ESCADRON DES SYSTÈMES D'INFORMATION OPÉRATIONNELS ET DE CYBERDÉFENSE

REGARD SUR LA CYBERDÉFENSE

Opérant depuis des années sur des systèmes d'information complexes, l'Armée de l'air a capitalisé une solide culture cyber.

Pénétration des réseaux à des fins d'espionnage, prise de contrôle à distance, destruction d'infrastructures vitales, autant de menaces qui démontrent l'utilité d'experts dédiés à la cyberdéfense dans l'Armée de l'air.

*Par l'**adjudant Jean-Laurent Nijean***

Ukraine, juin 2017. Il est 10 h 30 et une cyberattaque d'une ampleur effroyable est en cours. En quelques heures à peine, un logiciel malveillant se répand à une vitesse alarmante dans les réseaux informatiques du pays, puis à l'étranger. Sur les ordinateurs affectés, un message en lettres rouges annonce que les données des utilisateurs sont chiffrées et qu'elles ne pourront être débloquées qu'en échange d'une rançon de 300 dollars. Baptisé « NotPetya », ce logiciel n'avait pas pour objectif l'extorsion de fonds, mais la destruction pure et simple des données informatiques. Les banques et des magasins sont contraints de fermer leurs portes. Les distributeurs de billets de banque sont hors service. Les transports en commun sont fortement perturbés. Des médias, télévision et radio, ne peuvent plus émettre. De même, les ordinateurs de plusieurs ministères sont infectés. Ce scénario catastrophe n'est malheureusement pas de la science-fiction, il est basé sur un fait authentique. Les questions de surveillance, de défense et de sécurité dans l'espace numérique sont autant de défis pour le ministère des Armées aujourd'hui. Celui-ci 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 (SI) pourrait poser un problème de souveraineté majeur en cas de prise de contrôle ou de paralysie de secteurs vitaux pour l'État. Le *Livre blanc sur la Défense et la sécurité nationale* de 2013 a ainsi fait de la cyberdéfense une priorité nationale. En 2017, la création d'une structure opérationnelle, le commandement de la cyberdéfense (ComCyber), donne un nouvel essor à ce domaine. 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, ou cyberespace, constitue un milieu à part entière dont la défense est une nécessité. « *Nous menons une posture permanente de surveillance du cyberespace pour augmenter la réactivité et prévoir les menaces* », explique le commandant Lucas, chargé des relations internationales au ComCyber.

La cyberdéfense, une priorité nationale

Le cyberespace au service des opérations aériennes

Depuis longtemps, l'Armée de l'air développe et opère des systèmes d'information et de communication particulièrement complexes, tant en France qu'à l'extérieur du territoire national, supports essentiels des opérations militaires. Elle est responsable des systèmes les plus stratégiques, ceux liés à la dissuasion nucléaire, à la posture permanente de sûreté, mais également à la conduite des opérations aériennes et aux systèmes d'arme sophistiqués comme les aéronefs de combat ou de transport, les drones et les radars de détection. Elle a acquis de solides connaissances en matière de sécurité des systèmes d'information. Au sein de l'Armée de l'air, l'escadron des systèmes d'information opérationnels et de cyberdéfense (ESIOC), également appelé centre air d'expertise cyberdéfense, de la base aérienne 118 de Mont-de-Marsan constitue le point focal technique de la lutte informatique défensive, du suivi du maintien en condition de sécurité et de la supervision opérationnelle de la sécurité des systèmes métiers de l'Armée de l'air. En matière de cyberdéfense, cet escadron assure des missions de lutte informatique défensive (LID), d'expertise en réponse à incident et de maintien en condition de sécurité (MCS) consécutives à la détection de vulnérabilités. Il est également amené à réaliser des analyses de sécurité dans le cadre de la recherche de vulnérabilités conceptuelles. *«Le cyberespace au service des opérations aériennes»*: c'est la devise de l'unité. *«Au travers de l'ESIOC, nous pouvons voir que l'Armée de l'air appréhende parfaitement l'importance des systèmes d'information pour la réalisation de ses missions»*, explique le lieutenant-colonel Ludovic, commandant en second de l'ESIOC. L'originalité de l'unité est de regrouper tous les métiers de l'informatique, (développeur, expert cyber, analyste, assistance à maîtrise d'ouvrage, administrateur, etc.). *«Nous sommes focalisés sur les SI qui concourent directement aux opérations aériennes*, précise le capitaine Baptiste, commandant le département cyberdéfense de l'ESIOC. *Ces experts, opérant dans le cœur de métier de l'Armée de l'air, permettent d'optimiser la réactivité.»* Cette interaction et cette complémentarité entre les différents métiers font la force de l'unité. *«Notre organisation nous permet d'assurer trois missions complémentaires, l'ingénierie logicielle pour le développement de SI opérationnels tournés vers la mission aérienne, l'appui aux opérations, véritable service après-vente des systèmes mis en œuvre sur le territoire national comme en opérations, et pour finir la cyberdéfense, domaine en plein essor»*, explique le commandant en second. À l'ère du *Big data*, l'appui aux opérations fournit des moyens de calcul et de stockage pour l'ensemble de l'ESIOC. La réunion de ces trois missions donne une grande réactivité à l'unité. *«Lorsque nous devons, par exemple, mettre un système d'information en supervision*, précise le capitaine Sacha. *Cela nécessite de l'espace serveur et des ressources en calcul pour traiter de gros volumes de données.»* De plus, le département «appui aux opérations» partage l'expertise qu'il détient sur certains SI dont il assure le soutien. Les spécialistes cyber ont directement accès à leur savoir-faire. En effet, lorsqu'une alerte remonte, consulter les spécialistes du SI concerné permet de déceler rapidement les faux positifs (fausse alerte). Le département «ingénierie logicielle», qui a notamment développé les logiciels Alliance (pour le DACAS, appui aérien rapproché numérisé) ou Melissa (pour la préparation de mission), est particulièrement sensibilisé au risque cyber. Il fournit des outils au profit de la cyberdéfense,

Capitaine Baptiste
Commandant le département cyberdéfense
À l'ESIOC, nous avons fait le choix de sélectionner notre personnel plutôt que de le recruter aléatoirement lors du plan annuel de mutation. Les candidats doivent passer un test de sélection. Ils doivent être avant tout passionnés et capables d'assimiler d'importantes connaissances techniques.

Des capacités de stockage et de calcul au service de l'ensemble de l'ESIOC.

Les experts surveillant depuis le centre opérationnel de sécurité.

Analyse fine d'un système d'information infecté dans une salle dédiée.

Adjudant Christophe
Technicien cyberdéfense
Nous augmentons le niveau de sécurité, mais le système parfait n'existe pas. Il y a toujours des vulnérabilités qui sont découvertes de temps en temps. Il faut des experts capables de surveiller, détecter les intrusions et intervenir pour repousser l'attaquant.

CYBER DÉFINITIONS

Cyberdéfense: 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 et le bon fonctionnement du ministère.
Cyberespace: domaine constitué du réseau maillé des infrastructures des technologies de l'information, des réseaux de télécommunication, des systèmes informatiques, des processeurs et des mécanismes de contrôle intégrés. Il inclut l'information numérique transportée et les opérateurs de services en ligne.
Cyberattaque: acte malveillant de piratage informatique dans le cyberespace. Elles peuvent être l'action d'une personne isolée, d'un groupe ou d'un État. Elles incluent la désinformation, l'espionnage électronique, la modification de données sensibles sur un champ de bataille ou la perturbation des infrastructures critiques (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.

LA CHAÎNE OPÉRATIONNELLE CYBER

Le volet opérationnel de la chaîne de cyberdéfense de l'Armée de l'air est placé sous l'autorité de l'officier lutte informatique défensive (OLID) de l'Armée de l'air, affecté au commandement de la défense aérienne et des opérations aériennes (CDAOA).
Il s'appuie sur :
- le centre air de conduite cyberdéfense (CACC) pour conduire les opérations cyber. Le CACC est également chargé de l'entraînement des forces dans le domaine. Chaque année, il organise une dizaine d'exercices pour entraîner les différents acteurs de la chaîne cyber ;
- l'escadron des systèmes d'information opérationnels et de cyberdéfense (ESIOC), l'unité tactique qui met en œuvre le centre opérationnel de sécurité (SOC) de l'Armée de l'air et qui déploie ses experts.
- un vivier de personnes formées à la cyberdéfense réparties dans différentes unités de l'Armée de l'air et contribuant au dispositif d'alerte.

à l'instar de Pavensis, un référentiel de données qui permet de décrire l'ensemble des SI que l'on doit défendre dans l'Armée de l'air. *« Il faut décrire chaque SI avec l'ensemble des briques qui le composent. Sur chaque brique, des vulnérabilités peuvent être décelées. L'industriel émet alors des correctifs,* explique le capitaine Sacha. *L'application permet de dresser l'état de sécurité des SI en présentant l'ensemble des vulnérabilités et leurs correctifs. »* Aujourd'hui, plusieurs centaines de systèmes d'information métier de l'Armée de l'air sont recensées dans l'application. *« Nous faisons également des études de sécurité pour défendre les systèmes,* reprend le capitaine. *Nous faisons des tests de robustesse pour chercher des failles. C'est indispensable pour pouvoir les protéger efficacement. »*

Cybersurveillance des systèmes d'information

Dès l'apparition de *malwares* comme le logiciel NotPetya, les experts comblent les failles de sécurité qui pourraient être exploitées sur un SI donné. Ce dispositif de LID est interarmées, il y a une chaîne pilotée par le ComCyber à l'aide de son centre d'opération. L'échelon interarmées est représenté par le CALID (centre d'analyse et de lutte informatique défensive). *« Sur le plan opérationnel, nous assurons la conduite des opérations de lutte informatique défensive (LID),* explique le lieutenant-colonel Christine, commandant le CALID. *Un centre de surveillance et de détection supervise les réseaux 24 h/24, via d'autres entités comme l'ESIOC, situées dans les armées. »*

Le premier objectif de la cyber est de cartographier les SI et de les évaluer. *« Nous faisons, dans un deuxième temps, sur un périmètre plus restreint, la cybersurveillance des systèmes les plus critiques,* explique le commandant en second. *Nous plaçons des moyens de surveillance (sondes) au plus près de ces systèmes. Les opérateurs qui se trouvent au SOC* (Security Operation Center - *centre opérationnel de sécurité) vont alors voir des alarmes remonter. »*

Lorsque le SOC détecte une alerte, il la transmet via le centre d'opérations cyber qui va solliciter le centre air de conduite cyberdéfense (CACC). Le CACC déclenche alors l'envoi d'un groupe d'intervention rapide (GIR) de l'ESIOC. Deux sous-officiers et un officier d'astreinte sont déployés pour intervenir sur le système. Ils agissent un peu comme la police scientifique sur une scène de crime. Le GIR effectue des prélèvements : disque dur, mémoire vive. Les trois hommes vont diagnostiquer la panne et voir ce qui s'est passé. Les assaillants sont-ils toujours dans le système ? Comment ont-ils procédé ? La réponse à ces questions permet de conseiller l'officier LID de l'Armée de l'air. *« Il faut déterminer l'impact sur le SI et mettre tout en œuvre pour poursuivre la mission,* explique l'adjudant Christophe. *Puis, à froid, nous analysons ces prélèvements pour savoir ce qui s'est passé. Nous agissons en lien direct avec le CALID. »*

Pour pouvoir faire face aux menaces, ces combattants du numérique doivent se former et s'entraîner, notamment lors d'exercices comme Defnet (voir encadré). Ces experts conçoivent également des exercices et des campagnes de *« phishing »* sur Intradef avec de faux virus pour sensibiliser le personnel de l'Armée de l'air aux risques.

« Nous sommes jumelés avec le 591 Signals Unit (591 SU), *l'unité spécialisée dans la cyberdéfense de la* Royal Air Force, précise le lieutenant-colonel Ludovic. *Régulièrement, nous organisons des entraînements ou des échanges avec eux afin d'être interopérables et d'être en mesure de mener des interventions conjointes si nécessaire. »* ■

Vision des alarmes lors d'un exercice au centre opérationnel de sécurité.

Un expert prélève les données d'un smartphone.

LES CYBERGUERRIERS EN ACTION

« DEFNET 2018 »

L'exercice « Defnet » s'est déroulé du 12 au 24 mars sur différents sites militaires et dans les écoles et établissements d'enseignement supérieur à Paris. Focus sur les combattants du numérique de l'Armée de l'air.

Base aérienne 118 de Mont-de-Marsan, une patrouille de Rafale rentre de vol. Le mécanicien récupère les données liées au vol. Il insère la carte dans le lecteur du système logistique du Rafale. Après un certain temps, le mécanicien détecte des anomalies. La procédure est alors en marche. La chaîne de sécurité des systèmes d'information est saisie. Un groupe d'intervention rapide est dépêché sur les lieux de l'incident. En attendant le dénouement de l'enquête, la flotte est clouée au sol.

Prise de contrôle à distance, compromissions, bascule de réseaux, etc. Depuis cinq années, l'ensemble du personnel spécialisé des armées françaises s'exerce au combat numérique. Fondé sur un scénario réaliste et dynamique, « Defnet » permet d'améliorer la coordination entre les différents participants des trois armées, directions et services, en cas d'attaque cyber majeure. Dans un contexte international fictif, les spécialistes cyber des armées doivent répondre à près de 40 incidents cyber visant plusieurs systèmes d'information (SI), dont cinq plateformes de simulation reproduisant des SI militaires et des automates industriels embarqués sur des équipements opérationnels.

S'exercer au combat numérique

« Nous avons eu l'idée d'un scénario que nous avons élaboré à deux techniciens, explique l'adjudant Christophe, animateur technique lors de « Defnet 2018 ». *Nous avons mis deux mois, entre la conception du scénario, la mise en œuvre du système d'information sur lequel nous allons jouer l'exercice, la réalisation des tests de l'attaque et l'exécution de l'attaque pour la préparation de l'exercice. »* La plus grosse difficulté est de trouver le vecteur d'attaque sur le SI concerné. Le système a été imposé par la direction de l'exercice, sous l'autorité du ComCyber. *« Nous avons eu la chance d'avoir l'équipe de l'administration du SI concerné au rez-de-chaussée du bâtiment,* explique l'adjudant. *Nous avons fait le montage de la plateforme en collaboration avec eux. Puis nous avons mis notre expertise en œuvre. »* ■

Joueurs et animateurs travaillant lors de l'exercice « Defnet 2018 ».