Exercice cyber à Nancy

Le commandement de la cyberdéfense

Enjeu et priorité stratégique, la cyberdéfense est garante de la souveraineté nationale. Avec de nombreux acteurs, le ministère des Armées participe activement à la protection et à la défense des systèmes d'information dans le cyberespace.

I/ Les missions et la chaîne de commandement du commandement de la cyberdéfense

Créé en mai 2017 par décret et placé sous l'autorité directe du chef d'état-major des Armées, le COMCYBER est un commandement opérationnel, qui rassemble l'ensemble des forces de cyberdéfense du ministère sous une même autorité permanente et interarmées. Il a pour mission la protection des systèmes d'information des armées, ainsi que la conception, la planification et la conduite des opérations militaires dans le cyberespace pour le ministère. Ce faisant, il a une mission naturelle de fédération et de conduite des actions des différents acteurs des armées, directions et services dans le cyberespace.

A/ Les missions du commandement de la cyberdéfense (COMCYBER)

Les opérations de cyberdéfense : le commandement de la cyberdéfense conçoit, planifie et conduit des opérations militaires de cyberdéfense ; il a également la charge de la protection et la défense des systèmes d'information du ministère des Armées à l'exclusion de ceux de la direction générale de la sécurité extérieure (DGSE) et de la direction du renseignement et de la sécurité de la défense (DRSD).

La stratégie de cyberdéfense : le commandement de la cyberdéfense coordonne les

contributions des armées et organismes interarmées à la politique nationale et internationale de cyberdéfense, notamment pour l'élaboration et la mise en œuvre des plans de coopération.

Le capacitaire : le commandement de la cyberdéfense contribue à l'élaboration de la politique des ressources humaines de cyberdéfense, à la coordination de la définition des besoins techniques spécifiques de cyberdéfense et au développement et à l'animation de la réserve de cyberdéfense.

Cyber : nous sommes régulièrement attaqués

B/ La chaîne de commandement du commandement de la cyberdéfense (COMCYBER)

a/ Le GCA : Groupement de la cyberdéfense des Armées

Dans l'exercice de ses missions, le COMCYBER dispose d'un état-major et d'une unité dédiée : le Groupement de la Cyberdéfense des Armées (GCA) créé le 1er septembre 2020. Le COMCYBER est déployé sur plusieurs emprises à Paris et à Rennes. Le GCA constitue pour le COMCYBER le lieu de développement et de décloisonnement des compétences en cyberdéfense par la création d'une entité unique accueillant les centres techniques suivants : CALID, CRPOC, CASSI et CHPI.

b/ Le CALID : Centre d'analyse en lutte informatique défensive

Situé sur deux pôles à Paris et à Rennes, jusqu'à son futur regroupement, le CALID est le centre de surveillance, de détection et d'alerte du ministère des Armées en cyberdéfense. Il fournit la première capacité d'intervention et d'analyse des événements de lutte informatique défensive.

Ses missions peuvent être divisées ainsi :

- anticiper les menaces ;
- détecter les attaques ;
- conduire les opérations défensives et analyser les attaques.

En tant que *computer emergency response team* (*CERT*) du ministère des Armées, il supervise les actions techniques des *security operations center* (*SOC*) des armées, direction et services et des *SOC* de théâtre. Il dispose d'une permanence 24h/24h. Dans le cadre des groupes d'intervention en cyberdéfense (GIC), le CALID peut être amené à projeter son personnel sur le territoire national comme à l'étranger.

c/ Le CASSI : Centre d'audits de la sécurité des systèmes d'information

Le Centre d'audits de la sécurité des systèmes d'information (CASSI) est un centre national dont la mission d'audit couvre deux domaines : la sécurité des systèmes

d'information (SSI) et les signaux parasites compromettants (SPC). Il intervient aussi bien en Métropole qu'Outre-mer et sur des théâtres d'opérations extérieures.

Jeunes élèves de BTS en cyberdéfense

Le CASSI mène des audits de conformité et contribue à homologuer des systèmes d'information. La démarche d'investigation avant ou pendant la mise en exploitation des systèmes d'information et des bâtiments inclut un diagnostic menant à des recommandations. Les équipes d'audits doivent :
- vérifier ou évaluer la qualité, l'efficacité et la cohérence des dispositifs mesurés et procédures de sécurité ;
- mettre en évidence les vulnérabilités résiduelles et conseiller en vue de leur résolution.

d/ Le CRPOC : Centre de la réserve et de la préparation opérationnelle de cyberdéfense

Le Centre de la réserve et de la préparation opérationnelle de cyberdéfense (CRPOC) est l'acteur majeur du recrutement et de l'affectation des réservistes de cyberdéfense. Il est en charge également de l'entraînement des états-majors, directions et services.

Le CRPOC, en lien avec le COMCYBER et les armées, s'occupe également de la préparation d'exercices nationaux et internationaux de cyberdéfense, tels que l'exercice annuel interarmées *DEFNET*, qui met en œuvre un scénario réaliste et dynamique visant à tester la chaîne de commandement et la coordination entre les différentes entités du ministère en cas d'attaque cyber majeure et l'exercice *Locked Shields*, organisé par le centre d'excellence cyber de l'OTAN à Tallinn en Estonie, qui réunit une trentaine de nations et a pour objectif d'évaluer les capacités de défense d'un réseau informatique complexe face à des cyberattaques.

Exercice **DEFNET** *2014*

e/ Le CHPI : Centre d'homologation principale interarmées

Les missions du centre d'homologation principale interarmées (CHPI) sont de procéder aux études de sécurité aboutissant à l'homologation des nouveaux systèmes d'information du ministère avant leur mise en service opéra-

tionnelle. À ce titre, il construit la première « brique » de sécurité des systèmes d'information du ministère au cours de leur vie opérationnelle.

II/ Le recrutement dans le domaine de la cyberdéfense

Pour remplir ses missions, le COMCYBER exerce un commandement opérationnel sur plus de 3 400 cyber-combattants. Comme annoncé par la ministre des Armées en septembre 2021, d'ici 2025, la défense française s'appuiera sur 5 000 cyber-combattants. Le recrutement s'effectue sous différents statuts (militaire, civil, réserviste), à tout type de niveau, notamment pour les passionnés du numérique. En effet, les profils recherchés sont divers, expert ou manager, premier emploi ou au titre d'un parcours professionnel diversifié. Ces postes couvrent un large spectre d'activités et des missions opérationnelles variées : de l'analyse à l'action, tels que 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 recherche de compromissions, l'investigation numérique et la veille sur les réseaux sociaux, la participation aux opérations et l'ingénierie en appui des opérations.

Rejoindre le ministère c'est :
- servir son pays dans un contexte de menaces en expansion dans le cyberespace ;
- protéger et défendre un des réseaux informatiques les plus étendus de France (plus de 300 000 machines) ;
- mener des opérations ;
- intervenir dans le monde entier.

A/ Les militaires d'active

Des postes militaires sont à pourvoir au sein des trois armées, des directions et des services du ministère des Armées. Ils sont ouverts aux techniciens et aux ingénieurs, expérimentés ou sortant d'école, formés au domaine de la cybersécurité, pour devenir officiers ou sous-officiers commissionnés.
Le statut de militaire commissionné (décret

La cyber défense des Armées

La Gendarmerie lutte contre la cyber criminalité

n°2008-959 du 12/09/2008) permet de devenir militaire, tout en bénéficiant d'une solde en adéquation avec votre niveau d'étude et d'expérience.

B/ Les civils de la défense

Le ministère des Armées développe ses capacités et offre de nouvelles opportunités professionnelles. Sécurité des systèmes d'information, défense contre les cyberattaques, opérations pour agir dans l'espace numérique, de nombreux postes civils (CDD et CDI) sont à pourvoir au sein des différentes armées, directions et services.

C/ La réserve opérationnelle de cyberdéfense : renforcer les unités opérationnelles

Afin de disposer d'une réserve directement employée par ses unités, le commandement de la cyberdéfense (COMCYBER) privilégie l'affectation des réservistes dans des postes opérationnels. Au vu des évolutions quantitative et qualitative des risques et menaces cybernétiques, les réservistes sont, plus que jamais, partie prenante de l'efficacité opérationnelle de la cyberdéfense militaire.

Dès aujourd'hui, les réservistes de cyberdéfense participent directement à la protection au quotidien des opérations du ministère. Ils apportent une expertise et des compétences singulières au sein des unités de cyberdéfense des armées : CALID, CASSI et 807e compagnie de transmissions, Centre interarmées des actions sur l'environnement (CIAE), etc. Au-delà de cette mission principale d'appui aux unités opérationnelles, le réserviste peut apporter son concours au recrutement et être employé pour des missions de veille technologique et soutien à l'innovation.

Sous statut militaire, avec un contrat d'engagement de 20 jours minimum, le réserviste opérationnel de cyberdéfense est employé directement au sein d'une unité cyber du ministère des Armées.

L'ancrage rennais de la cyber défense

D/ La réserve citoyenne de cyberdéfense : contribuer au rayonnement et aux réflexions de prospective du COMCYBER

Le commandement de la cyberdéfense s'appuie également sur la réserve citoyenne de cyberdéfense. Cette réserve rassemble des personnalités aux compétences d'intérêt majeur nécessaire à la montée en puissance des capacités cyber. Sous statut bénévole, le réserviste citoyen contribue aux réflexions technologiques, géopolitiques ou sociologiques liées à la cyberdéfense militaire, dans un esprit *« think tank »*, participe au rayonnement et à la communication vers la société civile.

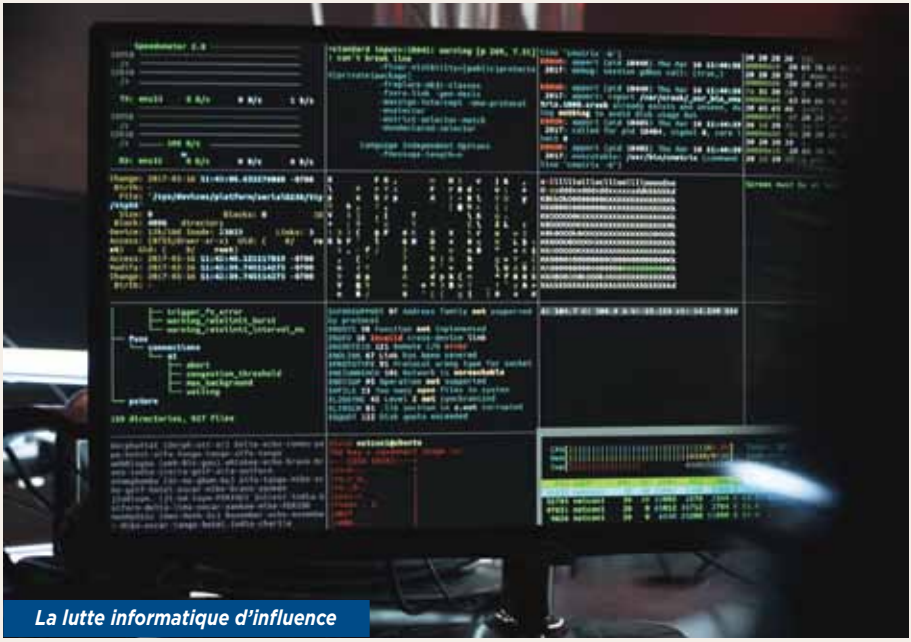
III/ Les doctrines de lutte informatique

Les opérations menées par le commandement de la cyberdéfense s'appuient sur un corpus doctrinal complet sur la lutte informatique défensive (LID), offensive (LIO) et d'influence (L2I). Ces textes structurent la chaîne cyber, et permettent une mobilisation rapide des moyens et des compétences disponibles tout en garantissant une cohérence d'ensemble de nos actions, en liaison avec les services de renseignement comme la DGSE, la DRM ou la DRSD et certains services de l'État.

A/ La lutte informatique défensive (LID)

La doctrine de lutte informatique défensive (LID) au sein du ministère des Armées regroupe l'ensemble des actions conduites pour faire face à un risque, une menace ou à une cyberattaque réelle. Elle couvre principalement les missions « anticiper, détecter et réagir » et complète les missions « prévenir, protéger et attribuer ».

Cette doctrine permet d'unifier et de centraliser la chaîne défensive mais également de



La lutte informatique d'influence

La lutte informatique offensive

favoriser les synergies et d'offrir une vision globale. Ce processus permet une mobilisation rapide des moyens et des compétences disponibles tout en garantissant une cohérence d'ensemble de nos actions. Elle permet également de renforcer la Posture permanente de cyberdéfense (PPC), créée par la loi de programmation militaire 2019-2025. Assurée par le commandement de la cyberdéfense (COMCYBER), cette posture permet de protéger 7 jours sur 7 et 24 heures sur 24 tous les réseaux du ministère des Armées afin d'anticiper et réagir à toute attaque contre les intérêts de notre Défense.

B/ La lutte informatique offensive (LIO)

La lutte informatique offensive à des fins militaires (LIO) recouvre l'ensemble des actions entreprises dans le cyberespace, conduites de façon autonome ou en combinaison des moyens militaires conventionnels. L'arme cyber vise, dans le strict respect des règles internationales, à produire des effets à l'encontre d'un système adverse pour en altérer la disponibilité ou la confidentialité des données.

C/ La lutte informatique d'influence (L2I)

La lutte informatique d'influence (L2I) désigne les opérations militaires conduites dans la couche informationnelle du cyberespace pour détecter, caractériser et contrer les attaques, renseigner ou faire de la déception, de façon autonome ou en combinaison avec d'autres opérations.

La guerre de l'information est partie intégrante de toute stratégie militaire : sans capacité à convaincre et à contrer l'influence adverse, tout engagement militaire est voué à l'échec. L'avènement des réseaux sociaux a renforcé ce postulat, accélérant considérablement la circulation d'informations vraies ou fausses et augmentant dans le même temps le volume, la portée et la résonance de ces informations. Des agresseurs potentiels disposent ainsi de la capacité à mobiliser rapidement la violence, en parole et en actes, et à fragiliser la légitimité des différents acteurs du règlement d'une crise. La guerre de l'information s'est déployée dans

La recherche des cyber combattants

Manoeuvres pour les soldats du numérique

le cyberespace, y trouvant un terreau particulièrement fertile.

D/ Droit international appliqué aux opérations dans le cyberespace

Porté par le commandement de la cyberdéfense (COMCYBER) et la Direction des affaires juridiques (DAJ), en lien avec la Direction générale des relations internationales et de la stratégie (DGRIS), un rapport précise la position française sur l'application du droit international aux opérations militaires dans le cyberespace. Il conforte l'engagement constant de la France en faveur du respect du droit international existant, y compris dans le domaine cyber.

Ce rapport poursuit 3 objectifs :

- éclairer les travaux des experts gouvernementaux réunis par l'organisation des Nations Unies, qui vont s'ouvrir pour un nouveau cycle de discussions ;
- rappeler et illustrer l'application du droit international, dont la Charte des Nations Unies et le droit international humanitaire à l'usage des technologies de l'information et de la communication en temps de paix et en temps de conflit armé ;
- réduire les risques d'incompréhension ou d'escalade non maîtrisée et contribuer à une lecture du corpus juridique existant cohérente avec l'objectif d'un cyberespace pacifique et sûre.

Officier expert en cyber sécurité

CENTRE D'EXCELLENCE CYBERDEFENSE AEROSPATIALE

Cahier spécial réalisé par Gilbert Robinet pour le numéro 137 de la revue ***ENGAGEMENT*** de l'ASAF - (www.asafrance.fr) Source : https://www.defense.gouv.fr/ema/nos-organismes/comcyber/le-commandement-de-la-cyberdefense/comcyber