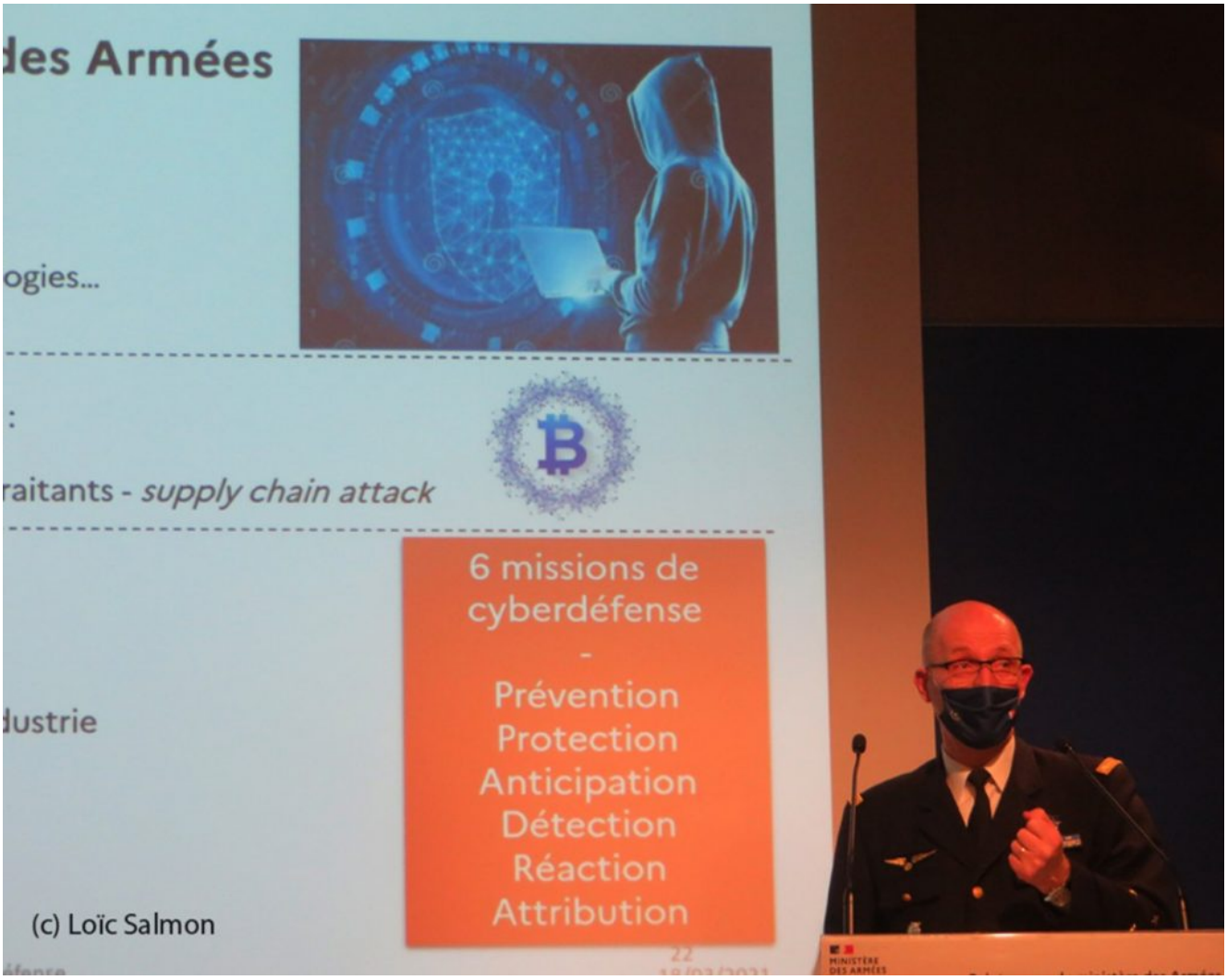
Défense : détecter les cyberattaques et réagir vite



La doctrine militaire française inclut le cyber comme arme d'emploi sur les théâtres d'opérations. Au-delà de son aspect technique, le cyber prend des dimensions juridique et politique.

A l'occasion de la 8ème édition de l'exercice interarmées « Defnet » (15-26 mars), l'état de la cyberdéfense militaire a été présenté à la presse, le 18 mars 2021 à Paris, notamment par Hervé Grandjean, porte-parole du ministère des Armées, et le général de division aérienne Didier Tisseyre (*photo*), commandant la cyberdéfense.

« Cyberconflictualité ». Le commandement de la cyberdéfense (Comcyber) dispose d'un état-major, installé à Paris, pour les orientations stratégiques, la conception et la conduite des opérations, via le centre opérationnel cyber. Le

Groupement de la cyberdéfense des armées a été créé le 1er septembre 2020 à Saint-Jacques de la Lande (Bretagne), à proximité de l'incubateur civilo-militaire « Cyberdéfense Factory ». Ce dernier permet aux petites et moyennes entreprises et aux universitaires de travailler au contact des opérateurs des armées et des experts de la Direction générale de l'armement. Outre la cybercriminalité, le terrorisme ou les actions hybrides de la part de groupes mercenaires rattachés à des Etats, l'hypothèse d'un engagement majeur dans le cyberespace est prise en compte, indique le général Tisseyre. Des exercices au sein de l'OTAN permettent de s'y préparer. Sur le plan national, il s'agit d'attribuer l'origine des cyberattaques, sans en divulguer la méthode pour éviter une vulnérabilité ultérieure. Leur gravité détermine la proportionnalité de la riposte, au niveau diplomatique, économique ou militaire. Le Comcyber travaille avec les services de renseignement dans la lutte informatique, défensive ou offensive, sur un théâtre d'opérations. Ainsi, l'exercice Defnet 2021 inclut des simulations de vrais incidents sur des systèmes d'armes en service, dans un contexte international au plus près de la réalité.

Defnet 2021. Cet exercice permet de tester la planification, la coordination et la mise en œuvre des mesures défensives face aux cyberattaques. Près de 260 « cybercombattants » sont mobilisés à Brest, Istres, Paris, Rennes et Toulon. Pour la première fois, les réservistes opérationnels sont intégrés aux équipes, afin de s'entraîner aux procédures militaires de gestion de crise cyber. L'Agence nationale de sécurité des systèmes d'information (ANSSI) et huit maîtres d'œuvre industriels, signataires de la convention sur la cybersécurité des systèmes d'armes en service, participent à Defnet. En outre, le Comcyber organise la compétition « Capture the Flag » entre 14 écoles d'enseignement supérieur à Paris, Laval, Rennes, Vannes, Saint-Malo et Lannion.

« Cybercombattants ». En 2020, l'ANSSI a détecté quatre fois plus de cyberattaques qu'en 2019 ainsi que 2.700 « événements de sécurité » au ministère es Armées, indique Hervé Grandjean. Pour contrer cette menace, la loi de programmation militaire 2019-2025 consacre 1,6 Md€ au cyber. Le nombre de cybercombattants, de 3.400 en 2020, doit atteindre 4.500 en 2025. Les armées assurent déjà des formations spécialisées : brevet de technicien supérieur « Système numérique informatique et réseau » au lycée militaire de Saint-Cyr l'Ecole ; mastère « Cybersécurité des systèmes complexes pour l'industrie et la défense » à l'Ecole de l'air et à l'Ecole centrale de Marseille ; mastère

« Cybersécurité des systèmes maritimes et portuaires », mis en place par l'Ecole navale et trois autres écoles d'ingénieurs en Bretagne.

Loïc Salmon

Défense : l'essor du numérique sur le champ de bataille

Cyber : capacité interarmées, niveaux stratégique et tactique

Cyber : nouvelle doctrine pour la lutte informatique