître l'environnement juridique de la sécurité privée, de maîtriser la gestion des risques et des situations conflictuelles, ainsi que la transmission des consignes et des informations.

La seconde partie est propre à la sûreté aéroportuaire. Sa durée est variable en fonction de la typologie d'emploi de l'agent, c'est-à-dire selon les missions de sûreté qu'il effectue. Cette partie de la formation, la plus importante en termes de volume, se compose de théorie, de pratique des équipements de sûreté ainsi que de formation imagerie. Il s'agit pour ce dernier point de maîtriser la lecture des images radioscopiques *via* un simulateur d'imagerie.

HUBSAFE TRAINING

Basée sur les plateformes aéroportuaires de Paris-Charles de Gaulle et Orly Sud, HUB SAFE Training est spécialisée dans les formations de sûreté et de sécurité à destination des professionnels du secteur aéroportuaire. Dispensées par des instructeurs formés par l'ENAC et certifiés par la DGAC, ces formations sont certifiantes, en parfaite conformité avec le cadre réglementaire.

Un agent de sûreté aéroportuaire peut effectuer des opérations de sûreté sur des passagers et leur bagage cabine, des bagages de soute, des véhicules, mais aussi du fret, des fournitures d'aéroport et des approvisionnements de bord. La combinaison d'une ou plusieurs de ces missions détermine la typologie de l'agent de sûreté.

La durée de la formation initiale est déterminée par cette typologie et peut aller jusqu'à 136 heures. La formation est sanctionnée par un examen organisé et contrôlé par l'ENAC sous la tutelle de la DGAC. Depuis le 1er juillet 2016, un nouveau barème a été mis en place nécessitant d'obtenir une note minimale de 10/20 à chacune des épreuves.

La certification des agents a une durée de validité de 5 ans. Celle-ci est réduite à 3 ans quand ils pratiquent les équipements d'imagerie. Au terme, les personnels doivent être à nouveau certifiés et donc représenter toutes les épreuves de l'examen.

La formation sur le tas

Cette modalité de formation est assurée par les sociétés de sûreté elles-mêmes. Il s'agit d'une mise en pratique de l'utilisation des équipements des postes d'inspection / filtrage et d'un apprentissage des procédures locales. Cette mise en pratique fait l'objet d'un compte rendu qui est porté au livret de formation de chaque agent. La périodicité est semestrielle.

L'évolution rapide des mesures de sûreté implique une mise à jour des informations données aux agents et la certitude qu'elles aient été comprises pour une application opérationnelle intelligente.

La formation adaptée et ENII

Lors de leur vacation au poste de lecture rayon X, les agents sont testés par le gestionnaire d'aéroport, et ce depuis 2015. Les manquements des agents en termes de détection de menaces font l'objet d'un état. Selon leurs faiblesses, les agents doivent suivre une formation adaptée suivie d'une ENII (Épreuve Normalisée d'Interprétation d'Images) pour laquelle ils doivent obtenir au minimum 75% de réussite. En cas d'échec répété quatre fois, l'agent est interdit d'écran et devra suivre à nouveau une formation initiale. Un simulateur est utilisé pour former les agents de sûreté à la lecture des images radioscopiques et au traitement de celles-ci. Chaque agent dispose d'un code d'accès, qui lui permet, après maîtrise des bases théoriques de la lecture et du traitement

des images, de pouvoir s'entraîner à la détection de menaces sur divers types de bagages en fonction de la typologie de l'agent : bagages cabine, bagages de soute, fret, fournitures d'aéroport et approvisionnements de bord.

Le niveau des exercices va croissant en fonction de la réussite de l'agent. Celui-ci peut, au fur et à mesure de son apprentissage, constater ses progrès mais aussi ses difficultés. En fonction de ces dernières, l'instructeur a la possibilité de programmer des exercices permettant à l'agent de travailler précisément sur ses faiblesses.

La formation périodique

Une fois certifiés, les agents de sûreté vont participer tout au long de leur carrière, une fois par semestre, à des formations périodiques. 7 à 12 heures de formation théorique et pratique, ainsi que 6 à 9 heures de formation imagerie seront dispensées. La durée correspond à la typologie au sein de laquelle l'agent exerce ses fonctions. Pour ce qui est de l'imagerie, elle varie selon le type de matériel utilisé.

L'objectif de ces formations périodiques est double. Il s'agit d'une part de rappeler les réglementations européennes et nationales et leur mise en pratique, et d'autre part de transmettre les nouvelles mesures de sûreté. Quand une disposition est nouvelle ou modifiée, les sociétés qui emploient les agents de sûreté transmettent ces informations en temps réel à leurs salariés, via les briefings de prise de service et les cahiers de consignes qui nécessitent une mise à jour constante. La formation arrive en soutien de cette démarche. Son objectif étant plus pédagogique qu'opérationnel, c'est l'occasion pour les agents de poser des questions et de comprendre les mesures et leur mise en œuvre.

Quid des équipes cynotechniques?

La formation initiale pour devenir conducteur de chien est comprise entre 280 heures et 560 heures. Ce nombre d'heures dépend comme pour les agents de sûreté des missions effectuées. Jusqu'en 2016, les équipes cynotechniques (un conducteur de chien et son chien) devaient uniquement obtenir une certification par le STAC[7] dans le domaine d'emploi sur lequel elles opéraient et se faire recertifier tous les ans. À présent, en plus de la formation initiale cynotechnique, le conducteur de chien doit obtenir la certification d'agent de sûreté dans la typologie dans laquelle il exerce.

(7) Service Technique de l'Aviation Civile.

Quels sont les enjeux actuels et à venir pour les centres de formation spécialisés dans la sûreté aéroportuaire ?

La formation sûreté est importante en volume et en fréquence pour les agents effectuant des opérations de sûreté mais aussi pour les instructeurs en sûreté. Pour la formation initiale des futurs agents, le défi, compte tenu du fait que la formation

Une double formation qui permet une parfaite adéquation à l'emploi.

est très dense, est de donner toutes les connaissances et les outils pour la réussite des stagiaires à l'examen du CQP ASA, mais surtout d'avoir le recul et la pratique nécessaires pour devenir un bon agent de sûreté. Il est évident que l'implication de la société opératrice de sûreté dans l'intégration et la prise de poste du nouvel agent est indispensable.

À présent, pour les agents déjà en poste qui sont formés tous les semestres, il est nécessaire de maintenir leur attention sur les menaces potentielles et sur l'évolution de celles-ci. Cela passe par la connaissance du terrain mais aussi des mesures locales par les instructeurs, ou encore par l'utilisation en formation des nouvelles menaces détectées… Il est à noter que les formations périodiques ou les recyclages sont sanctionnés par un test, et qu'en cas d'échec l'agent ne peut plus effectuer de mesures de sûreté sauf une nouvelle formation et la réussite de tests d'évaluation.

Les centres eux-mêmes sont très encadrés, par la DIRECCTE, la DGAC pour l'approbation des cours et des protocoles de formation imagerie et par la CPNEFP[8] s'agit à la fois d'être très rigoureux à l'égard de la réglementation et en même temps d'être novateur en termes pédagogiques. Le e-learning, les mises en situation réelles, la pratique, sont autant de modalités utilisées.

(8) CNPEFP : Commission Paritaire Nationale de l'Emploi et de la Formation Professionnelle.

L'organisme de formation doit donc être en mesure d'être réactif face au changement de réglementation et d'anticiper les changements à venir en termes de sûreté. Il paraît probable par exemple que la formation à l'analyse comportementale devienne incontournable, comme l'est depuis peu la relation de service au sein des aéroports qui devient un enjeu important pour les gestionnaires.

L'AUTEUR

Ancienne élève des Universités de Paris-Sorbonne et de Rouen, Charlotte BRUNET-RICCHI est titulaire d'un Master 2 en Ingénierie et Conseils et formation.
Elle a d'abord été formatrice, puis responsable pédagogique avant de devenir directrice d'un établissement de formation supérieure durant quatre ans. En septembre 2014, elle a pris la direction du centre de formation HUB SAFE Training inauguré au mois de janvier 2015.

Sûreté aéroportuaire
et gestion des flux

par MOURAD DAHMANI

La sûreté aéroportuaire mobilise des technicités diverses liées à la maîtrise de flux dynamiques : les passagers et les personnels des services, les bagages, le fret, les véhicules privés et de service, l'avitaillement et les aéronefs participent à un cycle d'activité continue d'une grande hétérogénéité fonctionnelle. La détermination nette des domaines de sûreté, une délimitation des cheminements et accès, un encadrement juridique précis des processus mis en œuvre et une formation sans faille des personnels sont les postulats d'une sûreté maîtrisée par les agents régaliens et les opérateurs privés qui déploient leurs compétences sur des surfaces stratégiques.

MOURAD DAHMANI
Adjoint au Chef de Secteur
Connecting Bag Services
Worldwide Flights Services

La sûreté est la mobilisation d'un ensemble d'outils matériels et humains ayant pour objectif d'assurer la protection des biens et des personnes de l'aviation civile contre les actes de malveillance. Il faut la distinguer de la sécurité qui veille à protéger des accidents pouvant survenir lors des activités professionnelles déployées sur les sites aéroportuaires dans une classique gestion du risque.

Différents textes, à l'échelle internationale, nationale et locale encadrent la notion de sûreté :

Au niveau international, la convention relative à l'aviation civile internationale, dans son annexe 17[1] et son manuel associé, établit les normes et pratiques recommandées pour la protection de l'aviation civile internationale. Les gouvernements

(1) Organisation de l'aviation civile internationale. Annexe 17 accessible par le lien suivant : http://www.icao.int/safety/AirNavigation/NationalityMarks/annexes_booklet_fr.pdf

La large palette des métiers de l'aéroport nécessite des processus de sûreté adaptés et appliqués par des personnels formés selon des processus certifiés.

tiennent compte de la législation internationale, évaluent les mesures impactées au niveau national et prennent les décisions adéquates. Au niveau local, seul le comité local de sûreté est concerné. Présidé par le directeur d'aérodrome, il participe à une mise en œuvre tactique des mesures et il donne un avis au préfet sur les mesures prises ou préconisées. Toutefois, un grand nombre d'acteurs, aux statuts et aux prérogatives diverses, se partagent le champ de la sûreté aéroportuaire.

Des acteurs aux missions complémentaires

La sûreté est mise en œuvre, sur le terrain, par différents acteurs : Les services de l'état, l'aéroport de Paris et des sociétés privées de surveillance et de contrôle.

Les services de l'État comprennent essentiellement la DGAC (Direction générale de l'aviation civile) qui au niveau logistique assure le financement d'une partie des équipements. La PAF (police aux frontières) est chargée de la sûreté côté « Ville », notamment de l'inspection-filtrage des passagers (PIFP). La GTA (gendarmerie des transports aériens) assure ses missions côté piste, notamment le contrôle des personnes au fret et aux bagages en soute. Dans le cadre de leur mission de protection, les services douaniers contrôlent la mise en œuvre effective, par les agents habilités et les transporteurs aériens, des mesures de sûreté relatives au fret sur les plates-formes de PARIS CDG, d'ORLY et du BOURGET. Ils participent sur ces plates-formes aux actions de surveillance normalisée, coordonnées par la DSAC,

des entreprises relevant de leur compétence (inspections d'agents habilités. La douane s'occupe également de la gestion des titres d'accès des compagnies aériennes et des prestataires associés dont WFS fait partie. Chacune des sociétés intervenant dispose d'un correspondant sûreté. Ce dernier gère les demandes et les renouvellements de titre d'accès, la bonne application des consignes de sûreté imposées dans le cahier des charges de la compagnie aérienne et fait remonter tout dysfonctionnement. Il est donc chargé de suivre les actions correctives liées à ce dysfonctionnement.

Les sociétés de contrôle et de surveillance réalisent les contrôles des passagers ainsi que de leurs bagages cabine sur les postes d'inspection-filtrage (PIF) de manière très méthodique en se basant sur l'expérience des traitants et des matériels de détection sophistiqués.

Comment se finance la sûreté des aéroports ?

En 1986, une taxe sûreté provisoire a été mise en place. L'article 136 de la loi de finances pour 1999 (n° 98-1266 du 30/12/1998) a institué, à compter du 1er juillet 1999, une taxe dénommée « taxe d'aéroport ». Elle est due par toute entreprise de transport aérien public, quelle que soit sa nationalité ou son statut juridique, à raison des passagers et de la masse de fret et de courrier embarqués sur les aérodromes dont la liste est définie par arrêté ministériel. Perçue par l'État, le produit de la taxe d'aéroport est affecté sur chaque aérodrome ou groupement d'aérodromes au financement des services de sécurité (incendie - sauvetage, de lutte contre le péril animalier), de sûreté et des mesures effectuées dans le cadre des contrôles environnementaux. Il contribue aussi, dans une proportion fixée annuellement par arrêté, au financement des matériels de contrôle par identification biométrique installés dans les aéroports. L'arrêté interministériel du 10 mars 2016 (publié au Journal Officiel du 13 mars 2016) fixe la liste et le tarif des aérodromes et groupements d'aérodromes éligibles à la taxe d'aéroport.

Comment la sûreté est-elle mise en œuvre ?

La mise en œuvre de la sûreté se décompose selon deux principes complémentaires : prévention et correction.

Fondé en 1971, WFS (Worldwide Flight Services) est l'un des leaders mondiaux en service aéroportuaire. La société s'est spécialisée dans la manutention du fret aérien et les services au sol (avions, passagers, bagages). WFS opère auprès de 300 compagnies aériennes dans le monde et prend en charge 4 millions de tonnes de marchandises et 50 millions de passagers par an. Présente dans près de 145 sites répartis sur 23 pays, WFS occupe aujourd'hui une place dominante en France (avec une activité dans plus de 10 aéroports) et compte 14 000 collaborateurs dans le monde.

La sûreté préventive

Elle consiste à empêcher l'introduction d'éléments prohibés tels que les armes (à feu, blanches), les explosifs ou tout autre engin dangereux. Les contrôles sont réalisés par le filtrage des passagers, de leur bagage à main ainsi que par le contrôle des bagages en soute.

Le contrôle du FRET, du courrier et de l'avitaillement est également assuré. Côté piste, la GTA effectue des contrôles aléatoires et continus de sûreté.

En outre, sur les destinations sensibles, des contrôles supplémentaires sur piste sont réalisés par un contrôle approfondi des badges et des personnels. On note, par exemple, la présence de la GTA au pied de l'avion pour les vols d'ELAL à destination de Tel-Aviv. Les containers des vols Delta Airlines vers les États-Unis sont plombés.

La circulation des passagers entrants et sortants doit être totalement maîtrisée. En effet, la séparation des flux est un élément important du dispositif pour éviter que des objets prohibés soient transmis en zone réservée entre passagers entrants et sortants. Les passagers en transit sont contrôlés avant leur accès à la zone réservée. Le traitement des colis abandonnés fera l'objet d'une procédure de destruction par les services de déminage.

La sûreté curative

Les mesures curatives ont pour finalité la sauvegarde de la vie des passagers et du personnel aéroportuaire. L'intégrité des infrastructures et matériels est également concernée. Ces dispositions prennent en compte la gestion des menaces, des regroupements de personnes (manifestations), des actes illicites et un plan d'intervention contre les commandos. Des équipes cynotechniques renforcent ces contrôles grâce aux chiens renifleurs pouvant détecter les produits explosifs.

Le contrôle d'accès est différencié selon les catégories de personnels pris en compte et leur zone spatiale d'évolution. La zone de sûreté à accès réglementée (ZSAR) est uniquement accessible aux personnes munies d'un titre d'accès (badges pour les personnels, titre de transport pour les passagers). On y retrouve des espaces tels que les salles d'embarquement, les passerelles, les pistes et zones de circulation de l'aéroport, les zones de tri des bagages au départ, les salles de livraison bagages le cas échéant ainsi que des espaces dits de sûreté. L'accès en zone « côté piste » n'est autorisé qu'en possession d'un titre d'accès aéroportuaire valide. Les personnels permanents disposent d'un titre de couleur rouge, la verte étant réservée aux accompagnants. Les zones d'accès sont décomposées en quatre

secteurs sûreté : A – Avion, P – Passager, B – Bagages et F : Fret. Ces zones sont délimitées et surveillées. Les passagers accèdent à leur zone grâce à leur carte d'embarquement.

Comment les bagages en soute sont-ils traités ?

Suite aux attentats du 11 septembre 2001, 100 % des bagages sont sécurisés. Cela signifie qu'ils suivent un cheminement via les contrôles aux rayons X. S'ils révèlent une anomalie ou un doute, les bagages en question sont acheminés vers un autre type de contrôle plus puissant appelé le tomographe. Un opérateur valide le contenu du bagage. Si les doutes persistent, les procédures de reconnaissance bagages et destruction bagage suspect sont déclenchées.

En cas d'absence d'anomalie, ce bagage arrive sur le tapis « bagages ». L'intervention de WFS, *via* ses bagagistes formés et sensibilisés, consiste à procéder au scan des étiquettes de chaque bagage avant chargement. Ce scan, appelé SRB (service réconciliation bagages) permet de faire le lien entre les bagages et l'appareil. L'identification des bagages s'effectue à l'enregistrement du passager, étape déterminante dans le processus de sûreté. Il s'agit d'un point d'entrée pour relier le bagage au passager ainsi qu'à son vol (escales incluses).

Une formation spécifique au contexte de la sûreté

WFS, via son centre de formation Airport college[2] , dispense des formations à tout son personnel et à celui de sociétés intervenant sur la plate-forme aéroportuaire. Le processus pédagogique différencié selon les publics intègre globalement ou de manière approfondie toute la palette des métiers de l'aéroport.

(2) http://www.airportcollege.aero/fr/formations/formations-reglementees

La sensibilisation à la sûreté générale recouvre l'inspection et le filtrage des personnes avec leurs bagages de cabine, des articles transportés et des bagages de soute. Les contrôles touchent également le filtrage des véhicules et les contrôles d'accès.

Les techniques de fouilles de sûreté et de protection des aéronefs requièrent la connaissance des dispositions légales applicables aux fouilles de sûreté et de la configuration des types d'aéronefs sur lesquels la personne devra effectuer des fouilles de sûreté. Outre une aptitude à identifier les articles prohibés, les personnels formés doivent développer la capacité de réagir de manière appropriée en cas de détection d'articles prohibés. Ils doivent également avoir connaissance des moyens de leur dissimulation. Il est également important d'acquérir les protocoles de concordance entre passagers et bagages, la gestion du fret

ou courrier aérien identifiable et les approvisionnements de bord ainsi que les fournitures d'aéroport.

Les volets de formations concernent également les superviseurs et les gestionnaires de la sûreté qui suivent des modules spécifiques afin de fournir un encadrement et un management des opérations de sûreté en adéquation les menaces et les évolutions légales et réglementaires des dispositifs à appliquer.

L'AUTEUR

Mourad Dahmani est initialement chef d'équipe EDAC sur la plate-forme Roissy CDG. Il y est en charge de la gestion des enregistrements Départ-Arrivée. Il devient ensuite correspondant Qualité Sûreté chez WFS. Son domaine d'activité recouvre l'amélioration en continu des process qualité, le suivi des cahiers de charge des compagnies et des règles de sécurité dans l'entreprise. Il occupe actuellement la fonction d'adjoint au chef de secteur WFS. Il est garant de la qualité de service attendue par le client, il participe à l'organisation de l'exploitation et il est chargé de l'application des règles de sécurité et de sûreté dans l'entreprise.

Missions et engagements
des forces aériennes d'Île-de-France

par JEAN-FRANÇOIS GAUCHERY

Représentant par excellence de l'interaction entre le sol et les airs, l'hélicoptère est un moyen déployé par la gendarmerie nationale à travers les territoires métropolitain et ultramarins. Son domaine d'emploi couvre non seulement l'ensemble des missions confiées à la gendarmerie mais peut également s'étendre au profit d'autres demandeurs. Sa polyvalence lui permet en effet d'intervenir dans de nombreux domaines.

L'évolution des enjeux concernant la sécurité intérieure pousse les acteurs des forces aériennes de la gendarmerie nationale à adopter de nouveaux modes d'actions qui sont rendus possibles par une perpétuelle remise en question visant à intégrer et à s'approprier les avancées technologiques. La Section Aérienne de la Gendarmerie (SAG) de Vélizy-Villacoublay entretient et développe ainsi son savoir-faire au travers des différentes missions qui lui sont confiées.

JEAN-FRANÇOIS GAUCHERY
Capitaine de gendarmerie
Groupement des forces aériennes de gendarmerie d'Ile-de-France

Un large spectre opérationnel

Intervenant en appui des unités terrestres de gendarmerie lors d'opérations anti-délinquance, elle est régulièrement employée dans le cadre des enquêtes pour la recherche du renseignement grâce à la caméra qui équipe ses hélicoptères. Les interpellations, qui suivent les phases d'enquête, sont également parfois l'occasion d'employer ce moyen qui permet de contrecarrer les tentatives de fuites et renseigne les éléments d'intervention sur d'éventuelles menaces à proximité. La seule présence de l'hélicoptère assure le plus souvent un impact dissuasif sur le délinquant et permet ainsi une intervention dans de

Groupement des forces aériennes de gendarmerie

La capacité d'appui des forces engagées au sol est précieuse dans le cadre de la manœuvre.

bonnes conditions. L'hélicoptère, en tant que « vecteur de puissance », permet d'assurer aux forces de l'ordre et d'intervention un ascendant sur un adversaire de plus en plus violent et de mieux en mieux équipé technologiquement.

Lors de disparitions inquiétantes de personnes présentant une sensibilité particulière, alors que la gendarmerie exerce la responsabilité des recherches dans sa zone de compétence, l'hélicoptère est aussi appelé afin de couvrir rapidement de vastes zones, la caméra thermique apportant une grande plus-value. Bien que le taux de découverte de personnes disparues demeure faible, l'hélicoptère permet de rapidement « fermer des portes » en ratissant une large zone parfois difficilement accessible. En outre, le principe d'obligation de moyens dans ce genre de cas implique l'engagement de l'hélicoptère lorsque ce dernier peut apporter une plus-value opérationnelle. Là encore, le savoir-faire des équipages

permet d'apporter une précieuse aide à la décision quant à son emploi auprès des éléments au sol.

L'unité est également amenée à intervenir lors de violences urbaines, comme récemment en juillet 2016 sur les communes de Persan et Beaumont-sur-Oise, afin de renseigner les forces mobiles sur les mouvements et actions des personnes violentes. De la même façon, l'hélicoptère est parfois employé lors d'opérations d'envergure de police de la route, principalement lors des grands départs, mais ce volet ne représente qu'1 % des missions réalisées.

En marge de ces principales missions, l'unité est amenée à intervenir par subsidiarité d'autres moyens. Il arrive ainsi d'effectuer des évacuations sanitaires en complément des moyens déjà engagés, du transport d'autorités ou de spécialistes en sécurité nucléaire ainsi que de leur matériel, etc.

La gestion des grands événements

L'unité est également régulièrement engagée sur de grands événements afin de sécuriser ces derniers par l'expertise de son observation et une capacité de projeter rapidement des forces d'intervention. A ce titre, la COP21 ainsi que les déplacements des convois officiels qui en ont découlé ont été sécurisés depuis les airs par les hélicoptères de la SAG de Vélizy-Villacoublay tant pour rechercher d'éventuelles menaces que par la capacité d'appuyer dans de très brefs délais une intervention au sol par l'embarquement de tireurs d'élite. La SAG travaille ainsi régulièrement avec le GIGN et le RAID afin de garantir un haut niveau de technicité dans le domaine de l'intervention. A titre d'exemple, le Tour de France 2016 a également nécessité l'engagement de la SAG qui avait la charge de transporter tout au long du parcours une équipe du GIGN qui, en cas d'attaque, aurait été héliportée directement sur les lieux.

Un engagement lors des opérations antiterroristes

L'évolution des menaces, en particulier la menace terroriste, a amené les équipages à approfondir leurs techniques d'intervention, à concevoir des kits de blindage permettant de durcir l'hélicoptère qui demeure par nature à la fois vulnérable et une cible de choix. Comme l'a montré l'engagement de la SAG aux côtés du RAID lors de l'assaut donné sur un appartement abritant des terroristes à Saint-Denis, la menace est bien réelle et la capacité à intervenir de jour comme de nuit, en mesurant le degré de risque consenti face à cette menace, est primordiale. Quelques jours auparavant, la SAG avait été sollicitée par la préfecture de police de Paris à l'occasion des attaques qui avaient ensanglanté la capitale le 13 novembre 2016. En 2015, lors de la traque des

frères Kouachi, la SAG de Villacoublay, ainsi que celles d'Amiens et de Metz, avaient également été engagées. Plus récemment, et dans la continuité des opérations antiterroristes, la SAG a été sollicitée par le GIGN pour assurer de façon rapide, sûre et discrète l'extradition depuis la Belgique d'un des principaux suspects encore en vie des attentats du 13 novembre 2016.

L'AUTEUR

Le Capitaine Jean-François GAUCHERY est issu de l'École de l'air. Après 12 années dans l'armée de l'air (qualifié sur Fennec, Puma, Caracal, 1 détachement en Guyane, 1 détachement à Djibouti, 4 opérations extérieures en Afghanistan, 1 opération extérieure en Libye, citation à l'ordre de l'escadre aérienne) il entre à l'EOGN au grade de capitaine en 2012. Il est affecté au groupement des forces aériennes gendarmerie d'Ile de France à Villacoublay (78) depuis août 2013 (qualifié EC 135, EC 145, il prépare les tests d'entrée à l'EPNER).

Le système de captation d'image embarqué

par **SÉBASTIEN CLERBOUT**

« *La technique est moins importante que les hommes ou que la société. L'important, c'est le projet humain qui est derrière* ». Ce principe énoncé par Dominique Wolton, intellectuel français, directeur de recherche au CNRS et spécialiste des rapports entre sciences, techniques et société procède d'une mise en perspective de l'intérêt de la technologie : celle-ci doit servir un dessein humain et répondre à un besoin avéré. L'outil technologique, n'étant pas une fin en soi, ne doit constituer qu'une réponse à une envie d'innovation et se doit en tout état de cause de conserver l'analyse humaine au cœur de l'action.

SÉBASTIEN CLERBOUT

Chef d'escadron
Chef du Bureau Études et Suivi des Programmes
Commandement des forces aériennes de la gendarmerie nationale

C'est dans cette optique que s'est développé depuis le début des années 2000 un outil opérationnel devenu incontournable, au fil du temps et de sa mise en œuvre, dans la gestion de l'ensemble du spectre missionnel de la gendarmerie nationale et des autres acteurs de la sécurité intérieure : le système de caméra embarquée à bord des hélicoptères du Commandement des forces aériennes de la gendarmerie nationale (CFAGN). Fondé sur un concept d'emploi qui envisage l'hélicoptère non plus comme un simple moyen de transport et d'appui direct (appui lumière, appui feu...), mais aussi comme un acteur à part entière de la manœuvre de renseignement et de commandement, ce système résolument moderne est la base d'une véritable rupture opérationnelle, dans la lignée de l'ISR (*Intelligence, Surveillance and Reconnaissance*) développé par les armées.

Le concept d'emploi

L'observation aérienne, qui constitue une source de renseignement capitale dans de

Les moyens mis en œuvre par le CFAGN permet de participer à la sûreté du territoire.

nombreux cas, est un moyen de pénétrer le « *brouillard de la guerre* », autant lors de phase préparatoire à l'action que dans sa conduite en cours de mission, notamment en cas de «friction». La liberté d'action dont bénéficie l'aéronef, hors des conditions météorologiques fortement dégradées, et l'économie des moyens qu'il permet, par une utilisation adaptée et réduite au juste besoin des forces engagées au sol, est un levier démultiplicateur d'efficacité. La nécessité de connaître la situation opérationnelle ou tactique réelle se retrouve dans l'ensemble des dominantes d'intervention de la gendarmerie nationale : en police judiciaire, en sécurité publique générale (particulièrement en cas d'intervention contre-terroriste) et parfois même en mission d'assistance aux personnes. Le recours à un système embarqué de caméra performant et moderne présente alors plusieurs avantages décisifs, dont notamment :

– une capacité d'observation accrue en termes de détection ou d'identification, à longue distance (donc en discrétion et/ou sur une zone plus étendue), y compris de nuit,

– l'acquisition d'un renseignement direct au travers de l'image et, lorsque la caméra est couplée à un système de retransmission, sa diffusion simultanée à de multiples autorités ou intervenants (unicité et instantanéité de la compréhension de la situation),

– une fixation et une diffusion en temps réel ou différé de l'image permettant notamment une compréhension accrue de la configuration du terrain et de la situation, la recherche de la preuve pénale, voire la constitution d'un moyen de recours en cas de mise en cause de l'action de l'État,

– une opportunité pour le chef militaire de pouvoir gérer l'intervention depuis son poste de commandement tout en bénéficiant d'une vision réaliste de la situation par une « *immersion au cœur de l'action* » et non au travers de comptes rendus radiophoniques plus ou moins précis.

Cependant, pour qu'un système de caméra soit exploité au maximum de ses capacités, il est capital qu'il soit embarqué à bord d'un aéronef piloté. C'est en cela que l'on peut trouver une complémentarité entre l'hélicoptère et le drone. Ce dernier, s'il peut comporter des avantages indéniables (relative discrétion, capacité d'intervention en milieu dangereux ou contaminé) ne transmet toutefois que de la donnée brute, non valorisée, tout en étant, pour des raisons réglementaires et techniques, restreint à une utilisation ponctuelle (géographiquement du fait de sa difficulté d'insertion dans l'espace aérien, temporellement pour des raisons d'autonomie). *A contrario*, l'hélicoptère, sans même parler de sa réversibilité et de ses capacités multi-rôles, possède une capacité d'emport (charge utile) bien supérieure et peut donc mettre en œuvre des capteurs aux capacités techniques extrêmement perfectionnées. En outre, la présence d'un équipage, intégré à la manœuvre et disposant sur place d'une vision globale, confère une autonomie à ce vecteur tout en lui permettant de valoriser la donnée brute en lui donnant la qualité de renseignement directement traitable par l'échelon local.

Le système embarqué

L'EC 135 a bénéficié des enseignements tirés de la mise en œuvre du système HESIS qui équipait l'AS 350. Il a été pensé dès le départ comme un système d'arme, pleinement intégré, et n'a pas été conçu comme un vecteur sur lequel des fonctionnalités, dont la caméra, sont ajoutées au détriment parfois du devis de masse et du centrage de l'aéronef.

Cet aéronef est équipé d'une caméra de type WESCAM MX 15i implémentée d'un système de retransmission en temps réel. Cette caméra est dotée, outre d'un capteur « voie jour », d'une capacité IR (infrarouge) qui exploite le rayonnement électromagnétique émis par tous corps, dans une gamme de longueur d'ondes située entre le domaine visible et les micro-ondes. Elle l'amplifie et recompose une image exploitable avec différents niveaux de contraste. Ce principe se différencie en cela de l'amplification de lumière qui capte et multiplie les photons résiduels, requérant donc l'existence d'un fond lumineux, même extrêmement faible (lumière lunaire ou stellaire) et ne pouvant donc évidemment être utilisé que de nuit pour des raisons de saturation du capteur.

La capacité à opérer à distance de l'objectif a en outre été accrue au travers d'un couplage entre la caméra et le système de navigation propre de l'hélicoptère. Il est ainsi possible de pointer la caméra automatiquement vers un objectif sans même en être à portée visuelle humaine. Ceci permet par exemple d'adapter les trajectoires pour rester à distance de l'objectif, voire de simuler la

réalisation d'une autre mission (police route ou autre) tout en procédant à une reconnaissance discrète. Enfin, la finalité de nombreuses interventions étant la constitution de la preuve pénale, le système intègre un géo-référencement et un horodatage automatiques des images, elles-mêmes disponibles dans les formats informatiques classiques.

L'exploitation technique et les limites

L'outil technologique n'est pas autogéré et l'humain reste au cœur du système. En effet, comme le disent certains spécialistes, « *l'intelligence augmentée reste toujours préférable à l'intelligence artificielle* ». En « appui image », l'équipage est ainsi composé d'un ou deux pilotes, en charge de la gestion technique du vol et de la mission au plan tactique, et d'un mécanicien de bord responsable de la mise en œuvre de la caméra. Parfois, un observateur relevant de l'unité appuyée est amené à prendre place à bord de l'hélicoptère pour faciliter l'appréhension du terrain et affiner le besoin en renseignement en cours d'action.

Pour ce qui concerne la retransmission de la vidéo, plusieurs moyens techniques sont disponibles. Le choix du recours à l'un ou l'autre de ces systèmes est principalement dicté par l'impératif temporel ou le besoin opérationnel exprimé :

– Handy-view : écran portatif de mise en œuvre immédiate, offrant une portée de 2 à 3 kilomètres, utilisable dans des véhicules terrestres, nautiques ou aériens,

– station de réception transportable (valises durcies) ou fixe (système de racks) : mise en œuvre en 1 à 2 heures selon le site, offrant une portée de plusieurs dizaines de kilomètres,

– camion de réception : véhicule autonome qui intègre l'ensemble des systèmes radio opérationnels, offrant une portée de plusieurs dizaines de kilomètres grâce à un mât télescopique en fonction de la configuration du terrain.

Une fonctionnalité assez récente, développée en partenariat avec le STSI², se révèle particulièrement appréciable en complément de ces systèmes. Elle permet l'intégration sur un serveur informatique, accessible par un binôme « identifiant-mot de passe », de l'ensemble des flux vidéo après réception par une station fixe et la diffusion sur l'intranet gendarmerie. Cette capacité innovante a notamment permis de gérer la diffusion en temps réel des images filmées lors de l'EURO 2016 à l'ensemble des autorités militaires ou administratives concernées.

Il s'ajoute encore à cela l'incrustation sur un fond cartographique de la position de l'aéronef, ainsi que de celle de l'image diffusée (appelée la fauchée).

Cependant, la diffusion d'images capturées par un moyen aérien, parce qu'elles s'adressent à des autorités qui ne sont pas forcément rompues à leur utilisation, doit s'accompagner de deux précautions :

– la mise en place au centre de retransmission d'un militaire des FAGN qui établit le lien entre l'équipage et les autorités afin de présenter le contexte opérationnel

global et d'assurer la conduite de la mission en lien avec l'équipage embarqué. Ceci permet notamment d'éviter l'écueil de l'« effet tunnel », prisme biaisé dans lequel l'autorité, centrée et focalisée sur l'image présentée, peut en avoir une interprétation erronée. Ce type d'incompréhension est à rapprocher de la situation des violences urbaines de 2005 au cours desquelles certains journalistes, surtout internationaux, centraient leurs interventions uniquement sur les lieux d'affrontements intenses, laissant penser que la France entière était ravagée par les émeutiers,

– ne pas céder au micro-management, dans lequel l'autorité se focalise sur l'hélicoptère et tente de « téléguider » celui-ci, car ce mode opératoire s'effectue au double détriment de l'équipage (surcharge de travail dans un contexte souvent difficile voire dangereux) et de l'autorité (focalisation excessive et manque de prise en compte des autres sources de renseignement).

Enfin, le dernier impératif qui doit être absolument respecté est bien entendu le cadre réglementaire inhérent à la captation d'images. Elle est, pour ce qui concerne l'hélicoptère et sa caméra, soumise à la fois à la réglementation liée au respect de la vie privée et à l'image aérienne, mais aussi, en termes de constitution de la preuve, aux mêmes standards que ceux qui prévalent pour la prise de vue judiciaire (différenciés selon le type d'enquête et selon qu'ils constituent une observation simple, un dossier d'objectif ou un enregistrement pour insertion en procédure).

L'apport de cette technologie est donc devenu incontournable dans de nombreux secteurs d'intervention de la gendarmerie nationale. Il s'est accompagné de la mise en place d'une doctrine dédiée, d'un apprentissage rigoureux des aspects techniques liés à sa maîtrise et de la mise en place d'un corpus réglementaire précis. Cette capacité s'intègre parfaitement à la manœuvre globale pour y donner sa pleine plus-value opérationnelle.

Le système de caméra embarquée avec retransmission d'images ne peut que se développer plus encore dans le futur au regard des évolutions technologiques à venir. Le CFAGN s'y prépare donc déjà en étudiant la possibilité d'implantation de cette capacité rénovée sur ses AS 350.

L'AUTEUR

Le CEN Sébastien Clerbout est issu de l'école de l'air. L'essentiel de sa carrière en Gendarmerie se fera au sein des forces aériennes : SAG d'Amiens, Limoges et de Mayotte. Il sert ensuite à l'état-major du CGAG comme chef du BOE (Bureau organisation et emploi) puis du BESP (Bureau Études et Suivi des Programmes).
Il est lauréat de l'EMST (Ecole multinationale supérieure des télécommunications) et titulaire d'un master spécialisé en ingénierie en avion et hélicoptère avec une spécialisation drône. Il a obtenu une mention exceptionnelle dans le cadre d'un stage d'entreprise au sein du groupe AIRBUS HELICOPTER DEFENSE & SPACE (conception d'un prototype anti-drône en phase d'homologation et d'industrialisation).

HAROPA

UNE ECONOMIE INTERCONNECTÉE QUI NÉCESSITE UNE STRATEGIE DE SÛRETE

L'obtention d'un seuil critique en terme commercial impose de regrouper des structures portuaires complémentaires par leur offre et leur continuité géographique. Leurs hinterlands, qui cumulent des fonctions de stockage de transformation et de distribution, doivent être parfaitement reliées aux zones de production et de consommation par une offre multimodale qui mobilise les ressources des voies navigables et des réseaux routiers et ferrés.

Ces espaces stratégiques, car ils concentrent l'essentiel des flux commerciaux de la France, doivent se développer dans un environnement durable qui apporte des solutions en terme de pollution, de services et d'accessibilité. Il faut également intégrer à cette sphère économique, génériquement à vocation économique, une stratégie de sûreté en la déclinant dans chacune de ses composantes en parfaite synergie avec les acteurs régaliens.

Les aires portuaires ont fait récemment leur révolution sous la pression de nouvelles menaces liées aux activités économiques illicites mais également aux faits de terrorisme. Les études engagées par la DGITM (Direction Générale des Infrastructures, des Transports et de la Mer) aboutiront sans aucun doute à une intégration des voies navigables dans une stratégie globale propre à la gestion de la sûreté d'une économie nodale et interconnectée.

Le premier système portuaire français est un espace stratégique

Entretien avec ANTOINE BERBAIN

La Revue : Les ports du Havre, de Rouen et de Paris se sont réunis. Pouvez-vous nous expliquer la démarche HAROPA ?

Créé en 2012, le « HAROPA » incarne l'ambition partagée des trois ports de la Vallée de la Seine : former un système portuaire de niveau européen en prenant appui sur les forces de chacun des trois ports du Havre, de Rouen et de Paris au cœur d'une des zones de production et de consommation les plus riches d'Europe forte de 22 millions de personnes. Pourquoi ce nom « HAROPA » ? Pour Havre Rouen Paris, mais aussi pour Harbours of Paris, mais également pour l'allitération avec EUROPA et matérialiser ainsi un ensemble de niveau européen.

ANTOINE BERBAIN
Directeur général délégué HAROPA

HAROPA, avec plus de 90 millions de tonnes de trafic, est un système portuaire de premier plan en Europe en cumulant l'offre de trois ports :

– le Port du Havre est le 1er port à conteneurs de France. Il est capable d'accueillir les plus grands navires à pleine charge 24h/24 et 7J/7 sans contrainte de marée. Il est également le 2e port français pour l'approvisionnement en pétrole brut.

– le Port de Rouen est le 1er port exportateur de céréales d'Europe de l'Ouest. Ce port maritime d'estuaire dispose de 33 terminaux spécialisés répartis le long de la Seine et permet de remonter avec des navires jusque dans l'agglomération rouennaise.

– le Ports de Paris, 1er port fluvial français, dispose de 900 hectares de foncier en Île-de-France, dont plus de 50 % situés en première couronne parisienne (ports de Gennevilliers, en aval de Paris, et Bonneuil en amont) ce qui permet de desservir l'ensemble de l'agglomération parisienne.

Haropa

L'hinterland des ports comporte une connexion des réseaux fluviaux, routiers et ferrés qui est la condition d'une respiration économique durable.

Ce concept est-il réellement novateur ?

Naturellement, d'autres y ont pensé, souvent en dépassant les questions portuaires tout en les utilisant pour fédérer le territoire de la vallée de la Seine du Havre à Paris autour d'un projet commun. Erik Orsenna dit que le port de Paris est évidemment Le Havre. Antoine Grumbach, dans le cadre de la réflexion sur le grand Paris en 2008, a insisté sur l'importance de la vallée de la Seine comme territoire partagé d'une même métropole internationale en paraphrasant la citation qu'aurait prononcée Bonaparte au Havre en 1802 « Paris, Rouen, Le Havre, une seule et même ville dont la Seine est la grande rue ». Jacques Attali considère que le Grand Paris peut être la capitale naturelle de l'Europe occidentale en intégrant la vallée de la Seine car il n'y a pas de grande métropole mondiale sans façade maritime. On voit qu'en 2008 une vision fédératrice à l'échelle de la Vallée de la Seine a émergé ou réémergé, si on repense à Bonaparte, et mis la vallée de la Seine sous la rampe des projecteurs.

Le développement de la Seine dépend-il de celui des ports ?

Les ports concentrent en effet une partie importante de l'activité industrielle, logistique et touristique avec des emplois directement localisés sur les ports. Ils sont de l'ordre de 70 000 sur les ports du Havre, de Rouen et de Paris et les emplois indirects, encore plus nombreux, sont estimés à 160 000.

Un autre enjeu est le maintien du caractère durable des chaînes logistiques qui permettent le transport des marchandises sur le territoire en étant compétitives, sûres, fiables et écologiques. Le deuxième enjeu, à l'échelle des ports, est de faciliter le passage des marchandises des bateaux vers les barges fluviales, les trains et les camions. Il impose la mise en œuvre de projets visant à améliorer sur l'ensemble de la vallée de la Seine la circulation des barges, des trains et des camions.

Le troisième enjeu concerne l'aménagement de ports qui gèrent environ 12 000 hectares de zones d'activités et de zones naturelles. L'activité des ports est située dans des zones écologiquement sensibles de la baie de Seine et du cours de la Seine. Elle doit donc concilier préservation de la biodiversité et développement de l'économie. Situés à proximités de zones habitées, les ports doivent également soigner les liaisons avec les villes et donner des garanties en termes de limitation des nuisances, des pollutions et des risques industriels.

Quelles sont les voies de progrès ?

Nous avons pour habitude d'évoquer les 4 piliers de notre offre :

L'offre maritime, qui est d'ores-et-déjà au meilleur niveau européen. Avec 600 ports touchés dans le monde, près de 50 armements qui offrent des services, l'accueil des plus gros porte-conteneurs existants sans contrainte de marée à Port 2000. Pour l'amélioration de l'offre maritime nous investissons massivement. Il s'agit du programme d'amélioration des accès maritimes du port de Rouen qui va améliorer d'1 mètre le tirant d'eau pour l'accès aux différents terminaux du port et permettre au bateaux jusqu'à 290 m de long de remonter jusqu'à l'agglomération rouennaise. Ce programme d'investissement de 180 M€, qui a débuté en 2012, est réalisé de l'aval vers l'amont et se terminera en 2018.

L'offre multimodale qui concerne le fluvial et le ferroviaire. Le transport fluvial constitue un réel atout pour nous grâce au réseau de la Seine qui permet de relier les ports, les différentes zones de production et les agglomérations qui sont à la fois des espaces de production et de consommation. C'est d'autant plus un atout que le réseau fluvial est loin d'être saturé contrairement aux réseaux routier et ferroviaire. Il y a donc un intérêt particulier à le développer.

Le transport ferroviaire permet comme le transport fluvial de transporter de grandes quantités de marchandises en un seul voyage, limitant, comme le fluvial, les émissions de CO^2. Si un train va pouvoir transporter la cargaison de 70 camions, une barge pourra transporter l'équivalent de 250 camions.

Le fluvial permet de transporter une plus grande quantité en un seul voyage mais le ferroviaire permet d'aller plus loin. Comparativement au transport fluvial, le transport ferroviaire permet en effet de desservir toute la France et de gagner des parts de marché au-delà de l'Île-de-France et de ses régions limitrophes. Il permet d'améliorer la compétitivité des chaînes logistiques passant par nos ports en étant économiquement plus performant que le transport routier sur de longues distances. L'offre ferroviaire reste une de nos principales faiblesses même si elle est en progrès aujourd'hui avec une dizaine de terminaux reliés par des services réguliers de transport combiné. Cette offre souffre notamment d'un problème de capacité dans la vallée de la Seine qui justifie le projet de modernisation d'un nouvel itinéraire ferroviaire, le projet « Serqueux Gisors » soutenu par HAROPA, complémentaire à l'axe ferroviaire historique Le Havre, Rouen Paris.

L'offre douanière est accessible *via* un guichet unique informatisé sur l'ensemble des ports de HAROPA. Il s'agit d'un système informatique (un cargo community system) auquel sont connectés les systèmes informatiques d'accueil des navires du Havre et de Rouen et de la douane. Ainsi les autorités portuaires, les différents acteurs organisateurs des chaînes de transport et la douane échangent leurs données de façon dématérialisée. Ce système permet notamment de faciliter les opérations dématérialisées de dédouanement. Ainsi aujourd'hui 98 % des marchandises sont dédouanées sans contrôle physique. Ce système continue à s'améliorer. La société SOGET qui le développe est en train de tester une nouvelle génération de son logiciel, S) One, sur l'axe Seine.

Quatrième élément de notre offre, l'offre foncière. Il s'agit de permettre l'installation d'entreprises sur l'ensemble de la vallée de la Seine et donc d'avoir une offre foncière suffisamment complète et diversifiée et également immédiatement disponible pour répondre aux besoins de nos prospects.

Après quatre années, quelle est votre analyse d'HAROPA ?

Nous regrouper nous a permis de nous positionner dans le peloton de tête en termes de trafic, ce qui n'est pas uniquement une question d'affichage. Cette posture rassure les chargeurs et les investisseurs. Elle donne un poids face aux institutions nationales et européennes

qui cernent ainsi plus facilement en compte l'importance des projets que nous proposons à leur financement. Mais nous restons 5e au sein du Range Nord[1] : nous sommes un challenger face à des géants 2 à 4 fois plus grands ! Dépasser Anvers ou Rotterdam, ou même les approcher, n'est pas un objectif atteignable mais nous voulons gagner des parts de marché. Et demeurer, comme en 2015, dans le trio de tête des ports en progression. Cet ensemble, devenu stratégiquement incontournable sur le plan économique doit également faire l'objet d'une stratégie de sûreté afin de préserver les intérêts des acteurs mais également de la nation. J'ai laissé à Serge Marigliano, le soin de décliner cet aspect sur Haropa Le Havre dans le cadre de l'article qui suivra mon intervention.

(1) Le terme de « range nord-européen » (Northern range) désigne la concentration des ports européens alignés le long du littoral servant de façade maritime à l'Europe de l'Ouest.

Haropa

UNE SANCTUARISATION QUI DEMANDE UNE FORTE EXPERTISE

Il s'agit essentiellement de la sanctuarisation d'une surface d'échange multimodale qui réunit tous les vecteurs possibles : navires, réseaux routiers et ferrés, voies navigables. Elle englobe également les moyens de communication liés à la numérisation des infrastructures : communication avec les navires et gestion de leurs rotations à quai, opérations de douanes, surveillance par radar des eaux territoriales, numérisation des containers, *etc.*

Les autorités s'appuient sur le code ISPS (*International Ship and Port Facility Security*), procédure internationale mise en place par l'OMI (Organisation Maritime Internationale) mais également sur des processus de certification qui permettent de durcir les processus de sûreté et d'apporter une haute valeur ajoutée par une capacité opérationnelle et une réduction des risques auxquels sont exposées les personnes et les marchandises.

La coordination centralisée des installations portuaires de sûreté par les agents de sûreté portuaire mobilise des infrastructures et des équipements de sûreté (clôture, vidéo surveillance, *etc*) mais également une ressource humaine qui applique son expertise aux métiers des ports. Une force de surveillance et d'intervention contribue activement à la sûreté des personnes et des biens sur l'ensemble de la zone portuaire au côté des forces régaliennes. Le cœur de l'architecture de la sûreté est constitué par des personnels habilités : les officiers de ports, les contrôleurs et surveillants ainsi que les correspondants sûreté qui, au sein des capitaineries, sont chargés de la surveillance générale des interfaces navires/port. L'autorité portuaire, responsable de la sûreté des entreprises implantées sur les terminaux doit également s'assurer de la qualité de l'interface avec l'État.

La sûreté,
facteur de développement des ports

par SERGE MARIGLIANO

La sûreté maritime et portuaire est devenue un enjeu incontournable notamment sur le plan commercial. Elle englobe la prévention et la lutte contre tout acte illicite volontaire (terrorisme, malveillance) à l'encontre du navire ou des installations portuaires, et la protection des personnes (marins, personnels, navires, passagers) et des biens (marchandises, équipements portuaires, bâtiments, *etc.*).

Suite aux attentats du 11 septembre 2001, il est apparu une volonté d'établir une procédure internationale pour la sûreté des Installations Portuaires et des navires. La prise en compte de la possibilité qu'un navire puisse être l'objet ou le vecteur d'un attentat a conduit l'Organisation maritime internationale à adopter le code ISPS (*International Ship and Port Facility Security)*. Son application est devenue obligatoire depuis 2004 pour les navires et installations portuaires et il est le premier texte de l'OMI qui impose des mesures terrestres aux Etats. La réglementation européenne a renforcé les mesures imposées par l'ISPS en rendant obligatoire pour tous les états membres des dispositions facultatives de la partie B du code ISPS (2004). En 2006, l'Union européenne a imposé la mise en œuvre d'une gestion de la sûreté au niveau des autorités portuaires ainsi qu'une coordination centralisée des installations portuaires de sûreté par les agents de sûreté portuaire.

SERGE MARIGLIANO
Responsable Pôle Sûreté et Continuité d'Activité du Grand Port Maritime du Havre

Un enjeu stratégique

Le transport maritime a pris une dimension stratégique en devenant l'épine dorsale du commerce international, avec 90 % du trafic

HAROPA

La carte des ports HAROPA montre l'importance de l'axe stratégique de la Seine.

mondial. Ce mode de transport couvre l'essentiel des matières premières et du transport en vrac. Depuis le milieu des années 60, un nouveau marché s'est développé avec les conteneurs maritimes.

HAROPA, qui regroupe les ports du Havre, de Rouen et de Paris, représente plus de 120 millions de tonnes de trafics maritimes et fluviaux en 2015. Ces trois ports ont mis en œuvre sur leurs installations respectives le code ISPS et plus largement des mesures et des processus sûreté adaptés à chacun d'eux. HAROPA représente 2,7 millions de m² d'entrepôts en service, avec 1,2 milliard d'euros d'investissements pluriannuels et 160 000 emplois directs et indirects. Son activité le porte à la 5e place dans la hiérarchie des grands ports nord européens, de 1er port à conteneurs pour le commerce extérieur de la France, de 1er hub logistique de France, de 1er port exportateur de céréales d'Europe de l'Ouest, de 1er port mondial pour l'exportation des vins et spiritueux, de 1er port français pour l'import-export de véhicules neufs et de 1er port intérieur au monde pour le tourisme fluvial.

Un port étant un point d'entrée-sortie important sur le territoire, la sûreté doit y être envisagée de manière globale et impliquer l'ensemble des acteurs, chaque maillon jouant un rôle essentiel dans la chaîne d'approvisionnement de la marchandise, sur mer, sur fleuve comme sur terre. Au sein du GIE HAROPA, les ports de Rouen, Paris et le Havre définissent, en fonction de leurs activités, leur Plan de sûreté portuaire (PSP), les zones stratégiques et les procédures pour maintenir un niveau de sûreté optimal.

Au port du Havre, la sûreté implique tous les services car celui-ci est devenu, fin 2009, le 1er port européen et le 2e au monde à obtenir la certification ISO 28000 pour le management de sa sûreté. Cette dernière lui permet de piloter sa sûreté dans une démarche globale d'amélioration continue au profit de ses clients, partenaires et infrastructures.

Spécificités des mesures mises en œuvre sur le port du Havre

Les acteurs de la sûreté d'un port sont chargés d'évaluer les risques avec l'État puis de formaliser et mettre en œuvre le PSP. Celui-ci comprend l'ensemble des mesures générales et particulières de

sûreté applicables sur le port et sur toute la chaîne d'approvisionnement de HAROPA – Port du Havre. Le PSP définit des zones d'accès contrôlé et des zones d'accès restreint qui bénéficient de mesures de protection renforcée. La zone portuaire de sûreté intègre toutes les zones d'activité sensibles, les installations portuaires, les parcs logistiques et les industries à risque, qui pourraient constituer des cibles privilégiées pour toute personne malveillante.

Face à une menace, notamment terroriste, évolutive et protéiforme, HAROPA – Port du Havre met en œuvre une politique de sûreté. Elle comprend le déploiement des infrastructures et les équipements de sûreté (clôture, vidéo surveillance, *etc.)*. Elle vise à garantir auprès de ses clients la sûreté de la chaîne d'approvisionnement de la marchandise en transit sur la zone portuaire. Le directeur général du port approuve ainsi les objectifs sûretés stratégiques qui sont déclinés par services et font l'objet de plans d'actions.

Elle repose, conformément à la réglementation européenne, sur un Agent de sûreté portuaire (ASP) mais également sur un service atypique. L'ASP, commissionné par l'autorité Portuaire, est rattaché à la Direction des Opérations. Il doit établir un plan de sûreté portuaire et le mettre en œuvre. Il organise et participe au Comité local de sûreté portuaire (CLSP) présidé par le Préfet, et il entretient des relations étroites avec les différents services de l'État. Enfin, il contribue à la conformité réglementaire des 23 Installations Portuaires (IP) présentes sur le domaine et placées sous la responsabilité des Agents de Sûreté des Installations Portuaires. Au Havre, l'ASP pilote et assure la mise en œuvre du système de management de la sûreté. Il est également en charge du pôle Sûreté et Continuité d'Activité comprenant un chargé de Défense.

La cybercriminalité concerne également les ports. La politique de sûreté prend donc en compte cette menace actuelle par la sécurisation des systèmes d'information sensibles. Un exemple récent montre l'importance de cette démarche. En 2011, un port européen a été la cible d'une cyberattaque d'envergure par une organisation mafieuse de trafic de drogue. Les trafiquants ont recruté des pirates afin de pénétrer les systèmes informatiques qui contrôlent le mouvement et l'emplacement des conteneurs maritimes. Ils cachaient leur butin au départ et, grâce aux pirates, envoyaient des chauffeurs, armés de mitrailleuses, récupérer leur chargement avant que les dockers du port ne les aient débarqués et ouverts. Même si la police locale a réussi intercepter les transactions et arrêter les auteurs, ce fait met en évidence la réelle menace dans ce secteur informatique.

HAROPA

La cartographie de la zone portuaire du Havre permet de se rendre compte des problématiques de sûreté.

Un service de sécurité unique en France

Au-delà de la technologie, le port du Havre met en œuvre d'importants moyens humains. Le HAROPA – Port du Havre dispose d'un service de sécurité unique en France. Ce Service, créé en 1947 à la demande des clients du port, s'adapte aux différentes évolutions. Il dispose à ce jour d'un effectif de 130 agents, recrutés notamment parmi d'anciens adjoints de sécurité de la police ou gendarmes adjoints volontaires. Commissionnés par l'employeur, le président du directoire du port, ils sont agréés par l'autorité préfectorale et le procureur de la République. Ils sont assermentés devant le TGI. Ils suivent une formation initiale de 5 semaines et une formation continue qui alternent formation interne et interventions d'organismes extérieurs. Immergé dans un univers particulier et vaste, ce service entretient des liens privilégiés avec les partenaires institutionnels que sont la police, la gendarmerie et la douane. Il participe ainsi aux réunions de la cellule anti-cambriolage locale. Sa connaissance approfondie du terrain, du monde portuaire et de ses acteurs constitue des points forts permettant une véritable coproduction en matière de sûreté sur la zone portuaire.

Commandé depuis toujours par un ancien officier de gendarmerie, le service contribue activement à la sûreté des personnes et des biens sur l'ensemble de la zone portuaire afin de maintenir en permanence un environnement favorable au bon exercice des activités industrielles et commerciales. Il s'agit donc de contribuer, au côté de l'État, à la sûreté globale de la zone portuaire au profit des clients et des infrastructures du port. Les agents interviennent quotidiennement pour fluidifier la circulation sur les 150 km de routes et 200 km de voies ferrées que compte le port. En matière de sécurité, dans ce cadre, ils mettent fin à toutes les situations dangereuses qu'ils sont amenés à rencontrer. Cependant, leur cœur de métier reste la sûreté, domaine dans lequel ils interviennent avant tout de façon préventive par une surveillance continue

24/7 de l'ensemble de la zone portuaire au moyen de patrouilles mobiles et par leur présence aux entrées des terminaux à conteneurs et du terminal roulier (contrôle d'accès et vidéoprotection). Ils protègent également plus de 120 sites logistiques et industriels privés et bâtiments sensibles du GPMH[1] au moyen d'une centrale de télésurveillance et des patrouilles qui restent en permanence en mesure d'intervenir rapidement (7 minutes en moyenne) en tout point du port, sur tout incident qui serait constaté ou signalé.

(1) GPMH : Grand port maritime du Havre.

À cela s'ajoute l'action sûreté de la Capitainerie : 52 officiers de port, tous formés ASIP[2], sont chargés de la surveillance générale des interfaces navires/port et 27 contrôleurs et surveillants de la circulation maritime travaillent au plus proche des navires et des métiers portuaires. Renforçant le dispositif de surveillance, des correspondants sûreté contribuent à l'application des mesures de sûreté telles que le contrôle d'accès et la surveillance des personnes entrant dans les zones identifiées. Conformément à la réglementation, l'ensemble de ces personnels fait l'objet d'une enquête par les services de l'État permettant leur habilitation à accéder aux ZAR et/ou aux informations classifiées Confidentiel Défense.

(1) ASIP : L'Agent de Sûreté de l'Installation Portuaire assume les responsabilités définies dans la section A/17.2 du code ISPS.

Les ports de Rouen et de Paris disposent d'organisations similaires adaptées à leurs activités. L'agent de sûreté du port de Rouen et le responsable du département « prévention et maîtrise des risques » du port de Paris assurent également, entre autres attributions, la coordination entre les responsables de la sûreté des entreprises implantées sur les terminaux du port et font l'interface avec l'État en intégrant la sûreté dès le niveau projet à toutes les nouvelles implantations sur le port.

Le Havre, premier port européen certifié ISO 28 000

Parce qu'il n'y a pas de nos jours d'activité commerciale ou opérationnelle pérenne sans une sûreté maîtrisée et efficace, HAROPA – Port du Havre a fait le choix dès 2009 de la certification ISO 28000.

HAROPA – Port du Havre est la première autorité portuaire européenne et la deuxième au niveau mondial (après Houston) à être certifiée ISO 28000. Cette certification lui apporte la reconnaissance du bon management de ses processus internes en termes de sûreté pour les navires, les marchandises et les entreprises établies dans le port. Elle témoigne auprès de ses clients d'un service à haute valeur ajoutée offert par celui-ci grâce à une capacité opérationnelle moderne et sûre.

Elle garantit la réduction des risques auxquels sont exposées les personnes et les marchandises le long de cette chaîne.

Elle traite des risques sécuritaires potentiels présents à tous les maillons de la chaîne et cible des menaces telles que le terrorisme, la fraude et la piraterie.

C'est donc avant tout la reconnaissance des méthodes sûreté de HAROPA – Port du Havre qui s'inscrivent dans une démarche dynamique de la maîtrise de ses actions sûreté. La volonté du GPMH étant de créer un espace sûr afin de rassurer ses clients, de s'améliorer en permanence et d'avoir une politique d'anticipation de la menace par le suivi d'indicateurs proactifs et de performance. Une nouvelle certification en 2015 souligne la volonté d'avoir une approche plus large que les exigences réglementaires en passant d'une approche purement administrative à une approche plus dynamique et opérationnelle qui engage tous les acteurs portuaires dans une démarche et une culture sûreté.

Activités, Sûreté et Ports HAROPA

La sûreté ne peut plus se résumer aujourd'hui à une action de gardiennage et de protection. Les clients qui ont des activités multiples ont aujourd'hui une forte exigence de sécurisation de leurs zones d'activités avec des mesures précises et adaptées aux risques et aux menaces qu'ils rencontrent.

Zones logistiques

Les zones logistiques au sein des ports ont vocation à se développer de manière plus rapide et dans des proportions plus importantes qu'ailleurs. Il est donc primordial de travailler en amont pour préparer l'installation de ces zones regroupant des matières diverses avec souvent une forte valeur ajoutée (bijoux, alcools, vêtements, véhicules de luxe, parfums..).

Opérateurs conteneurs et rouliers

Le port est doté de plusieurs réseaux de transport qui se croisent pour répondre aux flux de marchandises. Réseaux ferré, routier, fluvial et maritime opèrent simultanément pour exploiter les départs et les arrivées des marchandises et optimiser leur temps de présence sur les quais tout en respectant les procédures administratives et financières des douanes, et des manutentionnaires.

C'est dans cette perspective que le terminal multimodal du Havre a été mis en œuvre. Il permet à HAROPA de développer son offre de transfert de fret en combinant sur un même lieu tous les modes de transport. Il s'agit en effet d'une plate-forme sur laquelle les containers sont chargés en un minimum de temps sur trains (jusqu'à 1 000 m de long) ou sur barges fluviales qui remontent vers Paris et en retour drainent les produits de l'Île de France. Ce développement multimodal concentre en un même lieu de nombreux enjeux sécuritaires, chaque mode de transport ayant une problématique sûreté différente (vol, terrorisme…). Ces zones non soumises au code ISPS s'en inspirent cependant afin que soit assurée une cohérence dans la mise en sûreté des

installations sur l'ensemble de la zone portuaire.

Sites classés Seveso

Au travers de son plan de sûreté, HAROPA – Port du Havre focalise une grande partie de son attention sur les sites Seveso. Ils sont réglementés par les dispositifs de sécurité des activités d'importance vitale et sont intégrés dans le Plan Portuaire lorsqu'il existe un appontement qui les lie au code ISPS. Avec l'état d'urgence décrété suite aux différents attentats de 2015 et 2016, le niveau de sécurité a été élevé considérablement. Les sites classés Seveso sont sous la surveillance conjointe de la police, de la gendarmerie, de l'armée (patrouilles Vigipirate) et du service de la sécurité portuaire qui coordonnent leurs actions et échangent le renseignement en temps réel. Le port du Havre est également en lien régulier avec les responsables sûreté des différentes installations pour revoir régulièrement les dispositifs de sûreté et assurer le lien avec la sous-préfecture et la préfecture qui sont responsables de la sûreté sur le port.

Zones Croisières et Ferries

Enfin, le transport de passagers est une activité en plein développement depuis plusieurs années, que ce soit pour les navires de croisière ou les ferries. HAROPA – Port du Havre accompagne la ville du Havre à travers l'exploitant du terminal croisière concédé à l'office du tourisme et l'armateur du Ferry qui manage la sûreté du terminal sur lequel escalent ses navires. Le port conseille dans ce cadre les compagnies maritimes qui mettent en œuvre leurs propres équipements et ressources humaines en matière de sûreté, pour contrôler notamment les véhicules et les passagers. Les acteurs de la sûreté de HAROPA – Port du Havre font, là encore, le lien pour favoriser la sûreté et proposer avec l'État et les exploitants des solutions sûreté compatibles avec l'espace maritime.

L'AUTEUR

Ancien officier Gendarmerie, Serge Marigliano a participé à la rédaction de lois et décrets de sûreté en interministériel et au processus National d'audit sûreté. Après avoir été successivement responsable de la Sûreté, Sécurité des Aéroports de Lyon, directeur des opérations Groupe ICTS, directeur de la Filiale Aéroportuaire de SERIS Sécurité, responsable Pôle Experts Sûreté Aéroportuaire/Aéroports de Paris Ingénierie International (ADPI), il prend, en 2014, le poste de responsable Pôle Sûreté et Continuité d'Activité du Grand Port Maritime du Havre.
Membre de la réserve citoyenne de la gendarmerie nationale au grade de chef d'escadron, il est auditeur régional de Institut des Hautes Etudes de Défense Nationale – IHEDN. Dans le cadre de sa spécialité, il intervient pour le master management aéroportuaire de l'Ecole Nationale de l'aviation, et pour la Formation IPER OMI - Organisation Maritime Internationale.
Il est titulaire d'une licence de droit privé, d'un master « Droit de la sécurité » de l'université de Nice et d'un Exécutive MBA Management - ESG Paris.

Gendarmerie maritime

LES INVESTIGATIONS JUDICIAIRES EN MILIEU MARITIME REQUIERENT UNE EXPERTISE SPECIFIQUE

Le corpus juridique maritime est à la mesure de l'impérieuse obligation de sécuriser le commerce international. Toutefois, la structure de cet espace économique particulier engendre un large spectre criminel. Si le trafic se concentre sur des autoroutes de la mer pour rationaliser les flux, il attire ceux qui veulent y prélever des valeurs par des actes de piraterie, des détournements de marchandises et des pratiques numériques illégales. La numérisation des transactions commerciales, la conteneurisation et le volume des transferts obligent les autorités de contrôle à des opérations ciblées mais sans commune mesure avec l'étendue des fraudes.

La répression des infractions reste complexe. Le service de l'enquêteur doit maîtriser l'interaction des normes internationales, communautaires et nationales. Une coopération internationale est souvent requise devant la diversité des acteurs et des pavillons qui conditionnent des critères de compétence et des pratiques judiciaires spécifiques. Enfin les investigations demandent une forte expertise du milieu, le respect de contraintes économiques et une projection dans le temps qui nécessitent un corpus d'enquêteurs pérennes et susceptibles de projections opérationnelles.

L'or bleu au cœur
des appétits criminels

par **FLORIAN MANET**

Dans ses premières orientations, liées aux actes de piraterie et aux catastrophes entraînant la perte du bâtiment, le droit international de la mer va durablement se focaliser sur la prévention des fortunes de mer et, de fait, s'attacher à protéger la vie humaine en codifiant, par exemple, l'armement des navires, les dispositifs et les procédures de sécurité…. imposés à bord des navires de commerce des État parties à la convention SOLAS[1]. Il faut donc attendre la fin du vingtième siècle pour que des prescriptions en matière de sûreté[2] intègrent le corpus juridique maritime international. Successivement, le traumatisme du détournement du navire Achille Lauro[3] en 1985 et celui lié aux attaques terroristes du 11 septembre 2001 ouvrent le droit maritime aux enjeux de la sûreté maritime et, plus seulement, à ceux de la sécurité de la navigation.

FLORIAN MANET

Lieutenant-colonel de gendarmerie, commandant la section de recherches de la gendarmerie maritime.

Une prise de conscience tardive à la fin du XXe siècle

(1) La convention SOLAS ou *safety of life at see* adoptée en 1929 en réponse au naufrage du Titanic a été enrichie en 1929,1948,1960 et 1974.

(2) Le chapitre XI – 2 relatif aux mesures spéciales pour renforcer la sûreté maritime comporte le code ISPS ou code international pour la sûreté des navires et des installations portuaires. Il s'agit de mesures de prévention du risque terroriste ciblant le transport maritime dont certaines prescriptions s'imposent aux Etats partie à la convention.

Cette prise de conscience est d'autant plus pertinente que l'ouverture à la mer est désormais plus que jamais une des conditions du développement de la puissance économique d'un pays. Par nature, l'espace maritime semble aussi apporter une couverture confortable pour les malfaiteurs au vu de son immensité et du principe de liberté de circulation qui régit la navigation maritime. Toutefois, une situation paradoxale émerge

Haropa – GPMH

La concentration du commerce international sur des Hubs nécessite la connexion entre informations terrestres et maritimes pour donner une cohérence aux procédures judiciaires.

(3) L'événement tragique de l'Achille Lauro provoque l'adoption d'une résolution de l'OMI relative aux mesures visant à prévenir les actes illicites qui compromettent la sécurité des navires et la sûreté de leurs passagers et de leurs équipages. En 1988, la convention de Rome dite SUA relative à la répression d'actes illicites contre la sécurité de la navigation maritime collationne l'ensemble des prescriptions en matière de sûreté.

(4) La convention des Nations unies pour le droit de la mer adoptée à Montego bay en 1982 promeut dans l'article 17 le droit de passage inoffensif dans les eaux territoriales d'un état pour un navire battant un pavillon étranger.

rapidement : comment alors concilier harmonieusement ce principe consacré par les conventions internationales[4] avec des objectifs de sûreté ?

La mer appartient à ceux qui l'utilisent[6]

L'espace maritime mondial recouvre près de 360 millions de km². Cette immensité rend illusoire une surveillance fine de cette immensité en dépit de technologies performantes. D'autant plus que cet espace a été juridiquement subdivisé en mer territoriale, espace de 12 miles nautiques où les pouvoirs de police de l'état côtier s'exerce souverainement, puis en zone économique exclusive, espace de 188 miles nautiques où s'impose l'exploitation monopolistique de la ressource par l'état côtier et, enfin, en eaux internationales où les pouvoirs de police sont de fait assumés par les

(5) *In* « sûreté maritime : bilan et perspectives du code ISPS », DMF 2006, p 66.

(6) Roland Le Goff lors du séminaire *human sea* organisé à Nantes le 5/10/2015.

(7) Qu'il s'agisse de trafic de produits stupéfiants, de traite d'êtres humains...

marines militaires dans des conditions variant d'un contentieux[7] à l'autre.

Les océans sont parcourus par plus de 50 000 navires de 500 tonneaux naturellement concentrés sur les autoroutes de la mer qui relient entre eux les hubs[8]. Par conséquent, de nombreuses zones se trouvent alors privées de navigation donc de capteurs d'informations. Dans ces conditions, les enjeux centraux de la surveillance de l'espace et des flux maritimes, qu'ils soient matériels ou immatériels, ont progressivement redessiné l'organisation de la « police sur l'eau ». Ainsi, les marines de guerre ont-elles davantage coopéré entre elles et échangé des informations à l'image des coalitions internationales mises sur pied ces dernières années afin de lutter contre la piraterie maritime. Simultanément, les acteurs privés ont pris en charge une part croissante du fardeau en se dotant d'équipes de sécurité privée à bord des navires dans les zones infestées de pirates ou en reportant des informations aux centres opérationnels des armées.

(8) http://www.enpc.fr/sites/default/files/files/Hubs-portuaires-Debrie.pdf

La mer, terrain de jeu des criminels

Dans ces conditions, des structures criminelles ont investi le domaine maritime afin d'y faire prospérer des trafics illicites avec un retour sur investissement particulièrement favorable. L'étude de ces groupes organisés met en exergue une double conception de l'espace maritime au cœur de leur commerce criminel. Dans un premier temps, la mer peut être considérée comme un vecteur logistique où transite le produit du crime entre la victime et le receleur. Tel un parasite, la *supply chain*[9] criminelle s'invite dans les circuits logistiques globalisés. Employé comme moyen, le navire présente de nombreux avantages : discrétion voire furtivité[10] aux yeux des forces de sécurité, dissimulation ou camouflage du produit dans des marchandises conteneurisées, faible pression policière, modèle économique compétitif et transfert d'une grande quantité de marchandises pour un coût de transport faible.

(9) La gestion de la chaîne logistique ou GCL, en anglais : supply chain management ou SCM).

(10) La plaisance n'est pas équipée de système d'identification ou AIS.

(11) http://www.lemarin.fr/secteurs-activites/shipping/25575-le-havre-anvers-un-trafic-de-vehicules-voles-demantele

De fait, le continuum entre les services répressifs terrestres et maritimes constitue une parade essentielle face aux agissements des organisations criminelles dans ce contexte. Ainsi, par exemple, en ciblant un phénomène[11] de vol de

SÉCURITÉ – SÛRETÉ MARITIME

Selon P. Polère[5], la sécurité maritime ou safety peut être comprise comme « la prise en charge des risques d'origine naturelle ou provoqués par la navigation maritime ».
Selon le règlement européen 725-2004 reprenant le code ISPS, la sûreté maritime ou security est « la combinaison des mesures préventives visant à protéger le transport maritime et les installations portuaires contre les menaces d'actions illicites intentionnelles».

véhicules observé en Île-de-France, les investigations judiciaires identifient une filière de recel opérant jusqu'en Afrique via des conteneurs maritimes au départ d'un grand port français ou belge. Partagés avec les services de police judiciaire maritime, ces renseignements permettent de révéler des trafics illicites par voie maritime difficilement décelables depuis un port. De manière inattendue, la terre agit alors comme un révélateur puissant de l'activité criminelle maritime.

Pour d'autres structures, la mer apparaît uniquement comme le théâtre des opérations criminelles, le lieu privilégié de commission d'infractions à la loi pénale. Cette perception singulière met en lumière la richesse que recèlent les mers : les produits de la pêche, de l'aquaculture, l'exploitation des fonds marins, le tourisme, la valeur marchande d'un porte conteneur sont autant de facettes qui attisent les convoitises des malfaiteurs. Ce théâtre des opérations est néanmoins particulièrement exigeant. Au-delà des risques de périls en mer, il nécessite de la part des structures criminelles une détermination et un investissement en moyens nautiques assortis de compétences de navigateur. De fait, elles sous-traitent ce volet à des marins recrutés pour l'occasion en exploitant bien souvent la misère humaine.

La mer, avenir de la terre

Dans le contexte actuel de maritimisation de l'économie, les enjeux de sûreté maritime affectent naturellement les équilibres géopolitiques. Ainsi, la maîtrise des routes maritimes comme celle des territoires sont intimement liées. La géopolitique du crime en mer s'explique en retour par l'existence de zones de tension à terre. État failli, la Somalie a, malgré elle, rendu le golfe d'Aden peu sûr pour la navigation de plaisance comme de commerce par le développement de la piraterie. De fait, dans des économies en flux tendus, ces zones d'insécurité ont imposé de nouvelles routes maritimes, généré des surcoûts et, au final, déséquilibré les organisations industrielles comme commerciales. Sans être exhaustif, on peut aussi évoquer les risques de malveillance pesant sur des installations sous-marines telles que les pipelines, les câbles téléphoniques ou les fibres optiques qui courent au fond des océans et qui relient les hommes et les territoires.

Le panorama du crime en mer révélateur de la fragilité des océans

Dans un rapport publié en 2008, le secrétaire général de l'ONU, Monsieur Ban Ki Moon, identifie sept menaces distinctes en matière de sûreté maritime qui demeurent encore très actuelles même si des tendances nouvelles émergent. Si la mobilisation internationale a permis de juguler les effets de la piraterie, l'attention se porte aujourd'hui résolument sur la prévention des actes de terrorisme en mer. La typologie est la suivante :

- la piraterie et le vol à main armée contre les navires,

- les actions terroristes impliquant le transport maritime, les installations off-shore et d'autres intérêts maritimes,

- les trafics illicites d'armes et d'armes de destruction massive,

- les trafics illicites de drogue et de substances stupéfiantes,

- les trafics d'êtres humains par la mer,

- la pêche illégale, non reportée, non-régulée,

- les atteintes volontaires et illégales à l'environnement marin.

Ce panorama souligne la variété du crime en mer mais aussi l'ampleur de ses conséquences car le risque généré par l'activité humaine en mer ne pèse pas uniquement sur ceux qui acceptent de le courir. Ainsi, le cas concret des atteintes à l'environnement est sur ce point illustratif : une marée noire ou bien le développement d'espèces invasives en mer ou dans les ports suite à des opérations de déballastage non régulières opérées par un navire soulignent les effets durables d'une infraction sur un territoire et le difficile combat à mener pour remettre en état l'écosystème.

Pour être exhaustif, cette typologie mérite, cependant, d'être enrichie par des infractions de droit commun qui affectent quotidiennement l'environnement maritime (homicide, délinquance d'appropriation (vol de bateaux, de moteurs de bateau..), atteintes au patrimoine informationnel, cybermalveillance….). Ces faits du quotidien impactent véritablement l'activité des gens de mer.

LE DROIT MARITIME ENTRE INSÉCURITÉS ÉCONOMIQUES ET INSÉCURITÉS JURIDIQUES

Selon Platon , « *il y a trois sortes d'hommes : les vivants, les morts et ceux qui vont sur la mer*». De fait, dès l'antiquité, un droit maritime s'est très vite constitué autour de principes aujourd'hui codifiés et reconnus internationalement. Sans débattre sur son autonomie juridique au regard du droit civil ou commercial, le droit maritime affiche cependant des traits caractéristiques résultant des conditions spécifiques propres à la navigation maritime supposant une forte prise de risque physique comme économique face aux aléas naturels, un investissement financier et matériel conséquent assorti d'une dimension internationale prégnante. De fait, selon M.Vialard, le droit maritime est défini comme « *l'ensemble des règles juridiques applicables aux activités humaines en mer* ». Pluridisciplinaire et transversal, il tire ses sources de la coutume bien souvent internationale, de conventions internationales, du droit communautaire et du droit national. Reposant notamment sur le principe du droit du pavillon, il dispose aussi de juridictions adaptées aux délits maritimes, les tribunaux maritimes.
Dans ce contexte d'insécurité spécifique, le droit maritime consacre le principe de passage inoffensif dans les eaux territoriales et celui de la solidarité des gens de mer qui se doivent assistance.

La police judiciaire maritime, une réponse adaptée aux enjeux de sûreté

Dans ce cadre, la répression des infractions commises ou constatées en mer s'avère complexe et spécifique au regard des règles habituellement applicables sur la « terre ». Le cadre légal repose ici sur un équilibre subtil entre le droit public international, communautaire et national. L'efficacité de ce dispositif repose sur la réalité de la coopération internationale. Quel que soit le lieu de commission de l'infraction, dans ou hors des eaux territoriales, les critères de compétences constituent le fondement de la légalité de la procédure engagée. Le cadre légal une fois établi, l'enquêteur est alors confronté à de multiples difficultés qui donnent cette saveur « eau salée » à une procédure judiciaire maritime. Il lui faut afficher une maîtrise de la culture du milieu maritime : la connaissance du vocabulaire technique, de l'organisation du travail, des contraintes du milieu... qui conditionne la réussite de ses investigations.

La dimension internationale est omniprésente au regard de la physionomie de la zone de compétence: la nationalité des acteurs (armateurs, équipages tant officiers que matelots, passagers) et l'État du pavillon du vecteur sont autant de données à prendre en compte. La conduite des investigations est aussi tributaire de la localisation d'une scène d'infraction qui, bien souvent, se trouve fort éloignée du territoire national, difficile d'accès, éphémère et sujette à des interventions extérieures régulièrement constituées de navires déroutés.

Outre les conditions de travail particulièrement difficiles en mer, la dimension économique contraint malgré tout la réflexion des décideurs : les coûts générés par le déroutement ou l'immobilisation d'un navire sans compter la projection d'enquêteurs sur cette scène d'infraction peuvent s'avérer très vite prohibitifs.

Enfin, la saisine judiciaire est conditionnée par la connaissance par les autorités publiques d'un fait ou d'un événement générateur ou moteur de l'action publique, de l'existence d'une infraction préalablement commise. Derrière la problématique de la remontée de l'information se pose la réalité des

LE SERVICE DE POLICE JUDICIAIRE DE LA MER

Placée sous les ordres du commandant de la gendarmerie maritime, la section de recherches est le service de police judiciaire de la mer. Disposant d'une compétence nationale au sens du droit maritime, ce service spécialisé est organisé en deux pôles d'investigations judiciaires luttant contre les atteintes à la sécurité – sûreté maritime, civile comme militaire et contre le crime organisé en mer, adossés à une division d'appui rassemblant des compétences en analyse criminelle, en délinquance économique et financière, en cyber et en criminalistique

capteurs dont la nature, publique ou privée, la finalité, opérationnelle ou non... va interagir. Précisons aussi que ces infractions peuvent avoir été commises au milieu d'un océan ou dans les eaux territoriales d'un autre État souverain, à des milliers de kilomètres du service d'enquête saisi comme du magistrat compétent. Ces acteurs endossent bien souvent le rôle d'un agent diplomatique avant de procéder à un quelconque acte d'investigation. Il est, en effet, utile aussi de rappeler que la loi pénale française trouve à s'appliquer dans l'espace[12]. Ainsi, la compétence de la police judiciaire maritime s'exerce un empire sur lequel le soleil ne se couche jamais !

(12) Cf article 113-1 du code pénal.

Le nécessaire partenariat public-privé

Au vu de la spécificité du milieu maritime et des activités criminelles qui s'y déroulent, les pouvoirs publics constituent un aspect de l'action préventive. Ayant le monopole de la violence légitime, incarnant la force du droit, les administrations publiques ne peuvent pas déléguer leur action répressive. Toutefois, la force du système de sûreté maritime repose avant toute autre chose sur un partenariat étroit et intelligent entre utilisateurs de la mer. Les navires de plaisance, à passager ou de commerce... constituent autant de capteurs d'informations de la situation maritime, unis entre eux par un sens aigu de la solidarité des gens de mer. Au-delà des intérêts économiques ou diplomatiques, c'est l'engagement affiché par les acteurs maritimes autour de l'application effective de principes de bonne conduite qui contribue aussi à sécuriser la navigation maritime.

Enfin, international par construction, le secteur maritime apportera encore davantage de garanties pour son activité par l'approfondissement de la « constitution de la mer » ou droit international de la mer, notamment en matière de lutte contre le terrorisme et de trafic illicite de migrants. L'heure des encouragements ou des invitations diplomatiquement formulés ne semble plus de mise au vu de l'évolution du contexte international.

L'AUTEUR

Florian MANET, Lieutenant-colonel de gendarmerie, commande la section de recherches de la gendarmerie maritime. Fortement impliqué dans la sûreté des transports, il a occupé les fonctions de conseiller gendarmerie du secrétaire général de la SNCF de 2011 à 2015. Ces fonctions particulières ont confronté cet officier à l'ensemble des problématiques sûreté affectant un opérateur d'importance vitale, agissant dans un cadre européen et international.
A ce titre, il a, notamment, animé, au sein du Club des Dirigeants de Sûreté d'Entreprises, un groupe de travail inter-entreprises associant les forces de l'ordre, dédié à la lutte contre les vols de métaux.

Gendarmerie maritime.

LA PROTECTION DU NAVIRE DOIT ÊTRE ADAPTÉE À SA TYPOLOGIE ET À SES SYSTÈMES EMBARQUÉS

Les navires sont maintenant intégrés à la toile planétaire. Le phénomène du shipping en est une illustration qui oblige à repenser toute l'architecture de sûreté des organes de gestion du navire pour assurer une confiance en matière commerciale.

Si les systèmes embarqués sont porteurs de failles, le gestionnaire peut s'appuyer sur une forte réglementation pour mettre en œuvre des solutions adaptées au navire et à ses fonctionnalités. Les codes ISPS, les manuels de gestion de la sûreté et les plans sûreté sont des références pour une conduite de la cybersécurité du navire. En février 2016, la DAM a transmis à l'Organisation Maritime Internationale (OMI) une soumission traitant des éléments sur la cybersécurité appliquée au navire. Elle a permis de participer activement aux travaux du comité de mai 2016. La circulaire de l'OMI MSC.1/Circ.1526 du 1er juin 2016 précise désormais le besoin de s'appuyer sur les codes pour gérer la cybersécurité du navire.

La détection d'un seuil de menaces qui a été mis en place par la DAM avec l'assistance de l'ANSII concourt à donner des réponses adaptées : isolement des systèmes vulnérables, adoption d'outils systèmes pour faire face aux cyberattaques, sensibilisation des personnels. Le déploiement d'outils technologiques permet de lutter contre les attaques virales par un dispositif adapté de pare-feux, de gestion des authentifications et des antivirus évolués. Elle donne également des indications précieuses en matière de reprise après un incident, sur les modalités de sauvegarde des données et de gestion de l'échange avec les systèmes extérieurs.

Ces dispositifs renseignent sur la politique de cybersécurité d'un armateur et son adéquation aux injonctions juridiques des autorités internationales et nationales.

Cybersécurité maritime : la nécessité d'élever la protection du navire

par **SÉBASTIEN LE VEY**

Le monde maritime n'est plus à l'abri d'un acte de malveillance via son système de gestion d'information. Cet article vise à expliquer la démarche mise en place par la Direction des affaires maritimes (DAM) afin d'élever le niveau de protection du navire face à ce type de menaces. Basée sur le triptyque vol d'argent, vol de données, acte de terrorisme, cette agression appliquée au navire peut comporter l'atteinte à l'image de la compagnie du navire, le cyberespionnage commercial du navire, le cybersabotage du navire et la cybercriminalité.

SÉBASTIEN LE VEY
Administrateur principal des Affaires Maritimes
Chef de la mission sûreté des navires

Avant toute chose, il apparaît nécessaire de rappeler le contexte de ce type de transport. La mer est aujourd'hui un maillon essentiel et incontournable pour nos échanges économiques. Chaque pays est interdépendant des échanges qui s'effectuent principalement par voie maritime. Près de 50 000 navires et un million de marins participent à cet échange mondial. Dans ce contexte d'échanges, depuis 25 ans le domaine du numérique n'a pas cessé de croître à bord du navire de commerce. Le monde informatique est omniprésent à bord. Il semble désormais difficile de se passer de cette technologie qui régule les moyens de communication, la conduite et les moyens de gestion de la cargaison du navire. Cette transformation technologique du navire de commerce en a modifié sa gestion. Désormais les échanges sont quotidiens entre le navire, la compagnie, le port, l'agent maritime… Le navire n'est donc plus isolé numériquement du réseau des réseaux. Le navire s'intègre naturellement dans cette toile planétaire du Net.

Les applications numériques participent totalement à la gestion des fonctionnalités des navires et y importent leurs failles.

Par voie de conséquence, notre navire est devenu un ensemble complexe de systèmes industriels. La conduite de ces systèmes n'est malheureusement pas exempte de défauts numériques. Les systèmes embarqués peuvent ainsi être la clé d'entrée d'un acte de malveillance. Ces trois dernières années, les systèmes de positionnement automatique et par satellite, le système de cartographie ECDIS (Electronic Charts Display Information System), le système d'enregistrement des données (Video Data Recorder) ont fait l'objet d'analyses. Ces dernières ont révélé plusieurs failles numériques à corriger.

Ces simples constats illustrent la vulnérabilité du navire à un acte de malveillance qui peut porter sur sa déstabilisation, l'espionnage, le sabotage et dans certaines conditions la cybercriminalité.

Bien que les actes de malveillance restent à ce jour très limités contre les navires, il convient cependant de les protéger. Protéger un navire consistera à préserver les moyens opérationnels et organisationnels de ce type de transport. L'objectif final sera de garantir qu'aucun acte de malveillance ne puisse mettre en péril la conduite et l'exploitation du navire.

Où se situe le seuil de la menace ?

Pour mettre en place une démarche de sécurité des systèmes d'information du navire, il est important de pouvoir identifier correctement les valeurs et les biens à protéger afin de les protéger

efficacement. Ceci implique une approche rigoureuse en fonction du type de navire et de son exploitation.

À ce jour, seul le code international pour la sûreté des navires et des installations portuaires (code ISPS) définit une recommandation en matière de gestion des procédés informatiques. Ce code précise que la vulnérabilité du système informatique devrait faire l'objet d'une évaluation dans le cadre de la sûreté du navire afin de disposer de mesures adaptées à une quelconque menace. Évaluer le niveau des menaces est par conséquent essentiel pour mettre en place des outils de lutte efficaces. C'est dans ce cadre que la DAM a mis en place une démarche de détection du seuil de la menace. Cette dernière est déterminée au travers d'une enquête menée depuis un an à bord des navires sous pavillon français et d'audits navires réalisés par l'Agence nationale de sécurité des systèmes d'information (ANSSI).

Le recueil de ces éléments permet dès à présent d'établir trois enseignements. Le premier porte sur la nécessité de « sacraliser » les systèmes industriels à bord du navire. Ces systèmes resteront par définition basés sur des technologies qui n'évolueront que très peu après leur construction et sont par conséquent vulnérables. Il est donc fondamental de les isoler et d'éviter les interconnexions avec d'autres systèmes de gestion du navire. Le second enseignement porte sur le besoin d'élever le niveau de protection du système d'information du navire en disposant d'outils systèmes adaptés à l'exploitation du navire et d'un système de gestion permettant de faire face à une cyberattaque. Enfin le troisième enseignement concerne le besoin de disposer de marins sensibilisés à cette menace. Ils pourront ainsi mieux détecter une incohérence système.

Quels moyens pour faire à cette menace ?

Les outils à mettre en œuvre dans le cadre de la protection de la sécurité de l'information à bord du navire sont de trois ordres : les outils technologiques, les outils de gestion et la formation.

Outils technologiques

Les outils technologiques doivent répondre à 5 engagements en matière d'hygiène de l'informatique :

– se protéger contre les codes malveillants,

– gérer l'architecture réseau,

– gérer les authentifications et autorisations d'accès,

– mettre à jour la sécurité des systèmes d'information,

– durcir les configurations,

La protection des données à bord d'un navire de la marine marchande ne réclame pas une approche du même

niveau que celle requise par un navire de combat. La stratégie d'une cyber protection efficace du navire civil peut donc faire appel à des moyens simples et peu onéreux présents sur le marché. La combinaison des outils technologiques à mettre en place peut être la suivante :

– Antivirus : ce système est un pré requis,

– Pare-feu : paramétrage des ports de l'ordinateur,

– VPN (Virtual Private Network) : connexion « tunnel » ,

– Anti-spyware : logiciel anti-espions,

– Sandbox : espace totalement étanche d'analyse de données,

– Logiciel de cryptage de messagerie, WIFI,

– IDS (Intrusion Detection System) : détection de toute intrusion,

– NAS (Network Attached Storage) : archivages de données.

Outils de gestion

Les outils de gestion à mettre en place devraient utiliser les règles de certification internationale. Pour un navire, ces règles sont encadrées par les codes ISM[1] et ISPS[2]. En référence à ces deux codes, le manuel de gestion de la sécurité inclut des références à la sécurité des systèmes d'information à bord du navire. Cependant, elles sont généralement très basiques. Quant au plan de sûreté, il correspond à une approche purement physique de la sécurité des systèmes d'information du bord. Le plan de sûreté du navire et le manuel de gestion de la sécurité sont les documents appropriés pour y inclure les références de gestion de la cybersécurité :

(1) International Safety Management – Code international de gestion de la sécurité

(2) International Ship and Port Facility Security - Code international pour la sûreté des navires et des installations portuaires.

– la politique de cyber sécurité de la compagnie,

– la gestion d'incidents issus d'un acte de malveillance : reprise du navire,

– l'autocontrôle du système d'information du navire,

– la sauvegarde des données,

– la gestion des échanges entre le navire et les intervenants extérieurs. Ce dernier aspect est essentiel car un cyber attaquant s'appuiera de façon certaine sur un intervenant extérieur pour contourner les mesures mises en place par la compagnie.

C'est dans ce cadre qu'en février 2016, la DAM a transmis à l'Organisation Maritime Internationale (OMI) une soumission traitant des éléments sur la cybersécurité appliquée au navire. Elle a permis de participer activement aux travaux du comité de mai 2016. La circulaire MSC.1/Circ.1526 du 1er juin 2016 précise désormais le besoin de s'appuyer sur les

codes déjà établis par l'OMI pour gérer la cybersécurité du navire.[3]

(3) http://www.developpement-durable.gouv.fr/IMG/pdf/Cyber_securite_-_renforcer_le_niveau_de_protection_du_navire.pdf

La formation

Le dernier levier qui permet d'élever le niveau de protection du navire consiste à former les marins. Le préalable de cette formation passe par une sensibilisation de l'équipage du navire. La DAM et l'ANSSI ont déterminé les éléments de base qui permettent d'éveiller la sensibilité du marin à cette menace.

Un guide verra le jour en septembre 2016 qui permettra aux marins d'appréhender ce risque. Une bonne hygiène informatique est un premier verrou qui contribue à faire face à cette menace dans la vie de tous les jours : gestion d'une clé USB, intervention de maintenance cadrée sur un réseau critique, administrateur réseau défini à bord, gestion des droits d'accès aux réseaux du navire…

Quel avenir pour élever le niveau de la cybersécurité du navire ?

La problématique de la cybersécurité du navire est posée. Le navire est relié à la toile et les systèmes embarqués peuvent comporter des défauts même si le seuil de la menace est relativement faible à ce jour. Toutefois, les systèmes technologiques et de gestion adaptés au navire existent et le monde du « shipping »[4] a posé un premier jalon de directives. Tout est donc en place pour protéger nos 50 000 navires. Pourtant, il subsiste une interrogation sur l'opportunité de le faire au regard de la marginalité actuelle des actes de malveillance numérique. La nécessité de mettre en place des mesures de sécurisation n'améliore pas la gestion de l'exploitation du navire et oblige à investir dans un domaine qui ne rapporte pas ! Le résultat de l'équation paraît de prime abord simple...

(4) Le e-shipping (online shipping) est le processus de passation de commande d'une prestation de transport entièrement réalisée sur Internet. Le e-shipping peut s'appliquer à l'ensemble des prestations de marchandises et des acteurs du transport (intégrateurs express, opérateurs postaux, sociétés de course urbaine, réseaux de points relais, messagerie rapide, fret routier, aérien ou maritime etc.).

Il faut cependant garder à l'esprit que la non prise en compte de cette menace à bord du navire pourrait être catastrophique et coûter bien plus cher qu'un investissement dans ce domaine. Imaginez les conséquences d'une cyber attaque sur un porte-conteneurs de 18 000 boîtes dont la valeur marchande peut atteindre 4 milliards de dollars ! En juin 2011, le port d'Anvers détecte une anomalie de son système de gestion des conteneurs. L'enquête conclura à la disparition de plusieurs conteneurs chargés de drogue en provenance d'Amérique latine. Le port d'Anvers venait de faire l'objet d'une cyber attaque rondement menée.

Quel que soit le mode de pensée, ce type de menace est désormais incontournable pour le monde maritime : plus les navires se numérisent, plus ils sont exposés. Par conséquent, il est essentiel de sensibiliser les armateurs. Il est essentiel également d'accompagner les armateurs pour concrétiser la mise en place d'outils de gestion, d'outils technologiques et d'une formation adaptée. Cet accompagnement est un des objectifs du directeur des affaires maritimes.

Maintenant, jusqu'où accompagner le pavillon français ? Cette frontière est fonction de l'évaluation de la menace. Si cette dernière correspond à la gestion de virus paralysant temporairement la cartographie électronique du navire, l'équipage devrait pouvoir y faire face avec des procédures adaptées. Si cette menace prend la forme d'une cyber arme sophistiquée dormante utilisant des failles système de type ODay, il est évident que ni l'équipage, ni le support informatique de la compagnie ne pourront y faire face ! Ce genre d'arme fait pourtant partie de la panoplie des outils à disposition de groupes criminels, de groupes terroristes ou d'États. En complément, n'oublions pas que le navire représente une excellente vitrine médiatique. Dans ce contexte, on peut raisonnablement s'interroger sur le besoin de disposer d'une « cyber flotte maritime stratégique » . À l'image de nos approvisionnements stratégiques qui imposent un quota de navires, on peut s'interroger sur le besoin pour la France de disposer d'un ensemble de navires garantissant un niveau d'exigence en matière de cybersécurité permettant d'assurer nos approvisionnements stratégiques. La France n'est pas à l'abri d'une cyber attaque en représailles à un choix fait par notre nation.

L'AUTEUR

Sébastien LE VEY est administrateur principal des Affaires Maritimes. Il occupe actuellement la fonction de chef de la mission sûreté des navires qui correspond à la gestion du domaine de la sûreté et de la cybersécurité appliquées aux navires sous pavillon français et dans le cadre du contrôle de l'état du port. Antérieurement, il a été pendant 11 ans en charge de la gestion de la sécurité/sûreté des navires auprès des affaires maritimes. Auparavant, il a servi pendant 12 ans dans la Marine nationale dans le domaine de la défense maritime du territoire au travers de diverses fonctions telles que la surveillance du territoire, la gestion d'opérations de sauvetage, l'encadrement et la formation.

Notes

Notes

DIRECTEUR DE LA PUBLICATION
Général de division **Philippe Guimbert**

Rédaction
Directeur de la rédaction :
général d'armée (2S) **Marc WATIN-AUGOUARD,**
directeur du centre de recherche de l'EOGN

Rédacteur en chef : colonel (ER) **Philippe DURAND**

Maquettiste PAO :
Major **Carl GILLOT**

Dépot légal
Raison sociale de l'éditeur :
CREOGN, avenue du 13e Dragons, 77010 Melun cedex
Général (2S) Watin-Augouard
Imprimerie : SDG - 11 rue Paul Claudel - 87000 Limoges
Avril 2017
ISSN 1243-5619

Message aux abonnés

La veille juridique de la gendarmerie nationale et la revue du centre de recherche de l'EOGN sont maintenant consultables sur le site internet du CREOGN
www.gendarmerie.interieur.gouv.fr/crgn/publications

vichie81

Perspectives inégalées et inattendues

La gendarmerie nationale s'est toujours attachée à maintenir en son sein un « escalier social ». Une gestion moderne des personnels procure des possibilités réelles et constantes de progression par la formation, la validation des expériences acquises et la réussite professionnelle. Cette thématique permettra d'explorer les facettes d'un épanouissement personnel dans la diversité des carrières offertes par la gendarmerie et d'approcher les pratiques d'autres administrations et du secteur privé.

MINISTÈRE DE L'INTÉRIEUR

www.gendarmerie.interieur.gouv.fr