Retour sur la genèse de la cyberdéfense militaire française

Par le Général de division aérienne **Didier TISSEYRE**
Officier général commandant de la cyberdéfense

Introduction

Il y a cinquante ans, en 1969, la DARPA [1] déployait aux États-Unis le réseau ARPAnet [2], dédié aux forces armées américaines. Vingt ans plus tard, ARPAnet laissait la place à Internet et au *World Wide Web*. Ainsi, la numérisation (ou *digitisation*) du monde débute autour du plus vaste « objet » artificiel créé par l'homme au XX^{e} siècle : le cyberespace. L'espace numérique, ou cyberespace, est un domaine d'innovation et de confrontation à la fois nouveau et en constante évolution. Nouveau, il nécessite d'être enraciné de façon solide pour continuer à se développer, tout en assurant la sécurité et la protection de ceux qui y opèrent ; en évolution constante, il requiert une approche agile et la remise à plat de nos organisations et de nos rapports de pouvoir.

Depuis 2011, le ministère de la Défense, puis des Armées, et en particulier le Commandement de la cyberdéfense, son bras armé, construisent de façon solide et pérenne un modèle agile et efficace de cyberdéfense.

Le cyberespace a sa propre dynamique, liée à une expansion technique qui semble ne pas connaître de limite : hier l'interconnexion des réseaux, aujourd'hui le développement des puissances de calcul dans l'exploitation des données, demain l'explosion du nombre d'objets connectés, après-demain les processeurs quantiques. Internet constitue probablement la révolution technique humaine la plus innovante : il est source de richesses et vecteur de connaissances, ainsi que de nouveaux modèles économiques et culturels. Il raccourcit les distances et rapproche les individus. Le centre de gravité de nos sociétés, jusqu'alors essentiellement lié à des populations et à des territoires, se déplace progressivement dans ce nouvel espace. La dépendance au numérique s'accroît au rythme des progrès techniques et renforce par là même l'exposition à des vulnérabilités nouvelles.

La plupart des luttes de pouvoir, des crises et des conflits contemporains connaissent désormais, et ce, systématiquement, un développement dans le cyberespace. Les armées doivent appréhender le combat cybernétique comme une fonction stratégique à part entière dont les effets se combinent aux autres dans une manœuvre globale.

Un nouvel espace de confrontation

Véritable rupture en termes de technologie et d'emploi de la force, l'arme cyber est amenée à bouleverser les modalités de la guerre sans en renouveler profondément les principes. Multiplicité d'acteurs étatiques, masqués ou non, organisations terroristes ou criminelles, frontières gommées, perceptions troublées, repères faussés, propagation rapide, droit international non respecté, code de conduite bafoué : tels sont les risques du cyberespace. Une zone grise, un brouillard, dont les effets sont, eux, bien réels, parfois dévastateurs. Le combat dans le cyberespace est de nature asymétrique, hybride, parfois invisible et en apparence indolore. Pourtant, l'emploi de l'arme

(1) *Defense Advanced Research Projects Agency.*
(2) *Advanced Research Projects Agency Network.*

cyber est susceptible de porter gravement atteinte aux capacités et aux intérêts souverains des États.

Nous pouvons aujourd'hui définir quatre grandes catégories de cybermenaces : l'atteinte à l'image (défigurations de sites officiels, campagnes de dénigrement, usurpation d'identité, propagande, amplification de rumeurs, déstabilisation…), l'action « mafieuse » (arnaques à la carte bancaire, rançons, trafics en tous genres…), l'espionnage (détournements discrets d'informations circulant sur les réseaux numériques d'une cible) et le sabotage (altération du fonctionnement d'un système par le biais d'une attaque informatique).

Ces menaces, qui naissent dans le cyberespace, ont les mêmes caractéristiques que celles de l'espace physique : des individus malfaisants préparent des actes terroristes, désinforment, leurrent, volent ou encore détruisent. Les frontières qui séparent ces acteurs (cybercriminels, hacktivistes, États, groupes terroristes, etc.) sont poreuses et la diversité des menaces qu'ils génèrent est extrêmement grande, allant de l'attaque sur un système de vote électronique à la paralysie de médias, en passant par l'extinction d'un système électrique. Ces scénarios s'appuient sur des réalités profondément asymétriques : de faibles moyens permettent d'obtenir des effets stratégiques, analogues à ceux d'actions plus conventionnelles, en particulier lorsqu'ils visent des infrastructures civiles critiques, ou des capacités militaires cruciales dont dépend notre souveraineté.

La fréquence et l'ampleur des attaques augmentent sans cesse dans le cyberespace, témoignant d'une prolifération préoccupante des moyens d'agression. Si peu d'États disposent pour l'heure des moyens de mener des actions cyberoffensives de grande ampleur, causant des dommages importants, leur nombre et leurs capacités devraient s'accroître rapidement, favorisés par le faible coût et par la diffusion rapide des technologies numériques. Ensuite, l'arme cyber d'État, dont la conception nécessite parfois des moyens colossaux, est susceptible d'être copiée et répliquée très facilement. Utilisant déjà Internet à des fins de planification, de propagande et de recrutement, les groupes terroristes pourraient devenir des acteurs à part entière du domaine cyber. Il existe, enfin, une réelle difficulté dans la détermination de l'origine des attaques.

Une montée en puissance rapide

Pour protéger, défendre et agir face à ces cybermenaces, la cyberdéfense française s'est construite grâce à la volonté gouvernementale et à sa prise en compte dans les lois de programmation militaire successives. Confrontée à des adversaires, des ennemis ou des concurrents dotés de capacités informatiques offensives, la France a bénéficié d'un ambitieux plan d'actions ministériel, fondé sur une doctrine et une organisation renouvelées, permettant à nos forces de se déployer et de conduire, face à cette menace, le combat numérique.

Le Livre blanc de la Défense et de la Sécurité nationale de 2008 avait fait état pour la première fois de la menace posée par le développement du cyberespace. La création de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a suivi en 2009, puis celle du poste d'officier général de cyberdéfense au sein de l'état-major des armées en 2011. La structure de cyberdéfense n'a ensuite cessé, tout au long de ces huit années, de se développer pour s'adapter aux nombreux enjeux opérationnels. Le Livre blanc de 2013 est venu préciser qu'au sein de la doctrine nationale, la capacité informatique offensive, associée à une capacité de renseignement, concourt de façon significative à la posture de cybersécurité.

Le Pacte Défense Cyber 2014-2016 a ensuite mobilisé le ministère des Armées dans l'objectif de faire de la France une grande puissance militaire de la cyberdéfense et de faire émerger une communauté nationale de cyberdéfense. Le « changement d'échelle » annoncé souligne la nécessité d'industrialiser la cyberdéfense militaire de la France. En octobre 2015 est créé le centre

des opérations de cyberdéfense (CO CYBER), qui a pour mission de planifier et de conduire les opérations militaires dans le cyberespace.

Le chemin accompli en une décennie est à la mesure de l'enjeu et des ambitions de la France de devenir une grande puissance cyber.

Le COMCYBER, Commandement de la cyberdéfense

Cette montée en puissance franchit un seuil symbolique très important en 2017 avec la création, par décret, du Commandement de la cyberdéfense (COMCYBER), qui est désormais – à l'intérieur de l'état-major des armées – l'organisme de référence et de tutelle des opérations militaires dans le cyberespace. Plus récemment, la « Revue stratégique de défense et de sécurité nationale », publiée en octobre 2017, la « Revue stratégique de cyberdéfense », publiée en février 2018, et la Loi de Programmation militaire 2019-2025, publiée en juillet 2018, consacrent un rôle majeur à la cyberdéfense militaire en lui conférant une plus grande visibilité et en augmentant ses moyens financiers et humains. Le 18 janvier 2019, la France, par la voix de la ministre des Armées, reconnaissait publiquement que la lutte informatique offensive figurait à son arsenal des moyens utilisables contre un adversaire, en réponse, ou non, à une agression préliminaire.

Pour garantir la souveraineté nationale dans le cyberespace, le ministère des Armées dispose de capacités lui permettant de se protéger contre les attaques informatiques, de les détecter et d'en identifier les auteurs. Il dispose également de la capacité à exploiter les failles informatiques d'un ennemi, en contexte de confrontation, et à maîtriser toutes les facettes du combat numérique. Le COMCYBER est directement placé sous l'autorité directe du chef d'état-major des armées, à l'image du Commandement des opérations spéciales.

Son décret de création précise qu'il est chargé de la protection et de la défense des systèmes d'information du ministère et de la conduite d'actions numériques à l'encontre des systèmes d'information adverses.

La cyberprotection consiste à bâtir d'épaisses murailles autour des systèmes d'information ainsi qu'à mesurer en permanence leur efficacité face à une menace toujours évolutive. La défense de ces systèmes vient en complément : plus dynamique, elle consiste à patrouiller, guetter, surveiller et intervenir sur les systèmes d'information en cas d'attaque, pour éradiquer la menace et reconstruire la muraille. L'action offensive, quant à elle, enrichit, avec l'arme numérique, la palette des options mises à la disposition de l'État. Le cyberespace est devenu un espace de confrontation à part entière au même titre que l'espace maritime, terrestre ou aérien, ou plus récemment l'espace exo-atmosphérique. Aujourd'hui, aucune opération militaire ne se conçoit sans cette dimension.

Le modèle actuel de ce commandement a été construit dans une logique d'économie des forces, de mutualisation des compétences et de concentration des efforts, mais aussi dans une logique de réseau, à l'instar de l'espace matériel et immatériel sur lequel il agit. Il permet une interaction fructueuse entre les acteurs du numérique étatiques et privés et assure une maîtrise des actions par l'intermédiaire d'une chaîne fonctionnelle dédiée. Le modèle français de cyberdéfense suit l'évolution sociétale actuelle : pour les citoyens utilisateurs du cyberespace, le ministère des Armées inspire sécurité et confiance ; il est le lieu privilégié de la création et de l'émulation d'une cyber-résilience. Le COMCYBER se veut fédérateur du ministère des Armées, et porteur d'une logique de renforcement des capacités interministérielles.

La défense de la France et de l'Europe doit s'adapter aux enjeux actuels et futurs du champ de bataille numérique. La supériorité opérationnelle de nos forces, c'est-à-dire la capacité à maîtriser des crises, comme celle d'entrer en premier sur un théâtre de conflit et à y contraindre un adversaire, passent désormais par la recherche et l'obtention de la supériorité dans le cyberespace.

C'est pourquoi la cyberdéfense au ministère des Armées est pensée dans l'action et construite dans la réalité d'un monde moderne qui a déjà réalisé sa transformation numérique.

Près de 3400 cybercombattants, répartis dans les armées et les différents services du ministère des Armées, sont placés sous l'autorité de l'officier général COMCYBER. Il appuie son action sur un état-major opérationnel d'environ soixante-dix personnes, organisé en quatre pôles.

Le ministère des Armées et le COMCYBER occupent une place singulière dans l'organisation nationale de la cyberdéfense. Cette dernière repose sur le principe de séparation des aspects défensifs et offensifs, et son organisation s'articule en trois grands partenaires, en plus du COMCYBER : l'ANSSI, la DGSE et la DGSI. Les aspects défensifs sont dirigés, au niveau gouvernemental, par l'ANSSI. Le ministère des Armées assure donc, par le biais du COMCYBER et en pleine coordination avec l'ANSSI, la défense de ses propres réseaux. Il peut, en outre, renforcer l'ANSSI si cette dernière le demande, au cas où notre pays serait victime d'une attaque cyber majeure.

Les moyens offensifs de la cyberdéfense sont détenus et mis en œuvre par le COMCYBER, en lien avec d'autres organismes. Sous l'autorité du chef des armées, il dirige l'emploi des moyens cyberoffensifs utilisés dans le cadre des opérations militaires.

Le COMCYBER s'appuie également sur un écosystème de partenariats internationaux. Comme pour tous les domaines sensibles dont la nature impose une culture forte du secret national – à l'instar du renseignement et des opérations spéciales – la cyberdéfense n'en est pas moins un domaine dans lequel des échanges internationaux, souvent sur un mode bilatéral, sont possibles, sinon indispensables. Ces coopérations prennent des formes diverses, de l'échange des bonnes pratiques à de véritables mécanismes de partage d'informations – permettant au COMCYBER d'affiner sa connaissance de la situation et de la menace cyber – jusqu'à la conduite d'opérations coordonnées. Balisées par des lignes rouges nationales, ces coopérations constituent aujourd'hui un levier de connaissance, d'efficacité opérationnelle et de rayonnement du COMCYBER au sein de la communauté militaire internationale de cyberdéfense.

Perspectives pour le futur

La montée en puissance de la cyberdéfense militaire se poursuit. Le passage à l'échelle évoqué plus haut est toujours d'actualité et de nombreux défis restent à relever.

En premier lieu se pose le défi de la ressource humaine. Cet aspect constitue d'ailleurs une des facettes du défi plus global de la numérisation du ministère des Armées. Il s'agit de recruter et de former les cybercombattants dont le ministère a besoin pour opérer dans le cyberespace, à un niveau qui soit à la hauteur des enjeux qui se posent à nous. Le recrutement et la fidélisation des cybercombattants est un redoutable défi à relever pour toutes les grandes organisations. Conjoncturelle ou structurelle, la pénurie des talents est une réalité qui crée de fait une tension concurrentielle très forte, sur un marché du travail très demandeur. Face à ce problème, le service public en général et la cyberdéfense militaire en particulier doivent d'ores et déjà faire preuve d'inventivité afin de capter l'attention des jeunes diplômés, en vue de susciter et de nourrir en eux un intérêt qui pourra se concrétiser par une collaboration plus ou moins longue. Il faut être clair, le secteur privé a l'avantage d'offrir les perspectives de rémunération les plus intéressantes. Le secteur public, lui, a l'avantage d'offrir un cadre de travail porté par la recherche d'efficacité et non contrainte par le chiffre d'affaires, donc favorable à l'excellence technique. Il offre de plus l'occasion de servir le pays de façon concrète et d'acquérir une expérience très solide et reconnue.

La formation des cybercombattants est également un défi de taille. Le modèle de formation actuel doit être renouvelé. Ce constat s'est d'ailleurs imposé dans toute la communauté du numérique des armées. Il s'agit de concevoir un nouveau modèle, mieux adapté aux réalités d'aujourd'hui et

à ce que l'on peut entrevoir de celles de demain. Il faut garantir au ministère la mise à disposition d'une ressource humaine cyber entretenue en permanence au plus haut niveau technique. Cet objectif nécessitera de faire converger les efforts de tous les acteurs du ministère. Une coordination interne renforcée sera indispensable. La création d'un centre d'expertise des formations et des parcours professionnels cyber du ministère des Armées, en somme une « académie cyber », pourrait constituer l'élément structurant de la réponse globale à cette problématique. Le ministère des Armées possède de vrais atouts à faire valoir en termes de formation.

Enfin, la cyberdéfense est confrontée à un défi technique dont l'ampleur ne se rencontre que dans le domaine du numérique. Aucun autre domaine ne connaît des cycles de renouvellement technique aussi rapides. Il s'agit, en permanence, de connaître toutes les évolutions réalisées (et si possible celles qui le seront à brève échéance), de maîtriser ces techniques et de former tout le personnel nécessaire pour les maîtriser sur une large échelle.

Plusieurs enjeux se dessinent à court terme, comme l'acquisition d'une capacité d'hypervision. À moyen terme, l'intelligence artificielle devra être mise au service de la détection et de la réaction aux agressions sans cesse plus perfectionnées que nous pourrions rencontrer. À plus long terme, l'informatique quantique devrait créer une rupture très importante avec, notamment, le basculement massif, complet et définitif de tout le chiffrement classique dans le domaine du vulnérable.

Conclusion

La cyberdéfense demeure une priorité très forte du ministère des Armées avec l'ambition de donner à la France les moyens de construire un outil à la hauteur de ses ambitions opérationnelles et d'assurer pleinement sa cybersécurité.

L'inauguration par la ministre des Armées le 3 octobre dernier à Rennes du premier bâtiment entièrement dédié à la conduite des opérations cyber, au sein du pôle d'excellence cyber bâti avec la région Bretagne et à proximité immédiate d'une Cyberdéfense Factory destinée à faire éclore des entreprises du domaine par l'aide de l'État, témoigne de cette dynamique qui permet à la France de rayonner et lui confère un statut de cyberpuissance.