Cyberdéfense : soutien pour le renseignement, la protection, la prévention et l'action

Rattachée directement au chef d'Etat-major des armées, la cyberdéfense militaire implique les armées de Terre et de l'Air, la Marine nationale et la Direction générale de l'armement pour analyser, planifier et intervenir aux niveaux défensif et offensif.

Elle a fait l'objet d'une communication à la presse, le 16 mars 2017 à Paris, par le vice-amiral Arnaud Coustillière, officier général cyberdéfense. De son côté, le lieutenant-colonel Victor Le Bihan a présenté l'exercice DEF NET 2017, qui s'est déroulé dans toute la France du 20 au 31 mars. Enfin, le capitaine de vaisseau Vincent Grégoire a expliqué la cyberdéfense dans la Marine au cours d'une conférence-débat organisée, le 22 mars 2017 à Paris, par le Centre d'études stratégiques de la marine.

COMCYBER. Commencée en 2011 avec quelques centaines de personnes, la « cyberdéfense » est devenue, en décembre 2016, le Commandement de cyberdéfense (COMCYBER), dont l'effectif devrait atteindre 3.200 militaires et civils en 2019, indique l'amiral Coustillière. Un échelon de préfiguration, créé en janvier 2017, met en place les textes juridiques et les processus nécessaires à la création du COMCYBER, qui sera structuré en 4 pôles : sécurisation des réseaux ; « défensif » avec l'intégration du CALID (Centre d'analyse de lutte informatique défensive) et ses relais au sein du ministère ; « action numérique » couvrant les différentes missions de combat ; la réserve. Pour recueillir les compétences destinées à développer les capacités techniques et tactiques, une campagne de recrutement vise les jeunes de moins de 30 ans, passionnés de numérique et désireux de servir leur pays. Tout juste diplômés d'écoles d'ingénieurs (bac + 5) ou travaillant déjà dans des petites et moyennes entreprises innovantes, ils bénéficieront de contrats de 3 à 6 ans, dont ils pourront valoriser l'expérience dans le monde civil ensuite. L'informatique irrigue tous les équipements des armées, systèmes d'armes et bureaux d'état-major. L'amiral a énuméré les menaces possibles : terrorisme basique sur internet ; grandes mafias ;

espionnage ; retour des grandes puissances, notamment la Russie. Dans ce domaine « gris », tous les maillons faibles d'un pays sont visés, en vue d'une déstabilisation et de son exploitation médiatique. Enfin, conformément à la doctrine de l'OTAN, le COMCYBER entretiendra des échanges selon les accords privilégiés avec quelques pays alliés, dont les Etats-Unis, l'Allemagne, la Grande-Bretagne, l'Estonie (pays d'accueil d'un centre de la cyberdéfense de l'OTAN) et les Pays-Bas.

Exercice DEFNET 2017. Pour entraîner à la lutte informatique défensive, l'exercice DEFNET 2017 s'est déroulé sur 11 sites pendant 2 semaines avec 5 plates-formes pour simuler 40 incidents. Il a mobilisé : 155 spécialistes militaires et 240 étudiants de 12 établissements de l'enseignement supérieur ; 3 industriels ; 1 unité de l'armée de Terre, 2 bâtiments de la Marine nationale et 2 bases de l'armée de l'Air. Pour la 1ère fois, des réservistes de la cyberdéfense ont été déployés sur la base aérienne de Rochefort. Dorénavant DEFNET sera organisé chaque année dans les armées.

Marine et cyberdéfense. La Marine s'adapter aux risques cyber selon trois axes, souligne le capitaine de vaisseau Grégoire : se structurer pour commander et agir ; protéger et défendre les systèmes d'information et systèmes d'armes ; agir dans le cyberespace au profit des opérations aéronavales. Elle protège ses unités et peut réagir à n'importe quel accident informatique pour conduire une opération en toute sécurité, notamment grâce à l'exercice DEFNET. Système complexe de capacités opérationnelles interconnectées, chaque navire est une plateforme de communication, d'information, de navigation et de combat. Ainsi, le maintien d'une eau réfrigérée à 6° C influe sur les conditions de vie à bord, la propulsion, les transformateurs électriques, le sonar remorqué, le radar multifonctions et les baies du système de combat. La cyberprotection va de « l'hygiène numérique » de base à l'homologation des systèmes sur les programmes navals. La cyberdéfense part des groupes d'intervention rapide en cas d'attaque, au renseignement, à l'entraînement des unités et à la coopération internationale avec les pays alliés. Pôles de référence, les centres de Toulon et Brest dépendent de l'amiral chargé des opérations et de la lutte informatique défensive et disposent d'experts pour les sous-marins, bâtiments de surface et infrastructures à terre. Ils vérifient les qualifications opérationnelles et développent des scénarios d'entraînement, à savoir des plates-formes de tests de simulation par des automates programmables et validés par le COMCYBER. Pour

réagir efficacement, il convient d'établir une cartographie des systèmes d'information du navire, lesquels se montent à 3.000 sur une frégate multi-missions ou un bâtiment de projection et de commandement. D'ici à 2019, un centre de cybersurveillance sera mis en œuvre pour : recueillir les renseignements d'intérêt cyber ; détecter les incidents en amont ; anticiper les cyberattaques en se plaçant à la place de l'agresseur qui aura perçu les vulnérabilités des systèmes. Un bâtiment de combat, réalisé en 5-10 ans, doit connaître une vie opérationnelle de 30-40 ans avec une garantie de la sécurité de ses systèmes, rappelle le capitaine de vaisseau Grégoire. Cela implique un lien entre les industriels de défense, la Direction générale de l'armement et les organismes de soutien de la Marine. La sécurité intervient dès la conception du navire pour réduire les risques aux niveaux des codes, de l'architecture, des réseaux et de la réflexion sur le maintien en condition opérationnelle. Elle est prise en compte pour la future frégate de taille intermédiaire et la modernisation du système de combat du porte-avions *Charles-De-Gaulle*. Par ailleurs, la Marine va recruter 125 personnes dans les écoles spécialisées d'ici à 2019 : officiers en master cyber ; officiers mariniers ; ingénieurs et techniciens civils. Elle devra ensuite les fidéliser, car ces personnels sont très recherchés dans le monde civil. Enfin, au niveau de la réflexion, une chaire industrielle sur la cybersécurité des systèmes navals a vu le jour en 2014 et regroupe l'Ecole navale, Télécom Bretagne et les groupes DCNS et Thales. Elle repose sur des post-doctorats et doctorats universitaires et des stages à l'Agence nationale de la sécurité des systèmes d'information.

Loïc Salmon

Cyberdéfense militaire : DEFNET 2015, exercice interarmées à tous les niveaux

Cyber : le combat numérique, nouvelle dimension militaire

Cyber : au cœur des enjeux de défense et de sécurité

Le ministère de la Défense a traité 24.000 actes malveillants de tous types en 2016. La loi de programmation militaire 2014-2019 prévoit un investissement global de 2 Mds€ pour la cyberdéfense et un effectif de 3.200 spécialistes, renforcés selon les besoins par 4.400 réservistes, dont 400 pour la réserve opérationnels et 4.000 pour la réserve citoyenne. Les missions des « combattants numériques » incluent : le durcissement des systèmes ; la recherche ; la veille et

l’anticipation des menaces ; l’audit ; les tests d’intrusion ; la supervision et la protection des systèmes d’information ; la détection et la recherche des compromissions ; l’investigation numérique et la veille sur les réseaux sociaux ; la participation aux opérations.