Le cyberespace

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.

La cyberdéfense : enjeu majeur pour le ministère des Armées

Les questions de surveillance, de défense et de sécurité dans l'espace numérique posent aujourd'hui de nombreux défis au ministère des Armées. Le ministère est en effet responsable des systèmes les plus stratégiques, ceux liés à la dissuasion nucléaire, mais également des systèmes d'armes sophistiqués : aéronefs de combat ou de transport, navires de surface ou sous-marins, véhicules de combat terrestres. Il doit pouvoir fonctionner en sécurité dans un environnement de plus en plus numérisé et assurer les engagements opérationnels en dépit des éventuelles attaques subies par les systèmes. Une atteinte aux systèmes d'information pourrait poser une question de souveraineté majeure en cas de prise de contrôle ou de paralysie de secteurs vitaux pour l'État.

Érigée au rang de priorité nationale par le Livre blanc pour la Défense et la Sécurité nationale de 2013, la cyberdéfense représente un enjeu majeur pour le ministère des Armées. Aujourd'hui, toute opération militaire comporte un volet cyber. Au même titre que la terre, la mer, l'air et l'espace, l'espace numérique constitue un milieu à part entière dont la défense est une nécessité permanente. Pénétration des réseaux à des fins d'espionnage, prise de contrôle à distance, destruction d'infrastructures vitales, les types de menaces sont nombreux.

La cyberdéfense regroupe l'ensemble des activités conduites afin d'intervenir militairement ou non dans le cyberespace pour garantir l'effectivité de l'action des forces armées, la réalisation des missions confiées et le bon fonctionnement du ministère. La cyberdéfense est à différencier de la cybercriminalité qui correspond à l'ensemble des crimes et délits traditionnels ou nouveaux réalisés, via les réseaux numériques.

Le commandement des forces de cyberdéfense des armées françaises : COMCYBER

Crée en 2017, le **COMCYBER** est l'unité opérationnelle commandant, de façon organique ou fonctionnelle, l'ensemble des forces de cyberdéfense des armées françaises. Placé sous l'autorité directe du chef d'état-major des Armées, le COMCYBER est responsable de la manœuvre cyber globale. Il a pour missions :

• la protection des systèmes d'information placés sous la responsabilité du chef d'état-major des Armées en sa qualité d'autorité qualifiée pour la sécurité des systèmes d'information ;

• la conduite de 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 conception, la planification et la conduite des opérations militaires de cyberdéfense, sous l'autorité du sous-chef d'état-major « opérations » ;

• la contribution à l'élaboration de la politique des ressources humaines de cyberdéfense ;

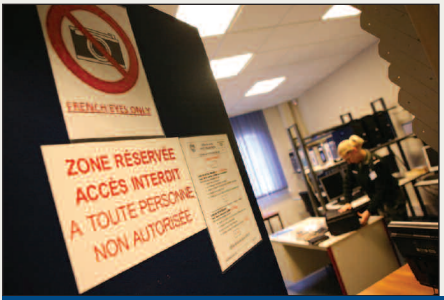
• la contribution des armées et organismes interarmées à la politique nationale et internationale de cyberdéfense, notamment pour l'élaboration et la mise en œuvre des plans de coopération ;

• la définition des besoins techniques spécifiques de cyberdéfense ;

• la cohérence du modèle de cyberdéfense du ministère et sa coordination générale ;

• le développement et l'animation de la réserve de cyberdéfense.

Le pôle breton de la cyberdéfense



Le CALID *des ordinateurs et des hommes*

Le COMCYBER exerce une tutelle opérationnelle sur près de 3 400 cyber-combattants au sein du ministère. Pour l'exercice de ses missions, il dispose d'un état-major et a autorité sur trois organismes interarmées : le **CALID**, le **CASSI** et le **CPROC**.

Le CALID

Le centre d'analyse en lutte informatique défensive (CALID) est le centre opérationnel expert en lutte informatique défensive. Il pilote 24 heures sur 24 la détection, le traitement et la réponse aux cyberattaques. Le CALID comprend également des capacités d'expertise de haut niveau. Il se déploie en France et à l'étranger, en prévision ou en réaction à une crise.

Éléments clés :

- date de création : 2006
- statut : organisme interarmées (OIA) rattaché au COMCYBER à partir de janvier 2019
- basé à : Paris et à Rennes.

Missions

Le CALID a pour mission de défendre l'espace numérique des armées (réseaux informatiques, systèmes de combat, de commandement, etc.) contre les menaces et attaques qui le visent. Il anticipe les menaces et attaques potentielles, surveille les réseaux pour détecter ces attaques puis agit pour les contrer et préserver les missions opérationnelles qui dépendent de ces systèmes.

- Il vérifie ou évalue la qualité, l'efficacité et la cohérence des dispositifs mesurés et procédures de sécurité ;
- il déploie des sondes sur les systèmes d'arme et de commandement en opérations, va rechercher des traces d'attaque sur des systèmes d'information ;
- il coordonne des groupes d'action spécialisée ou les actions des administrateurs de réseau.

Le CASSI

Le centre d'audits de la sécurité des systèmes d'information (CASSI) est un centre national

Le COMCYBER

Construction du bâtiment cyberdéfense à Rennes

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.

Éléments clés :

• date de création : 2008

• statut : organisme interarmées rattaché au COMCYBER à partir de janvier 2019

• basé à : Maisons-Laffitte, Brest, Orléans, Toulon & Rennes.

Missions

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 inclut un diagnostic menant à des recommandations. Les équipes d'audit doivent :

• vérifier ou évaluer la qualité, l'efficacité et la cohérence, des dispositifs mesurés et procédures de sécurité ;

• mettre en évidence les vulnérabilités résiduelles.

Le CPROC

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

Éléments clés :

• date de création : 2015

• statut : organisme interarmées rattaché au COMCYBER depuis juin 2017

• basé à : Saint-Cyr-Coëtquidan et Paris puis Rennes à partir de 2019.

Missions

Il s'occupe du recrutement, de la gestion et de l'entraînement des réserves de cyberdéfense. Le CRPOC, en lien avec le COMCYBER et les armées, s'occupe également du montage d'exercices nationaux et internationaux de

Un BTS de cyberdéfense au lycée militaire de Saint-Cyr-l'École

cyberdéfense, tels que :

• l'exercice annuel interarmées DEFNET, qui met en œuvre un scénario réaliste et dynamique afin de tester la coordination entre les différentes entités du ministère en cas d'attaque cyber majeure ;

• l'exercice OTAN *Lock Shields*, qui réunit de nombreuses nations et a pour objectif d'évaluer les capacités à défendre un réseau informatique complexe face à des cyberattaques menées par un État fictif.

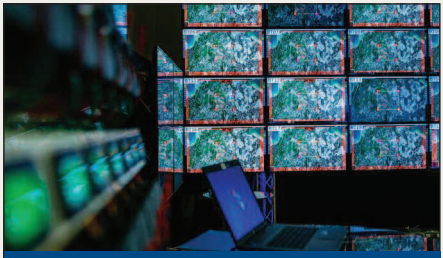
Recrutement

Le ministère a lancé un recrutement ambitieux de « combattants numériques » pour soutenir les missions de renseignement, de protection, de défense et d'action dans l'espace numérique. Au terme de la montée en puissance prévue par la loi de programmation militaire, 3 200 personnes participeront à la mission cyber en 2019, soit plus du double des effectifs qu'en 2012.

Le ministère recrute ses nouveaux combattants numériques : des hommes et des femmes passionnés par le numérique, de tous niveaux, de tous profils.

Le recrutement s'effectue sous différents statuts (militaire, civil, réserviste), à tout type de niveau 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, telles que



Un exercice de cyberdéfense à l'OTAN en 2017

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 émergentes préoccupant ;
- protéger et défendre un des réseaux informatiques les plus étendus de France (plus de 180 000 machines) ;
- mener des opérations ;
- la possibilité d'intervenir dans le monde entier ;

Des élèves ingénieurs formés à la cyberdéfense

Le général Olivier Bonnet de Paillerets

- une carrière permettant d'acquérir de nouvelles compétences très appréciées dans le secteur privé.

Combattant numérique : pourquoi pas vous ?

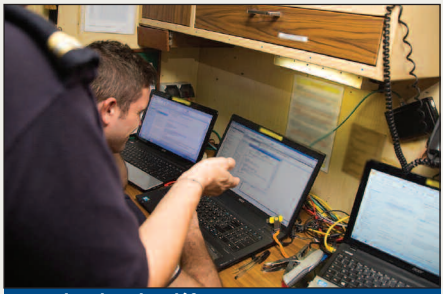
Le ministère des Armées développe ses capacités et offre de nouvelles opportunités professionnelles. Sécurité des systèmes d'information, défense contre les cyberattaques, opérations pour agir dans l'espace numérique, de nombreux postes civils (CDD et CDI) et militaires (de carrière ou sous contrat)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

Si vous avez envie d'innover, d'encadrer ou d'exploiter votre expertise technologique, pour la défense des intérêts numériques de votre pays, ces postes sont pour vous.

Un recrutement ambitieux de « combattants numériques » d'ici 2019 est lancé pour soutenir les missions de renseignement, de protection, de défense et d'action dans le cyberespace.

Les profils recherchés sont divers, expert ou manager, premier emploi ou au titre d'un parcours professionnel diversifié atour des compétences suivantes :

• ingénierie logicielle (expression du besoin, conception, développement, etc.) ;
• administration système et sécurité ;
• sécurité des systèmes d'information (assistance, conseil, expertise) ;
• évaluation des systèmes (audit, test d'intrusion, Red team, ...) ;


Exercice de cyberdéfense

Exercice national en 2016

• lutte informatique défensive (évaluation de la menace cyber, analyse de traces et supervision dans les SOC, forensic, reverse engineering, ...) ;
• veille sur les réseaux sociaux.

Les spécialistes ou experts cyber : devenez cyber-combattant au sein du ministère des Armées

Le ministère des Armées vous offre l'opportunité de servir votre pays et de garantir sa souveraineté en contribuant aux opérations militaires dans le cyberespace.
Pour cela, 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 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.
Ces postes couvrent un large spectre d'activités et requièrent des expertises variées :
• ingénierie logicielle (développement, reverse engineering,...) ;
• évaluation des systèmes (audit, test d'intrusion, Red team, ...) ;
• lutte informatique défensive (analyse de traces et supervision dans les SOC, investigation numérique, ...) ;
• veille sur les réseaux sociaux et anticipation des menaces ;
• actions numériques dans le cyberespace.
Les postes à pourvoir sont majoritairement localisés en région Ile-de-France et en région Bretagne.

Au service de l'État

Être militaire, c'est servir l'État. Cela implique des qualités humaines, de la rigueur, de la disponibilité et le sens des responsabilités. En étant militaire, vous pourrez participer aux opérations de sécurité en France ou à l'étranger.
Conditions pour le recrutement :
• être de nationalité française ;
• répondre aux limites d'âge selon le grade pour lequel le candidat est recruté.
• aptitude médicale au recrutement de militaire commissionné.

Devenez cyber-combattant au sein du ministère des Armées.
Envoyez vos CV à l'adresse internet suivante :
sga-cyber.contact.fct@def.gouv.fr

La réserve de cyberdéfense

La réserve de cyberdéfense : assister l'État et les armées en cas de crise numérique majeure

Le Livre blanc sur la Défense et la Sécurité nationale de 2013 a prescrit le développement d'une réserve à vocation opérationnelle activable en cas de crise majeure, portée par le ministère des Armées. L'actualisation de la Loi de programmation militaire pour les années 2014 à 2019 ordonne son développement.

Placé sous le commandement national de l'officier général cyberdéfense, la réserve de cyberdéfense a pour mission de contribuer à la résilience de la nation. Elle peut agir au profit non seulement du ministère des Armées mais également de l'agence nationale de la sécurité des systèmes d'information ou du ministère de l'Intérieur.

Sa composition

Lancée en mai 2016, la réserve de cyberdéfense se compose d'un réseau de volontaires organisé en unités militaires réparti en cellules régionales, sur l'ensemble du territoire. Elle est encadrée par des réservistes des forces armées

Des réservistes cyberdéfense

et par du personnel de l'État.

Cette réserve d'un nouveau genre allie à la fois des réservistes citoyens, des réservistes opérationnels et des militaires d'active.

Son périmètre d'intervention

Les interventions porteraient principalement sur les réseaux des opérateurs d'importance vitale, des administrations, des collectivités locales, des grands services publics et de leur sous-traitants, notamment s'il s'agit de PME n'ayant pas les moyens de rétablir un niveau de cybersécurité acceptable. Certaines équipes de l'échelon d'urgence seront habilitées à un niveau secret défense, pour pouvoir intervenir sur les réseaux classifiés.

Cela se traduit par :

- l'appui à la planification et à la conduite de la chaîne opérationnelle de cyberdéfense, sur le territoire national ;
- fournir un complément ponctuel d'expertise ;
- le déploiement de groupes d'intervention rapide sur le territoire national ;
- l'analyse de l'incident, des conséquences et proposer

Première journée des réservistes cyberdéfense

des mesures de remédiation ;

• le déploiement d'équipes de reconstruction de réseaux.

Devenir réservistes de cyberdéfense

La réserve de cyberdéfense recrute tout au long de l'année des spécialistes dans le domaine informatique, réservistes opérationnels ou citoyens. La réserve recherche différents profils : coordinateurs, experts, analystes, techniciens ; à différents niveaux : d'étudiants en 1ère année en informatique jusqu'à BAC + 5.

Le **réserviste opérationnel** souscrit un engagement à servir dans la réserve opérationnelle, un contrat rémunéré d'une durée de 1 à 5 ans renouvelable. Ces volontaires font le choix de servir leur pays sans faire du métier des armes leur seule profession.

Les **réservistes citoyens** sont des collaborateurs bénévoles du service public. Ils choisissent de servir leur pays en faisant bénéficier la Défense de leur expertise et leur compétence. En tant que bénévole, ils consacrent le temps qu'ils souhaitent et peuvent, à cette mission.

Les conditions générales pour devenir réserviste :

• être de nationalité française et résider en France ;

• avoir plus de 17 ans ;

• faire des études en informatique ;

• être en règle au regard des obligations du service national ;

• ne pas avoir de casier judiciaire.

Mots clés :

Cyberespace : le cyberespace est un domaine global constitué du réseau maillé des infrastructures des technologies de l'information (dont Internet), des réseaux de télécommunication, des systèmes informatiques, des pro-

14 juillet 2018, premier défilé des cyber-combattants

cesseurs et des mécanismes de contrôle intégrés. Il inclut l'information numérique transportée ainsi que les opérateurs de services en ligne.

Cyberattaques : acte malveillant de piratage informatique dans le cyberespace. Les cyberattaques peuvent être l'action d'une personne isolée, d'un groupe, d'un État. Elles incluent la désinformation, l'espionnage électronique qui pourrait affaiblir l'avantage compétitif d'une nation, la modification clandestine de données sensibles sur un champ de bataille ou la perturbation des infrastructures critiques d'un pays (eau, électricité, gaz, communication, réseaux commerciaux). La cyberdéfense du ministère vise à détecter et contrer les cyberattaques dont la cible et la finalité sont liées au ministère des Armées.

Remise de l'insigne d'expert en cyberdéfense

Cahier spécial réalisé par Gilbert Robinet pour le numéro 122 de la revue *ENGAGEMENT* de l'ASAF - (www.asafrance.fr) source : www.defense.gouv.fr