N° 2068

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

SEIZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 17 janvier 2024.

RAPPORT D'INFORMATION

DÉPOSÉ

en application de l'article 145 du Règlement

PAR LA COMMISSION DE LA DÉFENSE NATIONALE ET DES FORCES ARMÉES

en conclusion des travaux d'une mission flash, constituée le 15 mars 2023,
sur les **défis** *de la* **cyberdéfense**

ET PRÉSENTÉ PAR

Mme ANNE LE HENANFF ET M. FRÉDÉRIC MATHIEU,
Députés.

SOMMAIRE

___

Pages

INTRODUCTION

La commission de la Défense nationale et des forces armées a créé une mission flash sur les défis de la cyberdéfense le 15 mars 2023. Elle en a désigné rapporteurs Mme Anne Le Hénanff et M. Frédéric Mathieu.

Dans le cadre de leur mission flash, les rapporteurs se sont intéressés aux défis de la cyberdéfense. Cette notion a été entendue au sens des trois doctrines de lutte informatique que sont la LID, la LIO et la L2I. Ils ont également inclus dans le périmètre de leur mission flash la cyberprotection et la cyber-résilience et se sont intéressés à cette question tant à l'échelle du ministère des Armées qu'à l'échelle du SGDSN, autorité de tutelle de l'ANSSI.

Les rapporteurs ont conduit 25 auditions, à l'occasion desquelles ils ont entendu des représentants du ministère des Armées mais également de l'ANSSI, du SGDSN, du ministère de l'Intérieur, du ministère de l'Éducation nationale et du ministère de l'Enseignement supérieur et de la Recherche. Ils ont également pu s'entretenir avec des journalistes, des représentants d'ONG ainsi que des représentants d'entreprises de la BITD.

Par ailleurs, les rapporteurs ont effectué trois déplacements sur le territoire national et un déplacement à l'étranger. Sur le territoire national, ils se sont rendus à la DGA-MI, à Bruz, au groupement de la cyberdéfense des armées (GCA), à Saint-Jacques-de-la-Lande, à la 807e compagnie de transmissions de l'armée de Terre, à Saint-Jacques-de-la-Lande, ainsi qu'au Centre Support Cyberdéfense de la Marine nationale, à Brest. Ils se sont également rendus en Estonie et en Finlande.

Les rapporteurs formulent plusieurs recommandations, en conclusion de leur rapport, qui sont le fruit de leurs réflexions à l'aune des auditions qu'ils ont conduites mais également de leurs parcours personnels. Ils tiennent à remercier tout particulièrement l'ensemble des personnes avec lesquelles ils ont pu échanger sur ce sujet majeur, à la fois pour leur disponibilité mais également pour l'accueil qu'elles leur ont réservé.

PREMIÈRE PARTIE : CONCEPTS, DOCTRINES ET ACTEURS DE LA CYBERDÉFENSE

I. LE CYBERESPACE, NOUVEL ESPACE DE CONFLICTUALITÉ

Enjeu et priorité stratégiques, la cyberdéfense est garante de la souveraineté nationale. En lien avec de nombreux acteurs, le ministère des Armées participe activement à la protection, à la défense des systèmes d'information et à la conduite d'opérations dans le cyberespace.

La compétition et la conflictualité ne se limitent plus, désormais, aux seuls milieux traditionnels, terre, mer, air et à l'espace. Elles se sont étendues à ce nouveau champ au fur et à mesure que croissait l'utilisation des données numériques. Le cyber est désormais envisagé comme arme d'emploi dans toutes les opérations.

La revue stratégique de défense et de sécurité nationale de 2017 et la revue stratégique de cyberdéfense de février 2018 ont ainsi reconnu le rôle majeur de la cyberdéfense militaire. Cette consécration a trouvé sa traduction dans la loi de programmation militaire 2019-2025 qui a acté l'augmentation significative des moyens financiers et humains à hauteur de 1,6 milliard et le recrutement de 1 100 cybercombattants. Cet effort a été poursuivi dans la loi de programmation militaire 2024-2030 avec un budget de 4 milliards d'euros sur la période de la programmation, soit une hausse de 150 %. Cet effort vient répondre à une nécessité qui se fait chaque jour plus pressante. Les travaux doctrinaux publiés en 2019 sur la lutte informatique défensive (LID) et la lutte informatique offensive (LIO) dans les opérations militaires complètent la stratégie de cyberdéfense et contribuent à la préparation de l'avenir des opérations militaires en intégrant graduellement cette nouvelle capacité à la manœuvre d'ensemble des armées.

1. Le cyberespace : espace de vulnérabilité et d'opportunité

Si nos adversaires n'ont pas fondamentalement changé leurs objectifs – espionnage, sabotage ou encore manipulation – les modes opératoires et techniques utilisés pour y répondre sont sans cesse renouvelés par l'émergence continue de nouvelles pratiques et technologies liées au numérique, ainsi que l'hyper connectivité de nos équipements et réseaux.

Le cyberespace possède une dynamique qui lui est propre : instantanéité des échanges, diffusion en réseau, massivité de données accessibles à tous, effacement des frontières… Il est aussi un multiplicateur d'efficacité pour peu que l'on dispose

des bonnes données et informations, qui sont devenues une ressource critique, au cœur du fonctionnement politique, économique et social des sociétés modernes. Or, nos adversaires ont parfaitement compris l'avantage politique, économique ou opérationnel qu'ils pouvaient obtenir de l'exploitation des vulnérabilités de cette numérisation galopante, touchant aussi le champ de bataille.

Pour atténuer leur vulnérabilité, les systèmes militaires doivent offrir le meilleur niveau de « défendabilité » possible. Il s'agit, d'une part, de s'assurer de la bonne prise en compte du risque d'attaque cyber et des potentielles conséquences sur les organisations ou individus visés et, d'autre part, d'être en mesure d'adapter notre capacité d'action et de réaction à une attaque cyber, en fonction du contexte opérationnel ou de la réalité de la menace.

Le cyberespace se structure en trois couches indissociables, d'où procèdent toutes les menaces :

1/ une couche physique, constituée des équipements, des systèmes informatiques et de leurs réseaux ayant une existence matérielle (donc une territorialité qui ouvre sur un droit national, voire international) ;

2/ une couche logique, constituée de l'ensemble des données numériques, des logiciels, des processus et outils de traitement, de gestion et d'administration de ces données, ainsi que de leurs flux d'échanges, implantés dans les matériels pour leur permettre de rendre les services attendus ;

3/ et une couche cognitive, également appelée couche informationnelle, constituée des informations et des interactions sociales de toutes sortes qui se trouvent dans le cyberespace et des personnes qui peuvent déclarer plusieurs identités numériques

Au-delà de la notion de « défendabilité » des systèmes, la cyberdéfense au sein du ministère des Armées est déclinée en pleine cohérence avec les six missions définies par la revue stratégique de cyberdéfense publiée en février 2018 :

1/ prévenir : il s'agit de faire prendre conscience aux utilisateurs du risque représenté par la numérisation des organisations ou des équipements qu'ils servent. Cette mission incombe au Haut fonctionnaire correspondant de défense et de sécurité (HFCDS) du ministère ;

2/ anticiper : il s'agit d'évaluer en permanence les probabilités de cyberattaques et prendre des mesures préventives lorsque la menace paraît suffisamment forte. Cette mission incombe à l'Agence nationale de sécurité des systèmes d'information (ANSSI), en coordination avec les services de renseignement et le Commandement de la cyberdéfense (COMCYBER) sur le périmètre du ministère des Armées ;

3/ protéger : il s'agit de diminuer la vulnérabilité de nos systèmes informatiques, à la fois en compliquant la tâche des attaquants potentiels et en

facilitant la détection des cyberattaques. La protection est nécessaire tout au long du cycle de vie des systèmes ;

4/ détecter : il s'agit de rechercher des indices d'une éventuelle cyberattaque en cours. Cette mission relève de la responsabilité du COMCYBER et des unités subordonnées à la ministre des Armées. Pour compléter ses informations, il sollicite ses partenaires nationaux et internationaux ;

5/ réagir : il s'agit de résister à une cyberattaque afin qu'elle n'empêche pas la poursuite de notre activité. Dans la plupart des cas, le COMCYBER déclenche alors une opération de LID, en liaison avec l'ANSSI. Elle peut entraîner l'emploi de moyens qui sortent du domaine de la cyberdéfense, voire du ministère des Armées (saisie de la justice, action diplomatique, rétorsion économique, etc.) ;

6/ attribuer : il s'agit de préciser l'auteur d'une cyberattaque par des preuves ou un faisceau d'indices. Les services de renseignement sont au cœur de ce processus de recueil d'indices d'attribution. La décision d'attribution appartient aux plus hauts responsables politiques.

Les actions de prévention et de protection concernent les systèmes informatiques du ministère des Armées (zone amie). Les missions d'anticipation, de détection et de réaction s'intéressent aux systèmes informatiques appartenant aux autres catégories d'acteurs (zones neutre et ennemie).

2. Trois doctrines de lutte informatique : la LID, la LIO et la L2I

Les opérations dans le cyberespace reposent sur trois doctrines :

– la LID, qui regroupe l'ensemble des actions, techniques ou non, conduites pour faire face à un risque, une menace ou à une cyberattaque réelle ;

– la LIO, qui regroupe l'ensemble des actions entreprises dans le cyberespace, conduites de façon autonome ou en combinaison des moyens militaires conventionnels, pour produire des effets à l'encontre d'un système adverse afin d'en altérer la disponibilité ou la confidentialité des données ;

– et la L2I, qui désigne les opérations militaires conduites de façon autonome ou en combinaison avec d'autres opérations dans la couche informationnelle du cyberespace afin de détecter, caractériser et contrer les attaques, appuyer la communication stratégique, renseigner ou faire de la déception.

a. La LID

i. Généralités

La protection des réseaux informatiques et des systèmes d'information constitue le premier rempart pour empêcher une attaque informatique. Si ce premier rempart est indispensable, la dynamique de numérisation des systèmes qui

soutiennent les activités du ministère, y compris au profit de son engagement opérationnel via ses systèmes de commandement et ses systèmes d'armes, offre de nouvelles opportunités aux attaquants ; elle nous impose donc de développer de nouveaux modes de défense, adaptés à ces nouvelles menaces.

C'est sur la base de ce constat que le ministère des Armées a souhaité redéfinir sa politique en matière de LID. Cette politique ministérielle de LID, présentée sous forme d'une instruction ministérielle, développe des principes de réponse à ces questions, en précisant l'organisation et les missions qui s'appliquent à tous les organismes placés sous l'autorité de la ministre des Armées, ainsi que les attentes et contraintes de ceux qui contribuent, par des services ou des capacités, à son engagement (industriels…).

La LID regroupe l'ensemble des actions, techniques et non techniques, conduites pour faire face à un risque, une menace ou à une cyberattaque réelle, en vue de préserver notre liberté d'action. La LID couvre principalement trois de ces missions : anticiper, détecter et réagir et complète les missions : prévenir, protéger et attribuer. Elle contribue ainsi à la résilience des armées et plus globalement à l'élaboration des stratégies de réponse aux niveaux ministériel et interministériel.

Au sein du ministère des Armées, les opérations de LID sont planifiées et conduites par le COMCYBER, en coordination avec l'ANSSI, les services de renseignement, et éventuellement d'autres partenaires (nationaux ou internationaux).

ii. La cyberdéfense militaire au sein de l'État

La cyberdéfense de l'État relève de la responsabilité du directeur général de l'ANSSI. Pour le ministère des Armées, la conduite de la cyberdéfense de ses systèmes d'information est de la responsabilité du chef d'état-major des armées (CEMA).

Le COMCYBER, subordonné au CEMA, est pour sa part chargé de l'organisation et des opérations de LID pour l'ensemble du ministère. Il se coordonne très étroitement avec l'ANSSI dans l'exercice quotidien de ses missions de cyberdéfense.

Dans un souci de cohérence et d'efficience, la chaîne de commandement de cette cyberdéfense est dite unifiée, centralisée et spécialisée pour tout le ministère. C'est-à-dire qu'elle est pilotée et coordonnée par le COMCYBER et que composée d'experts et de la cyberdéfense, elle doit en outre favoriser les synergies entre les différentes organisations chargées de la LID tout en permettant de disposer d'une vision globale de la situation cyber.

Au sein du ministère, chaque état-major, direction et service, met en place les moyens de LID sur son périmètre de responsabilité en application du principe de subsidiarité. Chaque responsable de cyberdéfense au sein du ministère doit pouvoir s'appuyer sur une structure opérationnelle de type *Security Operating*

Centre (SOC) chargée de la supervision de ses systèmes. Les SOC constituent le premier niveau de détection des attaques cyber.

À l'échelle du ministère, sous les ordres du COMCYBER, le Centre d'analyse en lutte informatique défensive (CALID) assure une « hypervision » technique d'ensemble, qui synthétise et partage l'information des situations cyber produites par l'ensemble des SOC ou par ses moyens propres.

Au sommet de la chaîne de LID, le COMCYBER s'appuie sur le centre des opérations pour orienter le travail du CALID et des SOC. En particulier, il partage l'état de la menace cyber et des nouvelles vulnérabilités découvertes afin d'optimiser l'efficacité de la chaîne de cyberdéfense et de protection du ministère. Le CO agit aussi en soutien du CALID dans la gestion d'un incident cyber.

La transformation numérique du ministère se caractérise à la fois par la rapidité à laquelle elle est conduite et une connectivité toujours plus importante entre les systèmes, au sein du ministère, mais également avec nos différents partenaires dont les industriels de la Défense.

Ainsi, pour une meilleure efficacité contre la menace, ces partenaires extérieurs au ministère doivent être parties prenantes de la LID du ministère. En effet, l'attaquant recherche toujours un point faible ou indirect pour pénétrer les systèmes militaires.

iii. Une posture permanente cyber de LID pour la défense des systèmes numérisés

La LID du ministère obéit à des règles d'engagement et de confidentialité édictées par le COMCYBER. Une opération de LID peut nécessiter de dégrader ou d'interrompre un service. Cette décision relève généralement du chef de l'unité qui utilise le système en question. Néanmoins, si la gravité ou l'urgence de la situation l'exige, la coupure peut être imposée par un échelon supérieur ou le COMCYBER.

La tension générée par les attaques cyber, cycliques ou soudaines, de gravités variables, impose l'adoption d'une vigilance de tous les instants, qui s'incarne à travers la posture permanente de cyberdéfense (PPC) pour le ministère des Armées. La PPC est constituée de l'ensemble des dispositions adoptées pour assurer en permanence (24h/24, 7 J/7) la défense des systèmes informatiques du ministère dans le *continuum* « compétition-contestation-affrontement ».

La Revue stratégique de cyberdéfense de février 2018 a établi un classement des attaques informatiques qui tient compte de la caractérisation de l'impact (de négligeable à extrême) et de la possibilité de caractériser juridiquement cette attaque comme une agression armée. En cohérence avec ce classement, la PPC identifie quatre niveaux de menace à l'encontre des systèmes informatiques du ministère : jaune et orange, identifiant des risques potentiels plus ou moins importants, rouge, des risques hostiles jugés plausibles et écarlates, des risques majeurs et simultanés.

Cette échelle de risques, qui associe niveau de menace et objectifs de protection des systèmes, est complétée par un stade d'alerte, « vigilance », « renforcé », ou « crise », qui précise si l'attaque est à venir ou en cours, pour adapter en conséquence les mesures à prendre au sein du ministère, qui peuvent ainsi ponctuellement varier d'une zone ou d'un domaine particulier à l'autre.

b. La LIO

La LIO désigne l'ensemble des actions entreprises dans le cyber espace produisant des effets à l'encontre d'un système adverse, pour en altérer la disponibilité ou la confidentialité des données. Les effets de la LIO peuvent être matériel (neutralisation d'un système d'arme) ou immatériel (collecte de renseignement de manière temporaire, réversible ou définitive). La LIO peut être utilisée de manière autonome, mais c'est en combinaison des moyens militaires conventionnels qu'elle prend sa pleine dimension de potentiel multiplicateur d'effets.

En outre, la LIO a une temporalité propre : si les effets peuvent être fulgurants, son intégration dans la manœuvre opérationnelle globale est issue d'une planification longue et très spécifique.

L'objectif premier de la LIO est de contribuer dans le cyber espace à la supériorité militaire. Elle permet d'atteindre trois types d'objectifs opérationnels dans la conduite des opérations :

1/ l'évaluation de capacités militaires adverses par le recueil ou l'extraction d'informations ;

2/ la réduction, voire neutralisation de capacités adverses ;

3/ et la modification de la capacité d'analyse de l'adversaire.

Les cibles visées peuvent être exposées sur Internet, isolées, ou partie intégrante d'un système d'armes plus global. Les actions ne sont pas nécessairement au contact physique de l'adversaire.

Au sein du ministère des Armées, la LIO est organisée selon une chaîne de commandement unifiée sous la responsabilité du COMCYBER. L'emploi de la LIO exige une maîtrise des risques politiques, juridiques et militaires. Il est déterminé par le droit, le rapport coût/efficacité, la situation opérationnelle et le contexte politique général.

c. La L2I

La L2I désigne les opérations militaires conduites dans la couche informationnelle du cyber espace pour détecter, caractériser et contrer les attaques, appuyer la communication stratégique (StratCom) qui permet de cadrer la conception et la conduite de toute activité militaire des armées françaises comme un message cohérent, crédible et efficace auprès des principaux acteurs qui en ont

connaissance, renseigner ou faire de la déception, de façon autonome ou en combinaison avec d'autres opérations.

Le lieu d'action de la L2I est la couche informationnelle du cyber espace. Du fait des caractéristiques de cet espace, sa maîtrise requiert des compétences communes avec celles de la LID et de la LIO. La planification et la conduite des opérations de L2I dans cet environnement sont assurées par le COMCYBER et intégrées dans les actions interarmées. Elles consistent, pour l'essentiel, à détecter les attaques informationnelles susceptibles de nuire à la réputation des armées ou d'entraver leur action, à les caractériser, à les contrer et à promouvoir l'action de nos forces. La L2I peut aussi offrir, sur nos théâtres d'opérations, des opportunités de recueil de renseignement et d'opérations de déception qui doivent être pleinement exploitées.

Concrètement, les actions menées au titre de la L2I relèvent du soutien à la StratCom, de la perturbation de la propagande adverse, de la dénonciation des fausses informations et de la mobilisation des opposants de l'adversaire afin d'amplifier leurs actions.

3. Par-delà les doctrines de lutte informatique

Le cyberespace constitue donc désormais un espace de manœuvre et de confrontation à part entière, au même titre que les milieux terrestres, maritime, aérien, et extra-atmosphérique. Il est un milieu transverse sans lequel quasi aucune activité n'est possible dans les autres milieux. Il possède en particulier des liens étroits avec les champs électromagnétique et informationnel.

L'action dans ou depuis le cyberespace peut ainsi produire des effets dans l'ensemble des milieux et champs. Par exemple une attaque cyber peut faire dévier de sa route un satellite. Réciproquement, une action dans ces milieux et champs peut produire des effets dans le cyberespace. Par exemple une bombe lancée contre un centre de données peut détruire ses serveurs.

Dans ce contexte, le cyberespace a acquis une valeur stratégique permettant de garantir la liberté d'action des forces dans les autres milieux et champs. Or, la menace est multiforme, permanente, non territorialisée et peut impacter tous les niveaux tactiques, à l'avant comme à l'arrière. Ce milieu doit par conséquent être pris en compte dans la manœuvre pour se protéger et pour saisir les opportunités d'agir. Surtout, il doit être pris en compte dès la phase de compétition du *continuum* « compétition-contestation-affrontement », au quartier comme en mission.

De fait, il existe nécessairement des spécificités de milieu évidentes dans l'exploitation du volet cyber par les trois armées. Un sous-marin n'est pas soumis à la même menace cyber qu'un PC de division installé en zone industrielle d'une ville ou qu'un avion militaire posé sur une base aérienne de théâtre. De même, l'environnement numérique adverse d'une force navale, terrestre ou aérienne est intimement lié au milieu.

Les trois volets de la politique de cyberdéfense du ministère des Armées (LID, LIO et L2I) permettent aux trois armées de prendre en compte ces dimensions (se protéger, se défendre et agir) de manière adaptée et complémentaire grâce à une organisation assurant la cohérence d'ensemble du modèle cyber du ministère tout en respectant les spécificités des armées.

Mais si les doctrines sont une référence, elles ne constituent pas un carcan. Elles définissent les principes et les responsabilités et doivent s'adapter à l'emploi. Dans un domaine aussi jeune que les opérations dans le cyberespace, il est pertinent qu'elles soient revues régulièrement avec l'ensemble de la communauté cyber mais aussi plus largement la communauté militaire des opérations car tout évolue très rapidement. L'apparition dans le champ doctrinal du concept des opérations multi milieux multi champs dans le concept d'emploi des forces de 2021 traduit bien cet état de fait.

II. LES ACTEURS DE LA CYBERDÉFENSE AU MINISTÈRE DES ARMÉES ET AU-DELÀ

1. Les trois principaux acteurs de la cyberdéfense au ministère des Armées : le COMCYBER, la DGA et la DGSE

a. Le COMCYBER

Placé sous l'autorité directe du CEMA, le commandement de la cyberdéfense (COMCYBER) est un commandement opérationnel qui rassemble l'ensemble des forces de cyberdéfense sous une autorité interarmées déployé sur plusieurs emprises à Paris et à Rennes. Le COMCYBER effectue ses missions par délégation de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), qui est responsable de la cyberdéfense et de la cybersécurité des administrations publiques, des entreprises et, singulièrement, des opérateurs d'importance vitale (OIV).

Créé en mai 2017, le COMCYBER est en charge :

– de la conception, de la planification et de la conduite des opérations de cyberdéfense, ainsi que de la défense des systèmes d'information des armées, directions et services (ADS) du ministère des Armées (à l'exception de ceux de la DGSE et de la DRSD) ;

– de la stratégie de cyberdéfense par la coordination des contributions des armées et organismes interarmées à la politique nationale et internationale de cyberdéfense et par la mise en cohérence du modèle de cyberdéfense du ministère des Armées ;

– et de la dimension capacitaire de la politique de cyberdéfense par l'élaboration de la politique des ressources humaines de cyberdéfense, par la coordination de la définition des besoins techniques spécifiques à la cyberdéfense et par la gestion de la réserve de cyberdéfense.

Pour remplir ses missions, le COMCYBER exerce un commandement opérationnel sur plus de 3 600 cybercombattants, répartis entre l'état-major de la cyberdéfense et quatre entités :

– le centre d'analyse en LID (CALID), en charge de la surveillance et de la détection des cyberattaques, ainsi que de l'anticipation des menaces et de la conduite des opérations défensives. À ce titre, le CALID constitue le centre de veille, d'alerte et de réponse aux attaques informatiques (*Computer Emergency Response Team*, CERT) du ministère des Armées, qui veille en permanence 24h/24 sur la sécurité des systèmes d'information des ADS du ministère. Son personnel peut être projeté tant sur le territoire national qu'en opération extérieure (OPEX) ;

– le centre d'audits de la sécurité des systèmes d'information (CASSI), en charge de l'audit de conformité et de sécurité des systèmes d'information du ministère ;

– le centre cyber de préparation opérationnelle (C2PO), en charge de l'entraînement des EMDS au combat dans le cyberespace dans le cadre d'exercices nationaux et internationaux de cyberdéfense, parmi lesquels l'exercice annuel interarmées DEFNET et l'exercice international *Locked Shields* du centre d'excellence cyber à Tallinn en Estonie ;

– et le centre des homologations principales interarmées (CHPI), qui procède aux études de sécurité aboutissant à l'homologation des nouveaux systèmes d'information du ministère avant leur mise en service opérationnelle.

Ces quatre entités ont vocation à être intégralement regroupées d'ici 2025 au sein du groupement de la cyberdéfense des armées (GCA), créé le 1er septembre 2020 et situé au quartier Stéphant dans la région de Rennes. Le GCA est en charge de l'identification des besoins des ADS du ministère des Armées en réservistes de cyberdéfense. À ce titre, il assure leur recrutement, leur sélection et leur affectation sur le territoire national.

b. La DGA

La DGA constitue, avec l'ANSSI et la DGSE, le plus important pôle de compétences techniques au sein de l'État dans le domaine cyber. Elle constitue l'expert technique référent du ministère des Armées.

De manière générale, la DGA est responsable de la conception et de la réalisation des systèmes permettant de garantir aux forces, dans la durée, la résilience cyber des capacités qu'elles opèrent, et d'acquérir et de conserver leur liberté d'appréciation et d'action dans le cyberespace.

Cette mission se décline selon quatre axes :

1/ porter à un niveau adapté au niveau de la menace la cybersécurité des systèmes numériques et des systèmes d'armes afin d'être résilient face aux agressions cyber ;

2/ équiper nos forces armées de systèmes leur permettant d'acquérir et de conserver leur liberté d'appréciation et d'action dans le cyberespace, c'est-à-dire de conduire des actions dans les trois domaines de lutte informatique ;

3/ orienter, maintenir et développer les capacités technologiques et industrielles nécessaires, en cohérence avec la stratégie nationale de cyberdéfense ;

4/ accroître la cybersécurité de la BITD et contribuer à la cyberdéfense de la Nation au sein du C4 dont la DGA est membre aux côtés de la DGSE, de la DGSI, du COMCYBER et de l'ANSSI.

c. La DGSE

Dans le domaine de la cyberdéfense, la DGSE participe à la protection des intérêts fondamentaux de la France par des actions de renseignements ainsi qu'à la compréhension et à la réduction de la menace cyber (criminelle ou d'État).

Au titre de cette mission, la DGSE est membre du C4 et partage ses renseignements au sein de cette comitologie interministérielle. Sur le territoire national, sur autorisation du Premier ministre après avis de la CNCTR, la DGSE met en œuvre toutes les techniques de recueil du renseignement (TRR) autorisées par le code de la sécurité intérieure, selon le principe de proportionnalité. À l'étranger, la DGSE utilise tous types de TRR dont il dispose.

Par anticipation sur une action hostile pouvant toucher la France, le renseignement sur la menace cyber cherche à informer sur les acteurs, étatiques ou criminels, connus pour nourrir des projets agressifs dans l'espace numérique ainsi que sur les outils et les services commercialisés pour mettre en œuvre ces projets. En complément, par réaction à une action hostile ayant touché la France, le renseignement sur la menace aura pour mission d'identifier l'auteur de l'action et son donneur d'ordre.

2. D'autres acteurs au sein du ministère des Armées concourent, de près ou de loin, à la politique de cyberdéfense

a. La DIRISI

Parmi les acteurs en charge de la LID, la direction interarmées des réseaux d'infrastructure et des systèmes d'information (DIRISI) joue un rôle élémentaire. La cybersécurité de la DIRISI doit répondre à la fois aux impératifs opérationnels, réglementaires et légaux, mais également à la réalité de l'exploitation. À ce titre, elle est intégrée à l'ensemble des processus et outils de pilotage de la DIRISI et elle fait l'objet d'un pilotage fonctionnel d'ensemble assuré par la sous-direction

« cyber » de la DIRISI. L'organisation cyber de la DIRISI a pour fonction d'intégrer les objectifs de cybersécurité à l'ensemble des activités de la DIRISI.

La chaîne de commandement de la DIRISI inclut simultanément les responsabilités opérationnelles de délivrance de capacités SIC, de maîtrise du risque cyber inhérent aux capacités délivrées et de respect de la réglementation. Pour exercer ces responsabilités, la DIRISI dispose de spécialistes de la cybersécurité, en charge de conseiller et de piloter les actions cyber. Ces spécialistes constituent la chaîne fonctionnelle relative à la cybersécurité au sein de la direction.

La direction de la fonction cybersécurité est assurée par la sous-direction « cyber ». Elle a pour but d'apporter au directeur central une information fiable sur le niveau de prise en compte des objectifs de sécurité, sur le niveau d'exposition à la menace cyber, et de garantir la cohérence des actions menées à l'échelle de la DIRISI.

La direction « acquisition et logistique » est en charge de la déclinaison de la politique et des exigences cyber dans la rédaction des marchés pilotés par la DIRISI. La planification et la conduite des actions de cybersécurité relatives aux SI exploités par la DIRISI sont assurées au sein de la division « opération » et sont intégrées aux opérations SIC sous-jacentes. La DIRISI dispose ainsi d'un *Security Operational Center* (SOC).

b. La DRSD

La DRSD est le service de renseignement dont dispose le ministre des armées pour assumer ses responsabilités en matière de sécurité du personnel, des informations, du matériel et des installations sensibles. Sa mission consiste à déceler, identifier et neutraliser toute menace contre la sphère de Défense résultant de services de renseignement, d'organisations, d'agents ou d'individus sur l'ensemble du spectre TESSCo (terrorisme, espionnage, sabotage, subversion, criminalité organisée).

La DRSD agit en croisant les menaces et les vulnérabilités dans les domaines suivants :

1/ l'identification et la neutralisation des menaces sont basées sur le plan national d'orientation du renseignement (PNOR) qui décline les objectifs assignés aux services spécialisés de renseignement sur les 4 grands enjeux de sécurité et de défense définis par la stratégie nationale du renseignement. Le PNOR 2021 intègre également un second volet consacré aux enjeux structurants pour la France et nécessitant une approche transversale. Il fait l'objet d'actualisation régulière correspondant aux menaces nouvelles.

2/ la détection et la réduction des vulnérabilités qui reposent, d'une part, sur un corpus réglementaire et, d'autre part, sur des demandes des autorités, notamment par le concours de la direction de la protection des installations, moyens et activités de la défense (DPID).

Le triple rôle d'inspection du Service est défini dans le code de la défense : protection du secret, protection des points d'importance vitale (PIV) et protection du patrimoine scientifique et technique de la Nation (PSTN), à la fois pour les forces armées et pour les entreprises de défense. Il est ensuite décliné dans les diverses instructions interministérielles et ministérielles. Les priorités d'actions résultent pour partie d'une planification fondée sur des calendriers réglementaires et des délais imposés, mais également des demandes ponctuelles émanant des autorités.

En matière de cyberdéfense, la DRSD agit comme pour toutes les thématiques du spectre TESSCo, dans deux domaines qui font de la DRSD un acteur global en matière de renseignement et de sécurité :

1/ la contre-ingérence des forces (CIF) : le Service se place en appui du COMCYBER, particulièrement au travers de l'action d'un officier de liaison déployé par la DRSD au sein du COMCYBER ;

2/ la contre-ingérence économique (CIE) visant à protéger le patrimoine scientifique et technique de la Nation (PSTN) et la base industrielle et technologique de défense (BITD) contre toutes les formes de prédations, notamment cybercriminelle et de cyber espionnage ;

En outre, la DRSD poursuit le développement de sa capacité propre de contre-ingérence cyber en lien avec l'ANSSI et le COMCYBER. Ses actions en la matière portent de façon transverse (CIF et CIE) sur l'élaboration du renseignement nécessaire à l'anticipation et l'attribution des attaques, sur l'investigation après la constatation de compromissions et sur la cyber sécurité du contrôle gouvernemental dans le domaine nucléaire.

c. La DPID

La DPID a été créée en 2015 et placée sous l'autorité directe du ministre pour l'exercice de ses responsabilités en matière de protection des installations intéressant la défense nationale, protection des moyens et activités de la dissuasion, protection des personnes et des biens du ministère, sécurité des systèmes d'information intéressant la défense, protection du secret de la défense nationale, protection du potentiel scientifique et technique de la nation, gestion de la continuité d'activité ministérielle. Au-delà du ministère des Armées et de ses établissements publics, la responsabilité de la DPID s'étend aux entreprises de défense et en particulier à la base industrielle et technologique de défense (BITD) et ses opérateurs d'importance vitale (OIV).

La DPID est également le service dont dispose le Haut fonctionnaire correspondant défense sécurité (HFCDS) du ministère. Le HFCDS en titre est le chef du cabinet militaire du ministre des Armées. Les responsabilités du DPID ne recouvrent pas l'emploi opérationnel des forces armées qui relèvent de la responsabilité du CEMA.

À la fois échelon de synthèse au profit du ministre et de son cabinet et instance normative, la DPID œuvre au développement d'un esprit défense et de sécurité sur l'ensemble du ministère.

Afin de « *garanti[r] au Ministre que les installations, moyens et activités de la défense sont protégées contre les actes malveillants ou hostiles, les atteintes à la protection du secret et les cybermenaces* [(1)]», la DPID analyse les remontées de terrain sur les dispositifs de défense et de sécurité du ministère (incidents, inspections) et propose la réponse ministérielle (politiques et instructions ministérielles, orientation de la réponse capacitaire, homologations d'installations ou encore approbation des plans de sécurité « opérateurs »). La sécurité des installations et des moyens de la dissuasion – qu'elles relèvent d'opérateurs publics ou privés – est au cœur de l'action de la DPID.

La DPID compte une trentaine de personnes, civils et militaires, y compris des réservistes opérationnels, chacune ayant une expertise confirmée.

La sécurité numérique est venue s'ajouter récemment aux missions de la DPID. Pour améliorer la lisibilité de la gouvernance du numérique et de celle de la sécurité numérique, le fonctionnaire de la sécurité des systèmes d'information (FSSI), auparavant rattaché à la DGNUM, a été transféré à la DPID en 2019. Ce transfert a permis de recentrer la DGNUM sur sa mission de « DSI groupe », en charge de s'assurer de la bonne prise en compte des orientations et des normes produites par la DPID dans les projets conduits par les DSI du ministère des Armées.

Cette évolution a permis d'intégrer au sein de la DPID les sujets de sécurité numérique et les enjeux de défense et de sécurité « classiques » dans une logique de cohérence globale. Dans le cadre de cette gouvernance rénovée, la DPID est devenue l'autorité ministérielle de sécurité numérique (AMSN) par délégation du HFCDS. En s'appuyant sur le FSSI, l'AMSN pilote la gouvernance ministérielle de sécurité numérique et produit les documents de portée générale qui permettent de décliner les documents interministériels et d'encadrer l'action du ministère.

En s'appuyant sur la DRSD, le COMCYBER, la DGA, le SGA, la DGSE, la DGNUM et la DIRISI, le FSSI propose les ambitions et objectifs stratégiques de sécurité numérique ministériels. Il propose également la politique ministérielle de sécurité numérique et en contrôle l'application, en s'appuyant en particulier sur la DRSD dont il mandate les inspections. Il prépare la comitologie ministérielle de sécurité numérique.

Un comité ministériel mensuel de la sécurité numérique, présidé par le DPID, animé par le FSSI, en présence des autorités qualifiées en matière de sécurité des systèmes d'information (DGA, SGA, CEMA, DRSD et DGSE) et des acteurs précités, permet d'aborder régulièrement les sujets nécessaires à la cybersécurité du ministère : les ressources humaines, les finances, la cryptographie, l'actualisation

(1) Décret 2015-1029 du 19 août 2015 relatif à la direction de la protection des installations, moyens et activités de la défense

de la menace, les retours d'expérience, la cybersécurité des entreprises de défense, entre autres. Ce comité est chapeauté par un comité directeur présidé par le HFCDS et par un comité exécutif présidé par le ministre ou son représentant.

Enfin, une cartographie ministérielle des risques en matière de sécurité numérique et un tableau de bord, en cours de stabilisation, permettent de prioriser les actions du ministère dans une logique de maîtrise des risques.

d. La DGNUM

La DGNUM a pour mission de proposer la politique ministérielle du numérique et d'en piloter la mise en œuvre.

Dans le cadre des comités exécutifs (COMEX) ministériels de 2020 et 2021, une nouvelle organisation de la gouvernance de la conduite et du suivi des projets numériques a été décidée. La DGNUM a favorisé l'unification de la gouvernance haute de l'ensemble des SI, garantissant une plus grande transversalité, en associant les trois subordonnés sous l'égide du comité exécutif du conseil du numérique et des SIC (CECNum), avec à l'échelon subordonné une gouvernance par grands domaines.

Dans ce cadre, la DGNUM a animé le chantier ministériel « organisation et gouvernance » qui a permis de mettre en place une nouvelle organisation et de fixer la gouvernance numérique du ministère à travers des textes rénovés. Cette nouvelle organisation mise en place depuis 2020 vise à simplifier, moderniser et améliorer les processus, à mutualiser et à rassembler les fonctions complexes et transverses et à renforcer les prérogatives des autorités d'emploi des produits et services, numériques et SIC.

Le modèle d'organisation retenu pour transformer la fonction « SIC et numérique » du ministère des Armées s'appuie sur celui des principaux grands groupes français caractérisé notamment par l'existence de DSI ayant un rôle renforcé dans la gestion de leur portefeuille et l'exploitation de leur SI.

Cette organisation s'appuie sur une gouvernance collégiale de la politique ministérielle numérique animée par la DGNUM. La mise en place de la nouvelle organisation s'est accompagnée de travaux de rénovation de la gouvernance numérique, s'attachant à bien définir les rôles et responsabilités des acteurs dans ce nouvel écosystème. Le bon aboutissement de ce chantier ministériel de rénovation de la gouvernance numérique a nécessité la mise à jour des textes officiels. Ainsi sont parus officiellement à l'automne 2022 l'arrêté du 9 septembre 2022 portant création et organisation d'instances relatives au SIC de la défense (rôle des principaux acteurs de l'écosystème numérique ministériel) et l'instruction du 9 septembre 2022 fixant la gouvernance ministérielle du numérique et des SIC.

e. Les trois armées

i. L'armée de Terre

Le numérique permet un développement considérable des activités humaines. Le cyberespace est la résultante de la numérisation des activités de nos sociétés et de l'interconnexion, directe ou indirecte, des systèmes et réseaux. À ce titre, le cyberespace comprend Internet et l'ensemble des autres fédérations de réseaux informatiques. Il englobe également, pour les armées, les systèmes d'information isolés, les systèmes d'armes et les systèmes industriels. Transverse par nature du fait de ses liens avec le champ matériel, le cyberespace est d'un point de vue militaire un lieu (champ de bataille), un moyen et un enjeu de conflictualité.

Par conséquent, les SI permettant aux armées de remplir leurs missions au quotidien sur le territoire national doivent être protégés. Il en va ainsi pour l'armée de Terre. De même, l'info-valorisation et le combat collaboratif, facteurs de supériorité opérationnelle de l'armée de Terre, doivent être protégés. Mais ce qui est vrai pour les armées l'est également pour nos adversaires. Les objectifs des opérations militaires dans le cyberespace ne se limitent pas à la protection de nos systèmes d'information et systèmes d'armes. Ils comprennent également l'entrave de systèmes adverses, la captation de renseignement ou encore la modification des perceptions de l'adversaire.

Dès lors, faisant un parallèle avec l'organisation de l'État et le niveau interarmées, la cyberdéfense de l'armée de Terre désigne l'ensemble des moyens lui permettant de se défendre et d'agir dans le cyberespace. Elle lui permet de sécuriser ses activités, de contribuer aux réponses apportées aux agressions contre la Nation et à la réalisation des effets cyber en vue d'atteindre des objectifs militaires dans le cadre d'opérations militaires.

La cyberdéfense au sein de l'armée de Terre comprend donc :

1/ une organisation ;

2/ des politiques et des doctrines d'emploi ;

3/ des ressources humaines ;

4/ et des équipements.

Dans le cadre de cette organisation et de ces politiques et doctrines d'emploi, le CEMAT est responsable, par délégation du CEMA et en coordination étroite avec le COMCYBER, de la protection et de la défense des systèmes d'information et des systèmes d'armes que l'armée de Terre développe et emploie. Il est également chargé de former et de préparer des unités aptes à concourir aux opérations planifiées et conduites dans le cyberespace par le COMCYBER. Dès lors, l'armée de Terre distingue deux chaînes opérationnelles particulières et complémentaires :

1/ la cyberprotection, pour assurer ses missions de sécurisation de ses propres activités où l'on retrouve les volets chiffre et homologation. Pour ce dernier, le CEMAT est autorité d'homologation principale (AHP). Il est ainsi responsable des systèmes métiers que l'armée de Terre fait développer et met en œuvre (SIAG, SIOC et SA). Il s'appuie pour cette fonction et la gestion du chiffre sur une chaîne d'autorités d'homologation secondaire (AHS) à la tête de chaque grand commandement ou service, au nombre de six (SIMMT, DRHAT, STAT, EMAT, COMALAT, COMSIC). La chaîne cyberprotection est donc déconcentrée au sein de chacun des commandements « métiers » de l'armée de Terre ;

2/ et la cyberdéfense (LID, L2I, LIO), pour garantir sa participation aux opérations militaires dans le cyberespace.

Concernant ce dernier point, le CEMAT a décrit dans sa vision stratégique parue le 19 avril 2023 la cyberdéfense comme un nouveau facteur de puissance qui doit irriguer les forces terrestres à travers les niveaux corps, division, brigade et régiment. Ainsi, son ambition cyber pour la période 2024-2030 doit permettre à l'armée de Terre d'élargir et de renforcer sa contribution à la cyberdéfense en assumant, par délégation ou sous le contrôle opérationnel du COMCYBER, un rôle opérationnel renforcé, et ce dès le temps de la compétition.

Au cours des 5 dernières années, l'armée de Terre, à travers un effort important de recrutement et de formation, s'est positionnée comme le principal pourvoyeur de ressources humaines et de compétences cyber des armées. Elle a également structuré son aptitude à se défendre. Il s'agit désormais pour l'armée de Terre de développer ses capacités sur le segment « Engager », qui correspond aux doctrines de L2I et de LIO.

Pour atteindre cet objectif, l'armée de Terre a initié une transformation de l'organisation de sa chaîne de commandement cyber. Une évolution majeure est la densification de la chaîne cyber opérative et tactique avec les créations par transformation des commandements des actions spéciales terre (ancien COMFST), commandement des actions dans la profondeur et du renseignement (ancien COMRENS) et commandement de l'appui terrestre numérique et cyber (ancien COMSIC) qui développeront, entraîneront et assureront l'engagement des capacités permettant de délivrer des effets cyber intégrés à la manœuvre interarmes ou de participer à une opération interarmées dans le cyberespace. Pour assurer la permanence des missions confiées par l'échelon stratégique, un commandement opérationnel « influence » dans le domaine de la L2I et un commandement opérationnel « sécurité du numérique » dans le domaine de la LID seront également créés.

Le commandement des forces opérationnelles terrestres (CFOT) est pour sa part chargé de concrétiser au sein des forces terrestres la nouvelle ambition Cyber Terre, avec pour seul objectif les opérations. À ce titre, au-delà du pilotage de l'action des trois commandements cités précédemment, il structurera les processus permettant d'opérationnaliser le C2 cyber au sein des forces terrestres et sa totale

intégration avec la chaîne interarmées. Il est également le garant de la préparation opérationnelle au cyber et du cyber à tous les niveaux.

Enfin, un officier général du numérique et du cyber, appuyé par un bureau cyber à l'EMAT, a été désigné pour contrôler la réalisation de cette ambition. Le périmètre d'action de l'OGNUM « cyber » concerne l'ensemble des systèmes numérisés de l'armée de Terre (SIAG, SIOC et SA), la conception et la conduite de la politique numérique de l'armée de Terre et la réalisation de l'ambition Cyber Terre. Le positionnement et les responsabilités (capacitaires, finances, ressources humaines, animation des trois domaines de lutte, homologations...) du bureau cyber de l'EMAT en font l'interface unique d'entrée et de sortie de l'EMAT pour les sujets cyber.

Le COMCYBER, en tant qu'autorité fonctionnelle du périmètre EMA, est l'interlocuteur interarmées privilégié. L'essentiel des travaux des armées est réalisé en concertation avec le COMCYBER. Les relations avec les autres armées, directions et services sont davantage de l'ordre de la coordination (échanges de RETEX, bonnes pratiques, procédés, *etc.*), ou de la comitologie (capacitaire, doctrinale, ressources humaines, *etc.*), mais il existe en réalité peu d'interactions officielles directes avec ces derniers.

Sur les sujets capacitaires, portés par le PEM Cyber, l'EMAT participe aux différents travaux pilotés par la division « cohérence capacitaire » de l'EMA afin de porter les besoins spécifiques de son action cyber « au sol ». En phase de réalisation, les incréments du PEM Cyber sont conduits par le COMCYBER, en collaboration avec les armées. Concernant les programmes d'armement spécifiques de l'armée de Terre, l'armée de Terre collabore étroitement par sa chaîne capacitaire avec la DGA dans le cadre de la cyberprotection, de l'homologation et des choix techniques de LID de ses systèmes numérisés.

Enfin, l'EMAT travaille en collaboration avec les SOC régionaux de la DIRISI pour le suivi des contrôles de cyberprotection réalisés dans les formations d'emploi de l'armée de Terre et la réalisation des plans d'actions de remédiation.

ii. L'armée de l'Air et de l'Espace

Au sein de l'armée de l'Air et de l'Espace, l'organisation de la cyberdéfense repose sur plusieurs niveaux :

1/ l'état-major de l'armée de l'Air et de l'Espace, en charge de la gouvernance haute comprenant le capacitaire, les ressources humaines et les finances, sous la tutelle de l'OGNUM de l'armée de l'Air et de l'Espace en tant qu'autorité cyber de l'armée de l'Air et de l'Espace ;

2/ la DSI, en charge de la conduite du volet cyberprotection (SSI) et de l'animation du volet LID, en lien avec le CDAOA ;

3/ le CDAOA, en charge de la planification et de la conduite des opérations de cyberdéfense (LID, L2I et LIO) et de l'intégration de la manœuvre cyber dans les opérations aériennes et spatiales. Ces activités ne se limitent pas au périmètre du CDAOA et sont menées au profit de l'ensemble des capacités opérationnelles de l'armée de l'Air et de l'Espace (CDAOA, CDE, CFAS) ;

4/ les unités cyber, pour l'exécution des missions (audits, tests d'intrusion, SOC…) ;

5/ les unités non cyber de l'armée de l'Air et de l'Espace, qui ont vocation à compléter leurs capacités classiques avec des capacités cyber (unités de ROEM ou des forces spéciales air), qui font partie de la communauté cyber des armées.

Cette organisation et la répartition des responsabilités dans le domaine opérationnel s'appuient sur une doctrine décrivant les principes d'intégration des opérations cyber avec les opérations aériennes ou spatiales. L'armée de l'Air et de l'Espace agit sur le périmètre du CEMA, en respectant les directives du ministère et du COMCYBER, et avec certaines délégations.

En matière de cyberprotection, l'état-major de l'armée de l'Air et de l'Espace rend compte au COMCYBER et agit par délégation en tant qu'autorité d'homologation principale des systèmes employés par l'armée de l'Air et de l'Espace. Le cadre normatif interministériel est décliné sous le pilotage de la DPID, en prenant en compte les spécificités du ministère. La DGA, en sa qualité d'expert technique ministériel en sécurité numérique, appuie l'armée de l'Air et de l'Espace sur le volet capacitaire et sur l'expertise technique.

En matière d'opérations cyber, l'armée de l'Air et de l'Espace a adopté une organisation en miroir du COMCYBER afin de faciliter le plus possible l'interopérabilité et lui permettre d'être en relation permanent avec le COMCYBER. L'organisation mise en place dans l'armée de l'Air et de l'Espace permet ainsi la mise en œuvre, au besoin, d'un certain niveau de subsidiarité, qui doit encore progresser, et des processus de délégation qui sont déjà en place et en cours de consolidation. Le COMCYBER conserve dans tous les cas une autorité fonctionnelle dans les opérations cyber et peut choisir de déléguer la conception opérationnelle de certaines opérations à l'armée de l'Air et de l'Espace dans son domaine de compétence.

À cet effet, un officier de lutte cyber électronique (OLCE) est désigné au sein de l'armée de l'Air et de l'Espace pour assurer, en lien avec le pôle « opérations » du COMCYBER, la planification et la conduite des opérations qui sont déléguées à l'armée de l'Air et de l'Espace ou exprimer au COMCYBER les effets cyber dont a besoin la composante aérienne ou spatiale. Il est l'interlocuteur du chef du pôle « opérations » du COMCYBER. Le centre des opérations cyber électroniques de l'armée de l'Air et de l'Espace (COCEA) l'appuie dans ses fonctions, en lien avec le COMCYBER. Enfin, les capacités d'engagement de

l'armée de l'Air et de l'Espace sont en lien avec les unités opérationnelles du COMCYBER telles que le CALID.

Les liens opérationnels avec les autres armées sont assurés par l'OLCE avec ses homologues. Des échanges informels sont réguliers et les échanges formels sont généralement réalisés sous couvert du COMCYBER. Des relations existent avec les autres armées, directions et services, en matière de partages de bonnes pratiques, de retour d'expérience, d'informations sur les menaces et les incidents. Que ce soit en matière d'homologation ou de défense, l'armée de l'Air et de l'Espace s'inscrit en tant qu'expert des domaines aéronautique et spatial et s'appuie sur les capacités complémentaires de la DIRISI.

iii. La Marine

L'organisation en place au sein de la Marine consiste en un échelon de coordination et sept domaines qui sont tous sous la responsabilité d'un officier général de l'échelon central, membre du COMEX de la Marine :

1/ le domaine « ressources humaines » ;

2/ le domaine « capacitaire » ;

3/ le domaine « sécurité numérique et sécurité des systèmes d'information »

4/ le domaine des « opérations cyber » ;

5/ le domaine du maintien en condition de sécurité ;

6/ le domaine des homologations ;

7/ et le domaine des partenariats.

Chacun de ces domaines dispose d'une comitologie qui lui est propre.

3. Deux acteurs principaux au-delà du ministère des Armées : l'ANSSI et la DGSI

a. L'ANSSI, autorité chargée de la sécurité des systèmes d'information de l'État

Service à compétence nationale (SCN), l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a été créée par décret en 2009 (1). Elle est rattachée au Secrétariat général de la défense et de la sécurité nationale (SGDSN), qui assiste le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale. L'ANSSI comprenait environ 660 ETP en 2023.

(1) Décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information ».

Aux termes de l'article L. 2321-1 du code de la défense, « *dans le cadre de la stratégie de sécurité nationale et de la politique de défense, le Premier ministre définit la politique et coordonne l'action gouvernementale en matière de sécurité et de défense des systèmes d'information. Il dispose à cette fin de l'ANSSI qui assure la fonction d'autorité nationale de défense des systèmes d'information* ». La principale mission de l'ANSSI est dès lors d'assurer la sécurité des systèmes d'information de l'État et de veiller à celle des administrations, des opérateurs d'importance vitale (OIV) et des opérateurs de services essentiels (OSE), auprès desquels elle exerce par ailleurs une mission de conseil et de soutien.

L'article 3 du décret susmentionné précise les missions de l'ANSSI :

– elle assure la fonction d'autorité nationale de défense des systèmes d'information. En cette qualité, elle propose au Premier ministre les mesures destinées à répondre aux crises affectant ou menaçant la sécurité des systèmes d'information des autorités publiques et des opérateurs d'importance vitale et elle coordonne, dans le cadre des orientations fixées par le Premier ministre, l'action gouvernementale en matière de défense des systèmes d'information ;

– elle anime et coordonne les travaux interministériels en matière de sécurité des systèmes d'information ;

– elle élabore les mesures de protection des systèmes d'information proposées au Premier ministre. Elle veille à l'application des mesures adoptées ;

– elle mène des inspections des systèmes d'information des services de l'État et d'opérateurs publics ou privés ;

– elle met en œuvre des dispositifs de détection des événements susceptibles d'affecter la sécurité des systèmes d'information de l'État, des autorités publiques et d'opérateurs publics et privés et coordonne la réaction à ces événements ;

– elle recueille les informations techniques relatives aux incidents affectant les systèmes d'information des personnes mentionnées à l'alinéa précédent. Elle peut apporter son concours pour répondre à ces incidents ;

– elle délivre des agréments aux dispositifs et aux mécanismes de sécurité destinés à protéger, dans les systèmes d'information, les informations couvertes par le secret de la défense nationale ;

– elle participe aux négociations internationales et assure la liaison avec ses homologues étrangers ;

– et elle assure la formation des personnels qualifiés dans le domaine de la sécurité des systèmes d'information.

La direction de l'ANSSI est constituée d'un directeur général, M. Vincent Strubel, nommé par le Premier ministre sur décret, et d'un directeur général adjoint,

assistés par un directeur de cabinet et un chef de cabinet. Pour répondre à ses missions, l'ANSSI est organisée en 4 sous-directions :

– la sous-direction « opérations » (SDO), qui assure, au niveau opératif et tactique, la mise en œuvre de la fonction d'autorité de défense des systèmes numériques d'intérêt pour la nation dévolue à l'ANSSI. Elle constitue à ce titre le centre opérationnel de la sécurité des systèmes d'information. Cette sous-direction assure les fonctions de CERT (1) gouvernemental et national français et, à ce titre, le sous-directeur « opérations » porte le titre de chef du CERT-FR ;

– la sous-direction « expertise » (SDE), qui porte la mission globale d'expertise et d'assistance technique de l'agence. Elle apporte son soutien à l'ensemble des autres sous-directions de l'ANSSI, aux ministères, aux industriels et prestataires de la sécurité et aux OIV ;

– la sous-direction « stratégie », qui anime, de manière transverse, le processus de planification stratégique, la contribution de l'agence à l'élaboration et à la mise en œuvre des politiques publiques en faveur de la sécurité du numérique, communique vers l'ensemble des publics de l'ANSSI et développe l'animation du réseau de ses partenaires-clés ;

– et la sous-direction « administration », qui est responsable de la programmation et de l'exécution des activités de soutien et d'administration de l'ANSSI.

b. La DGSI

Membre du premier cercle des services de renseignement, la DGSI est la seule entité qui peut exercer sa mission de cyberdéfense sur le territoire national aussi bien dans un cadre judiciaire que de renseignement.

Lorsqu'une cyberattaque menace les intérêts fondamentaux de la Nation, la DGSI, agissant au titre de ses missions de contre-ingérence, de contre-espionnage et de contre-terrorisme, peut mettre en œuvre des techniques de renseignement dans le cadre de ses investigations.

Plus spécifiquement, la DGSI suit les modes opératoires cyber susceptibles de porter atteinte aux intérêts fondamentaux de la Nation et agit, de manière proactive ou réactive, pour contrer ces menaces.

(1) Computer Emergency Response Team.

SECONDE PARTIE : LES 6 DÉFIS À RELEVER POUR DOTER LA FRANCE D'UNE CYBERDÉFENSE DE PREMIER PLAN

I. LE DÉFI DE LA GOUVERNANCE : ADAPTER L'ORGANISATION DE LA CYBERDÉFENSE DE L'ÉTAT POUR UNE NATION CYBER-RÉSILIENTE

1. Une menace évolutive qui ne cesse de croître et de se complexifier

Selon l'ANSSI, la menace informatique se maintient à un niveau élevé avec 831 intrusions avérées portées à sa connaissance en 2022 contre 1 082 en 2021. Si ce nombre est inférieur à celui de 2021, cela ne saurait être interprété comme une baisse du niveau de la menace. En effet, si une chute de l'activité liée aux rançongiciels a bien été observée par l'ANSSI sur les opérateurs régulés publics et privés, à l'exception des hôpitaux, elle n'illustre pas l'évolution générale de cette menace cyber qui se maintient à un niveau élevé en se déportant sur des entités moins bien protégées, en premier lieu desquelles les structures hospitalières, les collectivités locales et les PME.

Les attaques associées à un objectif de gain financier demeurent les plus courantes. Après une baisse observée au premier semestre 2022, l'ANSSI a constaté une multiplication des cas d'attaques par rançongiciels depuis l'été 2022, en particulier à l'encontre des collectivités territoriales et des établissements de santé, avec des impacts souvent conséquents sur le fonctionnement de ces entités. Les autres activités cybercriminelles comme les arnaques, les services de vente d'accès à des systèmes d'information ou de programmes malveillants à la demande et le cryptominage se sont maintenues.

L'espionnage informatique perdure également à un niveau élevé, tant en France que dans le monde. Il constitue la catégorie de menace qui a le plus sollicité les équipes de l'ANSSI en 2022. La majorité des cas traités par l'agence continue à impliquer des modes opératoires associés en source ouverte à la Chine. Ces intrusions répétées de modes opératoires étrangers témoignent d'un effort continu pour s'introduire dans les réseaux d'entreprises stratégiques françaises, souvent des OIV ou des OSE. L'ANSSI a également constaté une tendance aux attaques sur la chaîne d'approvisionnement dans lesquelles les acteurs malveillants visent les entreprises, les partenaires, les sous-traitants, les prestataires et les organisations de tutelle, au niveau de sécurité plus faible que leurs cibles finales, dans le cadre de campagnes d'espionnage global au long cours.

L'agression de la Russie contre l'Ukraine a également été favorable à des campagnes d'espionnage stratégique au cours de l'année 2022, à l'encontre des pays européens et des membres de l'OTAN. Ce conflit armé a fourni un contexte propice

à des actions de déstabilisation en Europe, dont des campagnes menées par des activistes soutiens des belligérants. Si les attaques par sabotage informatique ont été, jusqu'à présent, relativement circonscrites au théâtre du conflit, d'autres modes d'actions tels que des attaques en déni de service distribué, des défigurations de sites Internet ou des opérations informationnelles associées à des exfiltrations de données ont affecté de nombreuses victimes en Europe et en Amérique du Nord, y compris en France.

Du fait de sa massification, la cybercriminalité devient un sujet de sécurité nationale. Les attaquants se sont adaptés et ont su saisir de multiples opportunités offertes par le contexte géopolitique, la généralisation d'usages numériques mal maîtrisés, les faiblesses de sécurisation des données et l'application tardive des correctifs de sécurité par les utilisateurs.

L'évolution de l'écosystème cybercriminel au cours des dernières années s'est également distinguée par une professionnalisation et une spécialisation des acteurs, cause et conséquence des gains financiers acquis. Cette évolution s'illustre au travers d'offres de services spécifiques comme les rançongiciels vendus en tant que services, les ventes d'accès à des systèmes d'information ou encore les solutions d'hébergement dites *bullet proof*.

L'ANSSI a assisté, ces derniers mois, à l'évolution de la menace cybercriminelle du point de vue :

1/ technique avec une convergence des outils et des techniques des attaquants de nature stratégique et de ceux des criminels cyber ;

2/ de l'ampleur de la menace avec un passage à l'échelle des acteurs cybercriminels, permettant par exemple de cibler massivement tout un secteur d'activité, voir un pays entier. Cette menace touche de plus en plus d'établissements de santé, de collectivités territoriales et de PME alors qu'elle affectait il y a quelques années plutôt des organisations importantes (en taille, en visibilité, en ressources) ;

3/ des sources de vulnérabilités : si l'essentiel des attaques s'appuie toujours sur des vulnérabilités logicielles, pourtant le plus souvent connues et pour lesquelles des correctifs existent mais n'ont pas été appliqués, d'autres attaques ciblant des nouveaux usages mal maîtrisés sont également apparues. Ainsi, la migration de systèmes d'information dans le cloud, lorsqu'elle est mal appréhendée par les responsables de ces systèmes et fait l'objet d'hypothèses implicites non vérifiées (sur la prise en charge des mises à jour par le prestataire de cloud par exemple), peut créer de nouvelles vulnérabilités ;

4/ de la stratégie des attaquants, qui ciblent de plus en plus les sous-traitants et les fournisseurs au niveau de sécurité le plus faible, qui sont les vecteurs privilégiés des groupes cybercriminels et qui se répercutent largement sur toute la chaîne de valeur, susceptible de produire des effets en cascade ;

5/ et de son agilité et de sa capacité d'adaptation aux évolutions technologiques ou aux stratégies de réponse mises en œuvre.

2. Une gouvernance complexe coordonnée à l'échelle nationale par le SGDSN, autorité de tutelle de l'ANSSI, et le C4

Sous l'autorité du SGDSN, l'ANSSI est chargée de la mise en place et de l'animation de la gouvernance cyber de l'État en matière de LID et de politique publique cyber. C'est le rattachement de l'agence aux services de la Première ministre qui lui permet d'assurer légitimement et avec pertinence ce rôle de coordinatrice.

Cette gouvernance s'organise autour des trois piliers suivants :

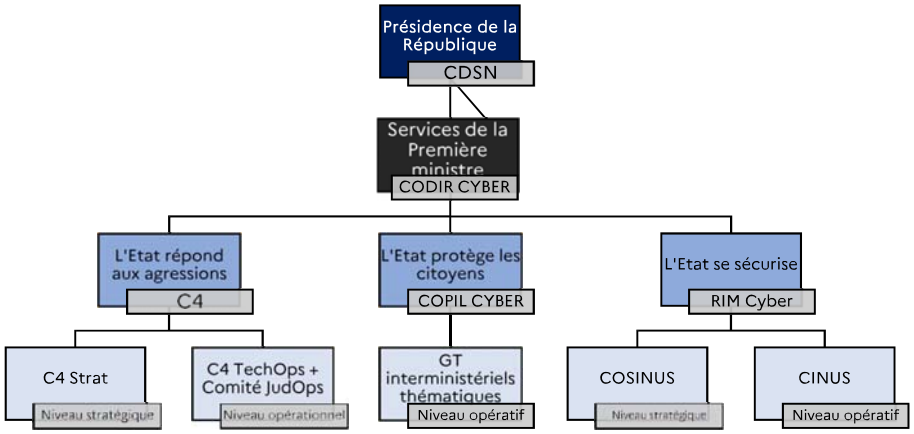
1/ « l'État se sécurise », a pour objectif de travailler à la cybersécurisation des ministères avec la mise en place de dispositifs d'accompagnement adaptés au contexte de chaque administration. Parmi les enjeux, on peut notamment mentionner l'amélioration de leur connaissance des enjeux cyber, leur responsabilisation ou encore la mutualisation de leurs efforts et leur autonomisation. Ce volet engage notamment pleinement le renforcement de la coordination entre l'ANSSI et la Direction interministérielle du numérique (DINUM).

2/ « l'État protège la Nation », a pour objectif de piloter les travaux interministériels visant à mieux prendre en compte les enjeux de sécurité numérique dans les politiques publiques afin de protéger les Français. L'ANSSI contribue notamment à la mise en place de politiques ambitieuses en matière de sécurité des entreprises et des citoyens, d'emploi et de compétences, de recherche et d'innovation et de coopération et de régulation européennes et internationales.

3/ « l'État répond aux agressions », permet d'organiser la réponse interministérielle de l'État aux agressions cyber dans le cadre du C4.

Cette gouvernance se traduit par une organisation qui lui permet de réunir les acteurs de l'État au bon niveau selon les enjeux (voir le schéma ci-dessous).

Schéma représentant les instances de la gouvernance cyber en France

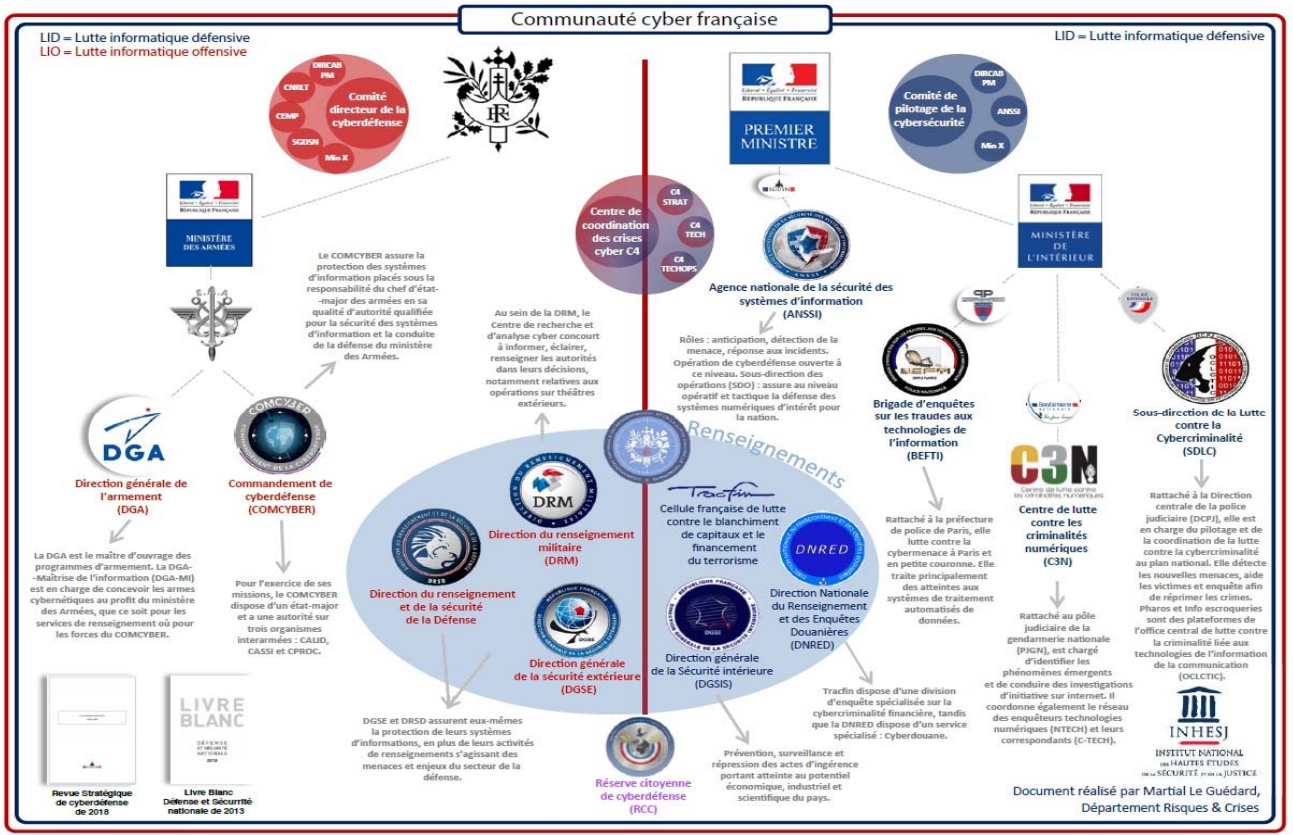


Source : ANSSI

Au-delà du C4 et de l'ANSSI, le schéma ci-après présente l'organisation de la cyberdéfense entendue au sens de la LID et de la LIO. Il convient de noter toutefois que ce schéma date de 2020 et qu'à ce titre, plusieurs informations sont manquantes :

1/ il ne traite que de la LIO et de la LID, la L2I étant apparue plus tardivement, en 2021 ;

2/ certaines entités du ministère de l'Intérieur telles que le COMCyberGEND, créé en février 2021, n'apparaissent pas non plus, pour les mêmes raisons.


Communauté cyber française
LID = Lutte informatique défensive
LIO = Lutte informatique offensive
LID = Lutte informatique défensive
Comité directeur de la cyberdéfense
DIRCAB PM
CNRLT
CEMP
SGDSN
Min X
PREMIER MINISTRE
Comité de pilotage de la cybersécurité
DIRCAB PM
ANSSI
Min X
MINISTÈRE DES ARMÉES
MINISTÈRE DE L'INTÉRIEUR
Centre de coordination des crises cyber C4
C4 STRAT
C4 TECH
C4 TECHOPS
Agence nationale de la sécurité des systèmes d'information (ANSSI)
Rôles : anticipation, détection de la menace, réponse aux incidents. Opération de cyberdéfense ouverte à ce niveau. Sous-direction des opérations (SDO) : assure au niveau opératif et tactique la défense des systèmes numériques d'intérêt pour la nation.
Le COMCYBER assure 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 et la conduite de la défense du ministère des Armées.
Au sein de la DRM, le Centre de recherche et d'analyse cyber concourt à informer, éclairer, renseigner les autorités dans leurs décisions, notamment relatives aux opérations sur théâtres extérieurs.
DGA
Direction générale de l'armement (DGA)
La DGA est le maître d'ouvrage des programmes d'armement. La DGA--Maîtrise de l'information (DGA-MI) est en charge de concevoir les armes cybernétiques au profit du ministère des Armées, que ce soit pour les services de renseignement où pour les forces du COMCYBER.
COMCYBER
Commandement de cyberdéfense (COMCYBER)
Pour l'exercice de ses missions, le COMCYBER dispose d'un état-major et a une autorité sur trois organismes interarmées : CALID, CASSI et CPROC.
Renseignements
DRM
Direction du renseignement militaire (DRM)
Direction du renseignement et de la sécurité de la Défense
Direction générale de la sécurité extérieure (DGSE)
DGSE et DRSD assurent eux-mêmes la protection de leurs systèmes d'informations, en plus de leurs activités de renseignements s'agissant des menaces et enjeux du secteur de la défense.
Tracfin
Cellule française de lutte contre le blanchiment de capitaux et le financement du terrorisme
DNRED
Direction Nationale du Renseignement et des Enquêtes Douanières (DNRED)
Direction générale de la Sécurité intérieure (DGSIS)
Tracfin dispose d'une division d'enquête spécialisée sur la cybercriminalité financière, tandis que la DNRED dispose d'un service spécialisé : Cyberdouane.
Prévention, surveillance et répression des actes d'ingérence portant atteinte au potentiel économique, industriel et scientifique du pays.
Réserve citoyenne de cyberdéfense (RCC)
Brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI)
Rattaché à la préfecture de police de Paris, elle lutte contre la cybermenace à Paris et en petite couronne. Elle traite principalement des atteintes aux systèmes de traitement automatisés de données.
C3N
Centre de lutte contre les criminalités numériques (C3N)
Rattaché au pôle judiciaire de la gendarmerie nationale (PJGN), est chargé d'identifier les phénomènes émergents et de conduire des investigations d'initiative sur internet. Il coordonne également le réseau des enquêteurs technologies numériques (NTECH) et leurs correspondants (C-TECH).
Sous-direction de la Lutte contre la Cybercriminalité (SDLC)
Rattaché à la Direction centrale de la police judiciaire (DCPJ), elle est en charge du pilotage et de la coordination de la lutte contre la cybercriminalité au plan national. Elle détecte les nouvelles menaces, aide les victimes et enquête afin de réprimer les crimes. Pharos et Info escroqueries sont des plateformes de l'office central de lutte contre la criminalité liée aux technologies de l'information de la communication (OCLCTIC).
INHESJ
INSTITUT NATIONAL DES HAUTES ÉTUDES DE LA SÉCURITÉ ET DE LA JUSTICE
LIVRE BLANC
Revue Stratégique de cyberdéfense de 2018
Livre Blanc Défense et Sécurité nationale de 2013
Document réalisé par Martial Le Guédard, Département Risques & Crises

3. Une spécificité organisationnelle : l'ANSSI n'est pas compétente pour les SI du ministère des Armées

Cette spécificité s'explique par la nature des missions de ce ministère, notamment le caractère très spécifique des solutions numériques sous-tendant les systèmes d'armes, qui nécessite une expertise propre, ainsi que le contexte d'emploi particulier de ces systèmes, en particulier dans le cadre d'opérations extérieures. La délégation dont bénéficie le COMCYBER permet au ministère des Armées de bénéficier d'une chaîne de LID sous statut et commandement militaires, plus adaptés à ce contexte d'emploi, et disposant d'une expertise spécifique dont la mutualisation avec l'interministériel ne présenterait pas d'intérêt.

Ces missions déléguées s'exercent naturellement en coordination étroite avec l'ANSSI, en particulier en ce qui concerne l'analyse de la menace et la mise en place d'outils techniques et méthodologiques communs.

4. Des relations nourries entre le ministère des Armées et l'ANSSI

a. Au sein du C4

En tant qu'autorité nationale en matière de défense et de sécurité des systèmes d'information, l'ANSSI échange régulièrement avec les différents services du ministère des Armées sur la cybersécurité de leurs propres réseaux et celle de la BITD, en particulier avec la DGA, le COMCYBER, la DGSE et la DRSD.

Ces relations se matérialisent notamment au sein du centre de coordination des crises cyber (C4) qui est animé par l'ANSSI et auquel participent notamment le COMCYBER, la DGA, la DGSI et la DGSE. Cette instance de défense est une enceinte interministérielle, partagée entre un niveau stratégique, le C4 Strat, dont la mission vise à assurer l'analyse de la menace relative aux agressions cyber et à préparer les stratégies globales de réponse, et un niveau opérationnel, parmi lesquels le Comité JudOps, pour l'articulation des autorités judiciaires et des services enquêteurs, ainsi que le C4 TechOps, dont l'objectif est la conduite des travaux opérationnels de qualification et de traitement des incidents d'ampleur.

b. Le truchement de la règle dite des 4i

Comme l'a indiqué le COMCYBER, la règle dite des 4i s'applique au domaine cyber comme à n'importe quel autre domaine dans lequel les armées ont des capacités d'intervention. Si les capacités de l'ANSSI devaient se révéler inexistantes, insuffisantes, inadaptées ou indisponibles, elle pourrait formuler une demande de concours auprès du ministère des Armées. Selon le COMCYBER, les capacités de l'ANSSI sont pour l'heure existantes, suffisantes, adaptées et disponibles, mais il est effectivement possible d'imaginer un scénario dans lequel ses capacités seraient dépassées par de multiples attaques, et se trouveraient de fait

insuffisantes et/ou indisponibles. Le COMCYBER a indiqué n'avoir jamais eu à intervenir au profit d'une collectivité territoriale, d'une entreprise du secteur civil ou d'un établissement de santé ; la responsabilité de ces organisations relevant du périmètre de l'ANSSI et la règle des 4i n'ayant jamais eu à s'appliquer.

Du point de vue du COMCYBER, les priorités de la cyberdéfense dans les armées doivent demeurer :

1/ la protection (y compris le chiffre) et la défense des SI du ministère des Armées, ainsi que la résilience des capacités opérationnelles (dont celles engagées pour et sur le TN, dans le cadre des JOP 2024 par exemple) ;

2/ les opérations militaires dans le cyberespace (LID, LIO, L2I) ;

3/ éventuellement, un appui envisageable à l'ANSSI au cas par cas dans le volet réponse à incident.

Ce dernier point est à l'étude dans le cadre d'un protocole pour les JOP 2024. S'il est trop tôt pour en connaître la teneur finale, le protocole visera à cadrer un éventuel soutien à l'ANSSI en cas d'événement cyber majeur : sur la base d'une demande de concours, un Groupe d'Intervention Cyber du ministère des Armées pourra être projeté sous pilotage de l'ANSSI. Le COMCYBER étudie également la mise à disposition temporaire de personnel au profit de l'ANSSI. Élaboré sur le fondement des procédures déjà applicables, mais adapté aux spécificités de JOP afin d'en améliorer la réactivité et la pertinence, le protocole aura vocation, s'il a donné satisfaction, à perdurer.

En outre, l'ANSSI et le COMCYBER élaborent actuellement un projet de convention de partenariat visant à préciser les principes selon lesquels le COMCYBER pourra apporter son soutien aux équipes opérationnelles de l'ANSSI dans le contexte d'une crise majeure d'origine cyber. Ce soutien pourrait intervenir aux bénéfices de toute organisation, publique ou privée, victime d'une cyberattaque sur le territoire national. Cette convention est en cohérence avec la règle des 4i, même si le ministère des Armées n'est, pour l'heure, pas intervenu en soutien de l'ANSSI sur le fondement de cette doctrine. Dans le cadre de son intervention au Monténégro, l'ANSSI a sollicité l'appui du COMCYBER dans un objectif de coopération et de renforcement des effectifs. Cette participation du COMCYBER a été jugée très satisfaisante par les deux parties et a notamment permis de tester la coordination entre l'ANSSI et le COMCYBER en contexte opérationnel réel.

5. La création de la communauté cyber des armées

Annoncée en filigrane lors des débats sur la LPM 2024-2030, la création d'une « communauté cyber des armées » a été officialisée en novembre 2023. En effet, au-delà des moyens financiers et humains, le COMCYBER indiquait en avril 2023 qu'un effort particulier serait fait pour adapter les modalités et les niveaux d'action de la cyberdéfense. Si certaines actions peuvent être conduites de

loin dans le cyberespace, d'autres nécessitent d'être à proximité des cibles, en particulier dans le domaine de la guerre électronique pour les capacités de brouillage. Or, dans le domaine de la LIO et de la L2I, il convient de « *descendre d'un niveau car si le niveau stratégique est bien construit, [il faut] désormais mieux appuyer les armées au niveau tactique afin d'agir sur le terrain au plus près de l'ennemi* » (1). Le COMCYBER indiquait également lors de son audition devant la commission de la Défense nationale et des forces armées qu'il souhaitait « *descendre vers les échelons opératif et tactique [en matière de LIO et de L2I], pour mieux appuyer les armées avec les outils et les capacités [que le ministère des Armées a] développés* » (2).

Il s'agit d'un véritable enjeu pour les trois armées qui vont devoir, progressivement, s'approprier des outils qui seront mis à leur disposition par le COMCYBER, de manière maîtrisée. À titre d'exemple, s'agissant de l'armée de Terre, celle-ci a défini une ambition Cyber Terre 2024-2030 qui comprend un volet de consolidation de sa sécurité numérique avec la création d'une seconde unité de LID, et un volet développement de son aptitude à engager l'adversaire, essentiellement sur les niveaux opératifs et tactiques, en L2I et en LIO grâce à la création d'une unité dédiée à la lutte contre l'hybridité. Il s'agit de mettre en œuvre les mécanismes qui permettront à l'armée de Terre de planifier et de produire, dès la phase de compétition, des effets dans les trois domaines de lutte, tout en renforçant sa résilience numérique. Pour proposer des moyens durcis au profit de la cyberdéfense dès le temps de la compétition, plusieurs décisions d'ampleur ont été prises parmi lesquelles :

1/ la transformation et la densification de son organisation de commandement cyber ;

2/ le renforcement en effectifs des premières unités cyber que sont la 807e compagnie de transmissions qui assure la supervision des SI au niveau tactique et met en œuvre la LID de l'armée de Terre, le 54e régiment du train et la 785e compagnie de guerre électronique spécialisés dans les actions cyber-électroniques, et le CIAE qui est l'effecteur de la L2I au sein des armées ;

3/ la volonté d'une prise en compte native de la LID dans tous les programmes d'armement (développement de la LID embarquée) ;

4/ le renforcement des unités concourantes au cyber, comme par exemple le centre du renseignement Terre pour exploiter les données cyber en appui de la DRM et du COMCYBER ;

---

(1) Thomas Gassilloud (président), Yannick Chenevard et Laurent Jacobelli (rapporteurs), Rapport d'information sur le bilan de la loi de programmation militaire 2019-2025, 15 février 2023 : https://www.assemblee-nationale.fr/dyn/16/rapports/cion_def/l16b0864_rapport-information#.

(2) Compte-rendu de l'audition à huis clos de M. le général de division Aymeric Bonnemaison, commandant de la cyberdéfense, devant la commission de la Défense nationale et des forces armées sur le projet de loi de programmation militaire pour les années 2024 à 2030 du jeudi 13 avril 2023 : https://www.assemblee-nationale.fr/dyn/16/comptes-rendus/cion_def/l16cion_def2223064_compte-rendu#.

5/ et surtout, la création de nouvelles unités cyber. Il s'agit de la 712e compagnie de transmissions, dédiée à la contre hybridité, et de la 808e compagnie de transmissions pour l'expertise défense cyber, à travers le développement des capacités d'entraînement de LID et l'aptitude à pénétrer et à évoluer dans les réseaux amis (*Red Team*).

6. Les limites du modèle centralisé : pour une diffusion de la cybersécurité dans les territoires

a. L'ANSSI peut-elle gérer toute la cybersécurité des entités publiques ?

Interrogée sur ses effectifs, l'ANSSI a indiqué que des progrès considérables ont été accomplis par l'État pour faire face à la menace cyber du point de vue défensif, sous-tendus par une montée en puissance régulière et forte des moyens alloués à l'ANSSI. La trajectoire d'emploi prévue par l'agence, qui vise à atteindre 660 agents en 2023 et plus de 800 agents à horizon 2027, répond au besoin de l'agence de poursuivre sa politique RH lui permettant de se doter d'experts et de profils aux compétences techniques extrêmement variées.

L'enjeu des effectifs et moyens déployés au sein de l'État pour répondre à la menace cyber est réel. Celui-ci ne concerne pas uniquement les effectifs déployés à l'ANSSI mais l'ensemble des acteurs qui sont directement impliqués dans la sécurité des systèmes d'information des infrastructures étatiques comme les OIV et les OSE, et plus généralement les effectifs consacrés au développement et à l'exploitation des infrastructures numériques de ces différents acteurs. En effet, pour remplir ses missions, l'ANSSI doit également pouvoir s'appuyer sur des équipes et notamment des DSI robustes.

Toutefois, le recours par l'ANSSI à des PRIS, c'est-à-dire à des entreprises privées, en cas de survenance d'une cyberattaque d'un niveau de criticité jugé insuffisamment élevé pour justifier une intervention directe de l'ANSSI, est un révélateur de la limite du système. Aujourd'hui, lorsqu'une entité du secteur civil, que ce soit une collectivité territoriale ou un établissement de santé, est victime d'une cyberattaque, l'ANSSI n'intervient pas systématiquement et de manière totale. Plusieurs entreprises ont été qualifiées par l'ANSSI pour intervenir et procéder à la remédiation des systèmes d'information affectés par une cyberattaque. Il s'agit des entreprises Advens, Intrinsec Sécurité, Lexfo, Orange Cyberdéfense, PwC Advisory, Thales Cyber Solutions et Wavestone.

Si le recours à des entreprises privées qui va facturer sa prestation à l'entité visée pour remédier à une cyberattaque n'est pas négatif en soi, il faut tout de même préciser que cela est notamment la conséquence du faible niveau des effectifs de l'ANSSI, et singulièrement de son CERT, qui ne pourrait de toute façon pas faire face au nombre de cyberattaques qui frappent les entités relevant de sa responsabilité. Cette situation est d'autant plus alarmante que la transposition de la directive NIS 2 va augmenter significativement le nombre d'OIV et d'OSE sous la

supervision de l'ANSSI, ce qui ne fera qu'accroître la charge de travail qui pèsera sur ses épaules.

D'aucuns pourraient plaider pour un renforcement des effectifs de l'ANSSI, y compris de son CERT, pour faire face à cette situation. Mais cette solution ne pourrait de toute façon pas résoudre le problème de fond, à moins d'augmenter de manière exponentielle les effectifs de l'Agence, ce qui n'est ni réaliste, ni nécessairement souhaitable car des effectifs supplémentaires doivent pouvoir être correctement intégrés par l'entité d'accueil. En réalité, en parallèle d'une augmentation des effectifs du CERT de l'Agence, il conviendrait surtout de diffuser la culture de la cybersécurité dans les territoires, au plus près des citoyens. L'ANSSI édite des guides, à destination, par exemple, des maires pour les sensibiliser à ce risque et les inciter à adopter les bonnes pratiques. Mais ces guides sont d'une grande complexité et souffrent d'un manque de lisibilité patent.

Les armées, qui ont cette culture et les compétences nécessaires, pourraient être davantage sollicitées pour partager leur savoir-faire aux entités du secteur civil (collectivités territoriales et leurs établissements publics, établissements de santé, mais également OIV et OSE) frappées par une cyberattaque. Contrairement à ce qui a pu être dit lors d'auditions, le travail en commun de militaires et de civils dans les collectivités territoriales ou dans les établissements de santé ne poserait aucune difficulté, les différences de culture, réelles ou supposées, entre les deux mondes n'étant pas nécessairement un facteur de complication mais plutôt une richesse.

Le sujet de la cybersécurité est encore trop perçu comme un sujet complexe, technique, réservé aux experts et pas suffisamment politique. Le niveau d'insouciance quant au risque cyber reste malheureusement encore trop élevé dans le secteur civil et constitue rarement une priorité. Il est temps que ce sujet soit pris au bon niveau politique, c'est-à-dire au niveau interministériel. La politique de cyberdéfense de l'État gagnerait à être plus lisible et devrait être appréhendée de manière globale pour renforcer la cyber-résilience de la Nation. La culture de la cybersécurité ne peut pas se décréter depuis un sommet et diffuser au sein de la société sans cette approche globale.

b. Franchir une nouvelle étape pour la cybersécurité des collectivités territoriales, des établissements publics et des établissements de santé

Par ailleurs, à l'issue de leurs travaux, les rapporteurs estiment qu'il est temps de franchir un nouveau cap en matière de cybersécurité. Les trop nombreux exemples de cyberattaques ayant frappé des collectivités territoriales et des établissements de santé prouvent qu'il est désormais urgent de rehausser le niveau d'ambition en la matière. Concrètement, ils estiment qu'il faut instaurer l'obligation de diligenter, à intervalles réguliers, des « contrôles techniques » en cybersécurité, notamment en lien avec le ministère de l'Intérieur et le commandement du ministère de l'Intérieur dans le cyberespace (nouveau nom du COMCyberGEND) sous la responsabilité des préfets des zones de défense et des préfets de région. Les rapporteurs ont pu apprécier concrètement les compétences et les savoir-faire des

gendarmes en matière de cyberdéfense. Ils savent ce qu'ils peuvent apporter à ces entités et, ce faisant, contribuer à la cyber-résilience de la Nation.

c. Renforcer la féminisation des agents numériques et cyber de l'État

En outre, renforcer la cyber-résilience de la Nation impliquera de féminiser les recrutements des agents numériques et cyber de l'État afin d'élargir le vivier de compétences et de talents ouverts au recrutement. Cela vaut évidemment pour les services de l'État mais également dès l'école secondaire, en luttant efficacement contre les stéréotypes de genre et en incitant les jeunes filles à s'engager dans cette voie professionnelle.

d. L'éducation au risque cyber dès le plus jeune âge

Par ailleurs, au-delà de la qualité de l'organisation et de la gouvernance de la cyberdéfense, il apparaît plus que nécessaire d'éduquer au risque cyber dès le plus jeune âge. De ce point de vue, l'école a un rôle primordial à jouer. En formant les jeunes au risque cyber dès l'école, un très grand nombre de cyberattaques pourraient être évitées. Il n'est en effet plus à démontrer que la sensibilisation accompagnée de l'adoption de réflexes simples avant, pendant et après une attaque de nature cyber permet d'en limiter les impacts, voire d'éviter celle-ci. C'est pour cette raison que l'ANSSI continue de valoriser son action et attache une importance forte aux actions de communication comme de formation. L'Agence continue de publier des guides aux niveaux variés à destination d'un public toujours plus large.

Il convient de relever ici également l'importance de la chaîne numérique et notamment des éditeurs de logiciels dans ces attaques. La menace cyber s'appuie souvent sur des vulnérabilités non corrigées, pourtant le plus souvent connues et pour lesquelles des correctifs existent, mais qui ne sont pas mises à jour et sur lesquelles les utilisateurs ne sont pas toujours informés. Pour autant, il convient également de préciser que la croissance constante des cyber-attaques s'accompagne d'une professionnalisation des acteurs malveillants qui en sont à l'origine et nécessite une adaptation en continue des moyens défensifs, qui ne se résume pas à des gestes simples ou à la seule prudence des utilisateurs.

En ce qui la concerne, l'ANSSI s'est déjà engagée sur cette voie. Elle collabore en effet de manière étroite avec le ministère de l'Éducation nationale sur cet enjeu, en vue d'intégrer des éléments de sensibilisation adaptés notamment dans le programme du collège. Elle est également partenaire depuis plusieurs années du GIP PIX, qui propose une évaluation des compétences numériques des collégiens et des lycéens, mais aussi des personnes sans emploi. D'une part, l'ANSSI contribue au financement de cette mission par une subvention, mais elle a aussi participé à l'élaboration de contenus pédagogiques pour fournir aux différents publics un premier niveau de sensibilisation dans le domaine de la cybersécurité. Ces contenus peuvent aussi être utilisés dans le cadre de sensibilisations auprès des agents publics, quels qu'ils soient, sous l'impulsion de leurs responsables de la sécurité des systèmes d'information.

Lors de leur déplacement en Finlande et en Estonie, les rapporteurs ont pu mesurer le niveau de cyber-résilience inculqué dès le plus jeune âge dans la société. Au-delà des initiatives salutaires à destination des plus jeunes dans le secondaire, c'est bien dès le primaire qu'il faut sensibiliser les enfants à l'hygiène numérique et, plus largement, à la cybersécurité, pour que celle-ci devienne un réflexe.

e. Renforcer la préparation aux crises cyber par la réalisation d'exercices en conditions réelles aux échelles nationale et internationale

Par ailleurs, afin d'améliorer le niveau de cyber-résilience de la Nation, la participation à des exercices est indispensable. Dans le cadre de leurs travaux, les rapporteurs ont été alertés sur la faible participation des armées et des services de l'État aux exercices cyber organisés à l'échelle internationale. Ils n'ont par ailleurs pas eu connaissance d'exercices cyber organisés par la France et en France à destination de nos partenaires.

Or, cela leur semble pourtant indispensable. D'ailleurs, s'agissant de la nature de ces exercices, ils ont acquis la conviction qu'il était nécessaire d'organiser des exercices en conditions réelles, à la fois à l'échelle nationale, interministérielle, mais également avec des États alliés dans le cadre de coopérations bilatérales ou multilatérales. Cela permettait de renforcer utilement le lien armées-Nation et les populations seraient d'autant plus sensibilisées face au risque cyber si les conséquences d'une cyberattaque – par exemple l'arrêt d'une centrale électrique pendant quelques heures – sont ressenties *in concreto* par les populations dans le cadre de ces exercices.

f. Pour une approche globale de la cybersécurité

Surtout, la distinction, relativement artificielle, entre le secteur civil et le secteur de la défense doit être levée. La guerre en Ukraine en est la parfaite illustration. La guerre en Ukraine illustre en effet l'usage de cyberattaques, en amont puis en soutien d'un conflit de haute intensité. En 2022, la cyberattaque la plus marquante a été celle ayant fait tomber le réseau de télécommunication de l'opérateur satellitaire VIASAT, réalisée une heure avant l'invasion de l'Ukraine. Précédemment, l'Ukraine avait vu son réseau électrique saboté à deux reprises (2015 et 2016) et une majorité de ses administrations et entreprises immobilisées en 2017 suite à la propagation d'un logiciel malveillant.

Cette crise démontre aussi, sur une note plus positive, l'efficacité d'approches défensives bien conçues et mises en œuvre, pour limiter les effets de telles cyberattaques. À ce titre, la progression des capacités défensives ukrainiennes depuis 2014 paraît évidente, et est une source d'inspiration pour les travaux conduits en France. Depuis, en France, les infrastructures les plus critiques, notamment les centrales nucléaires et établissements hospitaliers, bénéficient d'un suivi renforcé.

En cas de conflit de haute intensité, pourra-t-on se permettre de distinguer des domaines de responsabilité ? Imaginerait-on le COMCYBER refuser d'intervenir pour remédier à une cyberattaque de grande ampleur touchant une

centrale électrique sous le prétexte que cela relèverait, en droit, de la responsabilité de l'ANSSI ? Si l'hypothèse d'un conflit de haute intensité peut encore paraître lointaine à nos concitoyens, ne faut-il pas se préparer à sa survenance, y compris dans le domaine de la coopération entre les armées et le secteur civil ?

II. LE DÉFI DES RESSOURCES HUMAINES : RECRUTER, FORMER ET FIDÉLISER

1. Un objectif de 953 équivalents temps plein à l'horizon 2030 pour la cyberdéfense

La répartition des effectifs dédiés à la cyberdéfense dans la LPM 2024-2030 par « grand employeur » et « employeur non rattaché » (en ETP) est la suivante :

Ensemble des armées	351
Délégation générale pour l'armement (DGA)	192
Direction générale de la sécurité Extérieure (DGSE)	386
Direction du renseignement et de la sécurité de la Défense (DRSD)	20
Gendarmerie de la sécurité des armements nucléaires (GSAN)	2
Direction de la protection des installations, moyens et activités de la défense (DPID)	2
TOTAL	**953**

La répartition de ces effectifs à une maille plus fine, sur l'ensemble des états-majors, directions et services du ministère, était en cours d'élaboration en juillet 2023. Une fois cette répartition effectuée, les effectifs affectés respectivement aux trois domaines de lutte informatique pourront être définis.

Entre 2024 et 2030, le ministère des Armées développera sa capacité à générer la ressource nécessaire pour armer ces besoins nouveaux par le recrutement de nouveaux agents (militaires comme civils), la fidélisation du personnel qualifié et la réorientation. C'est le rôle de la GPEEC qui se fondera notamment sur une description aussi précise que possible des besoins à la fois par employeur et par domaine de lutte informatique.

Le ministère des Armées a donc programmé une montée en puissance des effectifs dédiés à la cyberdéfense. Ce développement de la cyberdéfense se heurte toutefois à la question des besoins en recrutement dans un secteur en tension. À l'échelle mondiale, la pénurie de cadres dans ce domaine est estimée à 1,8 million en 2023.

2. La difficile féminisation des agents cyber

Dans cet univers très compétitif, face à une pénurie majeure de compétences, le ministère des Armées souhaite attirer tous les talents de la société française et pratique donc une politique active de recrutement de femmes.

En France, alors que les femmes représentent environ 50 % d'une classe d'âge, elles montrent une désaffection marquée pour les filières scientifiques. Ainsi, les filières d'étude en informatique comptent moins de 14 % de femmes et 6 % en cyber. C'est pourquoi la France ne compte aujourd'hui que 27 % de femmes dans les métiers de l'informatique et 11 % dans le cyber.

Au ministère des Armées, le taux de féminisation actuel de 16,1 % reste insuffisant et s'explique en partie par ce biais sociétal et culturel. À titre de comparaison, les femmes représentent dans le monde 50 % des informaticiens et 25 % des salariés dans le domaine de la cybersécurité. Le ministère des Armées est convaincu de la nécessité de mieux attirer les femmes dans les métiers du cyber. La quête des potentiels se mène donc auprès de l'ensemble des femmes, très en amont au cours de la scolarité (collèges, lycées) afin de promouvoir les filières scientifiques et numériques, mais aussi au sein du ministère des Armées.

Pour ce faire, outre les actions de communication institutionnelle, le ministère s'appuie depuis 2018 sur le réseau Combattantes@Numérique. Il organise des rencontres tout au long de l'année et un grand événement annuel pour créer l'impulsion, promouvoir des rôles modèles, favoriser les échanges et donner envie aux jeunes femmes de rejoindre les métiers du numérique et éventuellement la cyberdéfense.

D'autres axes sont en cours d'étude dans le cadre du Plan Égalité professionnelle entre les femmes et les hommes du ministère :

1/ la lutte contre les stéréotypes et préjugés culturels, qui véhiculent une image masculine de la cyberdéfense (image du « geek » ou du « hacker ») ;

2/ la mise en valeur de modèles féminins, pour inciter les jeunes filles et jeunes femmes à poursuivre des carrières dans ce domaine ;

3/ la dénonciation des préjugés inconscients, même dans les organismes qui recherchent activement des femmes mais peuvent les désavantager involontairement en termes de promotion, de rémunération et d'accès aux fonctions d'encadrement ;

4/ et l'évolution d'une culture de travail parfois intimidante pour les femmes.

3. La mise en place d'un comité de suivi dédié : le CSR cyber

La DRH-MD co-préside le comité de suivi de la ressource cyber (CSR) cyber aux côtés du COMCYBER. À ce titre, elle est l'interlocutrice directe des gestionnaires dans le cadre du suivi de la ressource de cyber-opérateurs, la mise en œuvre d'actions et de leviers de ressources humaines permettant de recruter et de fidéliser la ressource. La DRH-MD, en lien avec le COMCYBER, est garante de l'actualisation annuelle du périmètre définissant les cyber-opérateurs.

Le suivi des flux de départs fait désormais l'objet d'une attention particulière avec la mise en place d'un questionnaire rempli par tout agent quittant le ministère des Armées, comprenant une partie commune et une partie spécifique à chaque gestionnaire. Il vise à bien comprendre les raisons de départ et envisager les réponses à développer au niveau ministériel ou local (gestionnaire, employeur).

La filière cyber fait en outre l'objet d'un suivi particulier dans le domaine de l'attribution de la prime de lien au service et de l'apprentissage afin de mesurer l'impact de ces deux dispositifs sur cette ressource. En termes de recrutement et de formation, le CSR cyber a permis le déploiement de mesures nouvelles :

1/ des campagnes de recrutement dans les écoles, avec plusieurs actions qui ont été mises en œuvre par le bureau d'appui au recrutement cyber (BARC) du COMCYBER. Ce BARC appuie l'action des CIRFA et mène des actions de communication externe telles que la JDC, l'organisation de campus cyber, des tests de niveaux ou encore la participation à des événements (DEFNET, Vivatech, *etc*.) ;

2/ la création d'un BTS cyber au sein du lycée militaire de Saint-Cyr-l'École. Celui-ci devait doubler ses capacités à la rentrée 2023 pour passer d'une promotion d'environ 35 élèves à 70 (deux classes de 35 élèves en vue de recruter, au terme de la scolarité, 50 % de personnels militaires et 50 % de personnels civils) ;

3/ la création d'un BTS CIEL à Brest sous tutelle du ministère de l'Éducation nationale, en partenariat avec la Marine nationale. Ce partenariat a été conclu pour accueillir 48 jeunes souhaitant s'engager.

4. Un ministère avec des atouts et des difficultés pour recruter et fidéliser ses agents cyber

Comme indiqué plus haut, la ressource cyber est donc rare et sa croissance est moins rapide que celle du schéma d'emplois, en forte augmentation depuis 2021. Les armées ont toutefois des atouts indéniables en matière d'attractivité :

1/ le sens de la mission ;

2/ l'attrait technique (défense de systèmes d'armes et systèmes complexes) ;

3/ la diversité des missions dont certaines ne sont réalisées qu'au sein des armées (LIO et L2I) ;

4/ les opportunités de formation et d'ascension sociale ;

5/ et l'attrait de l'expérience professionnelle au sein du ministère qui est valorisable pour une seconde carrière.

Elles sont néanmoins pénalisées par des faiblesses de différentes natures dont certaines pourraient être réduites :

1/ un manque de lisibilité des carrières ;

2/ la difficulté pour un jeune passionné par ce domaine à se projeter au sein des armées ;

3/ le temps requis pour concrétiser un recrutement, en particulier les enquêtes d'habilitation, qui est souvent incompatible avec la réalité du marché de l'emploi ;

4/ le niveau des rémunérations au recrutement pour les jeunes diplômés intéressés par une carrière militaire, la compétitivité étant meilleure pour le personnel civil recruté sous contrat grâce à la grille interministérielle mise en place par la DINUM (*cf. infra*) ;

5/ le niveau de rémunération global, notamment pour le personnel expérimenté, le ministère ne pouvant que difficilement s'aligner sur les salaires proposés par les entreprises du secteur privé.

Les départs ne sont pas plus importants dans le domaine cyber que dans l'ensemble du ministère (sauf à la DGA). Les principales raisons des départs sont la rémunération, le management, la localisation des postes, ainsi que le manque de perspectives de carrière. La problématique de la rémunération se fait prégnante à partir de 10-15 ans de service lorsque les perspectives salariales du privé sont largement supérieures à celles proposées par le ministère.

Il y a une forte concurrence entre les secteurs civil et public, mais également ponctuellement entre les différents services. À cet égard, une mesure de coordination interservices, encore en développement en juillet 2023, devrait permettre de sortir de cette logique de « concurrence » pour permettre une meilleure coopération.

Dans le détail, les motifs des départs identifiés sont les suivants :

1/ la rémunération ;

2/ l'incompatibilité de certaines activités avec le télétravail ;

3/ le manque d'équipements performants, source de démotivation pour les plus jeunes ;

4/ la mobilité inhérente au statut militaire ;

5/ la qualité de vie au travail (et notamment la verticalité de l'organisation) ;

6/ et le manque de reconnaissance.

Les mesures prises en vue de l'amélioration de la fidélisation notamment en termes de formation donnent satisfaction, comme le BTS cyber créé au sein du lycée militaire de la défense de Saint-Cyr-l'Ecole. En l'espace de quatre promotions, 106 cyber-opérateurs ont rejoint les employeurs du ministère des Armées. Une extension du partenariat est à l'étude, ce BTS rencontrant un grand succès avec plus de 800 candidatures reçues cette année sur Parcoursup pour 70 places offertes. Concernant l'apprentissage, 183 apprentis servent dans le domaine cyber au 31 mars 2023.

Le montant de la prime de lien au service, mise en place au profit de la famille professionnelle SIC, a été augmenté. Elle est de 50 000 € depuis le 1er janvier 2023 pour les cyber-opérateurs. Dans le cadre de la NPRM, une prime de compétences spécifique « supériorité numérique » était à l'étude en juillet 2023, recouvrant le périmètre de la cyberdéfense.

5. La vitalité de la région Bretagne dans le domaine de la cyberdéfense

La Bretagne est une région de plein emploi sur les profils qualifiés, qui ne connaît pas de difficultés de recrutement de personnels civils spécifiques. En moyenne, six candidats se présentent pour un poste, mais cela peut être est en dessous de la réalité car certains profils sont sourcés assez directement au regard des compétences visées. Sur certains postes, 35 candidats peuvent être amenés à se présenter. Ce dynamisme du marché de l'emploi rend plus délicat la fidélisation et place le ministère dans une gestion de flux à maîtriser. Les unités militaires cyber se positionnent sur des recrutements plutôt jeunes sur lesquels la différence salariale n'est pas encore marquée par l'expérience. Le sens de la mission et l'effort consenti en formations en interne sont des leviers intéressants auxquels s'ajoutent les jours réglementaires de récupération après astreinte, apportant au confort de vie. L'alternance est une source intéressante pour sélectionner et préparer à l'emploi futur. Plus de 200 candidatures ont été reçues cette année pour moins de 20 postes à pourvoir. Toutefois, l'équilibre est fragile, les unités ne pouvant pas s'offrir des profils séniors et le temps passé en formation est autant de temps obéré d'agent et de report de charge sur ceux déjà en poste.

Dans le domaine de la formation, des actions concrètes sont conduites avec l'inspection d'académie de Rennes par le Pôle d'excellence cyber pour orienter la formation en BTS. Et avec le soutien du conseil régional, 10 acteurs majeurs de la formation et de la cybersécurité se sont réunis autour du Pôle d'excellence cyber, pour développer en Bretagne un parcours régional de sensibilisation et de formation, du Bac-3 au Bac+8. Action qui débutera avec l'officialisation des lauréats de l'appel à manifestation d'intérêt « Compétences et métiers d'avenir ».

À titre d'illustration, le BTS CIEL est proposé à Brest sous tutelle du ministère de l'Éducation nationale. Un partenariat avec la Marine nationale (entre

le lycée naval et le lycée Vauban) a été conclu. Actuellement, la Marine recrute une dizaine de candidats, l'objectif étant de recruter 48 candidats annuellement à partir de 2027. Les candidats sont placés sous statut « élèves des lycées de la défense ». À l'issue de la formation, une intégration *via* l'école de Maistrance est possible en vue d'occuper des postes cyber en qualité de sous-officiers.

6. Une situation particulièrement alarmante à la DGA

Les démissions ont augmenté dans l'ensemble des métiers de la DGA et particulièrement en 2022 pour la cyberdéfense. La tendance forte observée en 2022 continue sur un rythme encore plus soutenu en 2023.

Dans le domaine cyber, et c'est également le cas d'ailleurs dans un certain nombre de métiers sous tension, la DGA fait en effet face à une concurrence accrue des industriels sur le marché de l'emploi. La particularité du cyber est que la sphère industrielle va largement au-delà de la BITD (tous les secteurs sont concernés par des enjeux de cyber sécurité), et que la concurrence s'exerce également entre les organismes étatiques du domaine. La grille de la DINUM est une avancée pour renforcer l'attractivité de ces emplois contractuels civils mais elle ne s'applique aujourd'hui qu'à l'embauche. Des mesures de revalorisation ont été engagées cette année pour les métiers en tension, dont le cyber, mais ces efforts doivent être poursuivis. 70 % des démissions enregistrées dans le domaine cyber à la DGA le sont aujourd'hui pour des questions uniquement salariales.

Parallèlement, la DGA construit avec les agents des parcours professionnels variés pour les faire monter en compétences selon nos besoins et leurs appétences, ce qui présente le double avantage de diffuser la culture cyber dans l'ensemble des métiers de la DGA et d'être un outil de fidélisation efficace car motivant.

Toutefois, le ministère des Armées assiste depuis deux ans à la démission de personnels qualifiés et expérimentés (auparavant les démissions se situaient principalement au cours de la période allant de quatre à six ans après embauche) qui fait porter un risque majeur sur le maintien d'un « squelette » de compétences, à même de maintenir au meilleur niveau la technicité cyber de la DGA. La DGA assiste également à une augmentation des démissions d'ingénieurs ayant deux ans, ou moins, d'expérience, ce qui ne permet pas de « rentabiliser » l'important effort consenti par le ministère en matière de formation. Dans le domaine cyber, des formations importantes sont en effet dispensées à l'embauche pour permettre aux jeunes embauchés d'atteindre une efficacité opérationnelle en deux ans environ.

L'analyse de la population des agents exerçant à la DGA des fonctions relevant du domaine cyber montre la prépondérance des ingénieurs civils contractuels (75 %) par rapport aux autres statuts (12 % d'officiers des corps de l'armement, 8 % d'ingénieurs fonctionnaires). Cela s'explique par le fait que cette ressource est immédiatement disponible contrairement aux ingénieurs fonctionnaires qui sont recrutés uniquement par concours. Il est à noter que depuis plusieurs années les concours d'ingénieurs fonctionnaires rencontrent un succès

mitigé, avec plus ou moins 50 % de postes pourvus. Ceci peut s'expliquer par le fait que, sur les métiers cyber, la sécurité de l'emploi est liée à la compétence et non à un statut. Les personnels compétents n'ont aujourd'hui aucune difficulté à trouver un emploi, tant le marché est structurellement déficitaire. De surcroît, l'organisation des concours implique une affectation des lauréats pratiquement un an après l'expression des besoins des employeurs, ce qui manque de réactivité sur les sujets évoluant rapidement comme c'est le cas dans le domaine cyber. La DGA recherche d'ailleurs des agents disposant de compétences données, indépendamment de leur statut. Ainsi le très fort pourcentage de contractuels au sein de la population cyber n'est pas une marque de défiance vis-à-vis des titulaires, mais correspond à un besoin de compétences qui n'existe, chez ces derniers, qu'en nombre très limité.

7. La piste prometteuse des parcours croisés entre les services de l'État pour fidéliser les agents cyber

Les parcours croisés existent au sein du ministère. Ceux-ci sont un levier pour réduire les départs hors ministère/État, car ils permettent de renouveler et donner une nouvelle dynamique à la carrière d'un agent.

Une concurrence existe entre les différents organismes de l'État. Si on se fonde sur les déclarations des ingénieurs de la DGA ayant démissionné, celle-ci est exacerbée par des différences de rémunération :

Salaires nets mensuels*	ANSSI	DGSE	DGSI	DGA
Sortie d'école	2 400 €	2 400 €	2 400 €	2 350 €
Expérience > 7 ans	3 300 €	2 900 €	4 300 €	2 850 €
Expérience > 11 ans	4 000 €	3 500 €	5 300 €	3 300 €

**Données 2021 fondées sur du déclaratif correspondant aux propositions salariales acceptées par les ingénieurs de la DGA ayant démissionné pour rejoindre une société privée – source : DGA.*

L'application de la nouvelle grille interministérielle de la DINUM devrait contribuer à réduire ces écarts.

En novembre 2021, le COMCYBER a proposé d'établir un pacte à la signature avec des entreprises nationales spécialisées dans le domaine cyber. Ce projet devait être transmis aux employeurs et aux gestionnaires pour avis courant 2023, notamment sur l'intérêt des armées pour la mise en place d'échanges avec les entreprises françaises du secteur de la cybersécurité (EDF, Orange, *etc.*).

Par ailleurs, pour la famille professionnelle Renseignement, sous l'égide de la CNRLT, un « pacte de non-agression » entre les différents services de renseignement de l'État a été signé. Il devrait, en toute logique, impliquer de la ressource du domaine Cyber.

8. L'absence d'obligation déontologique spécifique pour les départs vers le secteur privé dans le domaine de la cyberdéfense

Pour sécuriser la reconversion des militaires, la commission de déontologie des militaires a été créée en 1996. Nommé par le Ministre et relevant directement de lui, le rapporteur général de la commission de déontologie des militaires veille à la continuité de l'activité de la commission et à la cohérence de ses travaux.

En saisissant la commission de déontologie, le militaire qui souhaite travailler dans le secteur privé après cessation définitive ou temporaire de ses fonctions s'assure de la compatibilité de sa nouvelle activité professionnelle avec ses fonctions antérieures afin d'éviter le risque pénal de prise illégale d'intérêts.

Cependant, il n'existe, à ce jour, aucune obligation déontologique applicable spécifiquement aux spécialistes cyber qui projettent une embauche dans le secteur privé. Le ministère travaille sur un encadrement renforcé des militaires rejoignant une entreprise privée partenaire des armées. L'article 42 de la LPM évoque ainsi des domaines où ce renforcement pourrait trouver à s'appliquer et le domaine de la cyberdéfense en faire partie.

Dans le contexte de résurgence des tensions et compétitions internationales, certains États étrangers n'hésitent pas à rechercher activement, directement ou par l'intermédiaire d'entreprises agissant pour leur compte, la collaboration d'anciens militaires dont l'expertise technique ou le savoir-faire opérationnel présentent un intérêt stratégique pour le développement de leurs propres capacités militaires.

Dans le cadre de la LPM, un dispositif a été proposé qui permettra d'empêcher le départ d'anciens militaires détenant des informations sensibles vers des structures étrangères susceptibles de chercher à obtenir des informations stratégiques. L'article 42 de la LPM garantit en effet la prise en compte des intérêts fondamentaux de la Nation en cas d'activité privée en rapport avec une puissance étrangère.

Le mécanisme prévu à cet article se justifie par la nécessité de protéger les capacités et les modes d'action des armées, surtout dans le domaine de la LIO. En outre, les personnes qui souhaitent rejoindre les armées dans le domaine cyber n'ayant pas nécessairement en tête un plan de carrière prédéfini, l'idée selon laquelle ce mécanisme pourrait porter atteinte à la fidélisation des personnels doit être nuancée. Par ailleurs, les savoir-faire dans le domaine cyber deviennent obsolètes au bout de 2 ou 3 ans, ce qui diminue *ipso facto* le risque de transmission d'informations sensibles à des entreprises étrangères et, partant, le risque que des anciens militaires voulant rejoindre une entreprise étrangère soient empêchés de le faire.

Un décret en Conseil d'État déterminera les domaines d'emploi concernés (tels que les domaines du pilotage d'aéronefs, du nucléaire ou de la cyberdéfense). La liste précise de ces fonctions sera fixée par un arrêté non publié du ministre des Armées. Cela étant, le travail de déclinaison élargi aux civils doit être approfondi

car dans un contexte de forte concurrence sur le marché de l'emploi, toute contrainte supplémentaire fait peser un risque sur l'attractivité du ministère.

9. Le dilemme du recours aux personnels civils dans le domaine de la cyberdéfense

Faire carrière dans la fonction publique n'est plus aussi attractif qu'auparavant et les jeunes générations affichent une préférence pour le modèle contractuel qui autorise des parcours plus variés. Cette tendance à la contractualisation est particulièrement perceptible dans les métiers en tension et notamment le numérique. La loi de transformation de la fonction publique de 2019 ouvre largement la possibilité de recourir à des contractuels. Recruter davantage de contractuels doit permettre, d'une part, au ministère des Armées de recruter des compétences particulières dont le ministère a besoin notamment pour certains métiers nécessitant des compétences particulières ou pour certaines filières en tension. D'autre part, il doit permettre d'aller capter des jeunes talents, disposant de compétences répondant aux besoins du ministère des Armées mais qui ne souhaitent pas s'engager durablement au profit du ministère, sous statut militaire ou en tant que fonctionnaire.

Le recrutement d'agents contractuels est fortement favorisé par la grille de rémunération de la DINUM, plus avantageuse que les autres grilles salariales. Localement, cela peut créer des difficultés avec des titulaires managers moins bien rémunérés qu'une partie des agents de leurs équipes.

Peu de fonctionnaires possèdent *ab initio* les compétences cyber recherchées par le ministère des Armées. Néanmoins, leur expérience professionnelle acquise peut utilement être capitalisée en réorientant les fonctionnaires intéressés vers le domaine cyber au moyen du *reskilling*.

Une attention particulière doit également être portée à préserver un certain équilibre entre les personnels militaires et les personnels civils, afin qu'une trop forte civilianisation ne reporte pas la charge opérationnelle sur les personnels militaires devenus minoritaires (et qui, seuls, sont projetables). Certains postes opérationnels doivent impérativement être tenus par des militaires, notamment ceux en rapport avec la LIO ou ceux pouvant nécessiter d'être déployés en opérations. Ainsi, il est préférable d'apprécier les besoins opérationnels et les cadres d'emploi des différents employeurs afin d'évaluer la nécessité de disposer de personnel militaire ou civil.

Enfin, le recrutement d'une part croissante de contractuels impose un changement de paradigme dans la gestion des parcours professionnels, car une fois le recrutement effectué, il est important de fidéliser les compétences et l'expérience acquise au sein du ministère en étant en capacité de proposer des parcours professionnels attractifs.

10. Les réservistes

S'agissant des réservistes, le COMCYBER n'a pas de difficultés pour attirer les candidats. Mais le recrutement est freiné car la modernisation du processus de recrutement est actuellement en cours. L'intérêt de la réserve cyber réside pour les entreprises dans le fait de bénéficier de la montée en compétences de leurs salariés. Cependant, le ministère des Armées ne dispose pas de l'assurance que ces réservistes seront disponibles en cas de crise (emplois dans les OIV ou au sein de la BITD).

Sur les 305 réservistes de cyberdéfense, il y a 27 % d'aviateurs, 59 % de terriens, et 14 % de marins. Ils sont employés pour 55 % au COMCYBER et GCA, 13 % par l'armée de l'Air et de l'Espace, 22 % par l'armée de Terre et 4 % par la Marine. C'est une population de spécialistes et d'ingénieurs de haut niveau (féminisée à 14 %) qui renforce les unités opérationnelles cyber avec des compétences en réseau et protocoles, cryptographie, rétro-conception et analyse de vulnérabilités, audit, sécurité, communication, linguistiques, influence, entre autres. Les réservistes cyber apportent une expertise et un éclairage singulier, ainsi que des compétences rares ou détenues par peu de personnes dans les armées.

Dans le plan réserve 2035, la trajectoire est fixée à 500 réservistes de cyberdéfense. Elle sera consolidée en fonction des besoins et si elle est soutenue par la création de postes permanents dédiés à l'animation ou à la formation.

III. LE DÉFI JURIDIQUE : SÉCURISER LES ACTIONS DE NOS ARMÉES PAR LE DROIT

1. Le droit international s'applique dans opérations militaires dans le cyberespace

Le droit international s'appliquant aux cyberopérations, le ministère des Armées considère que les normes existantes sont suffisantes pour encadrer les activités dans le cyber espace en temps de paix et en contexte de conflit armé.

En temps de paix, les opérations dans le cyberespace sont régies par les règles générales du droit international public, notamment la Charte des Nations unies. Tout emploi de ces moyens doit donc respecter la souveraineté des États, l'égalité souveraine entre ces entités, l'obligation de régler les différends de manière pacifique ou encore la non-intervention dans les affaires intérieures des États.

En temps de conflit armé, les opérations militaires conduites dans le cyberespace par les forces armées comprenant les opérations de LID, de LIO ou de L2I sont soumises au droit international humanitaire, également appelé le droit des conflits armés. Sont ainsi applicables les principes régissant la conduite des hostilités, et toutes les opérations françaises sont encadrées par des règles précises

ainsi que des cadres d'emplois parfaitement conformes à ces principes, à l'instar des opérations conduites dans les espaces traditionnels de conflictualité.

2. Qu'est-ce qu'une arme dans le cyberespace ?

Le terme « cyberarme » renvoie à l'ensemble des moyens numériques utilisés en contexte de conflit armé et en lien avec celui-ci (armes, méthodes et moyens de guerre), mais aussi aux moyens numériques qui ne produisent pas de dommages (ceux utilisés à des fins de renseignement).

Les cyberarmes sont des armes de « combinaison » et de soutien des moyens conventionnels, même si elles peuvent être utilisées de manière autonome. Les cyberarmes peuvent être techniquement développées en fonction d'une cible et d'effets spécifiques recherchés, et devront être déployées en conformité avec les principes régissant la conduite des hostilités, de la même manière que pour les armes physiques.

Si le droit applicable aux armes, moyens et méthodes de guerre « physiques » s'applique également aux cyberarmes, il est vrai que les moyens de LIO présentent des spécificités (immédiateté de l'action, dualité des cibles, hyper-connexion et interdépendance des réseaux) qui nécessitent la mise en œuvre d'un processus de ciblage numérique spécifique. Ce processus est directement placé sous la responsabilité du chef d'état-major des armées qui bénéficie du soutien d'experts opérationnels et de conseillers juridiques opérationnels spécialisés.

3. Cyberattaques et agression armées dans le cyberespace

Une agression armée est un usage de la force d'une gravité significative, indépendamment du moyen utilisé. Il est donc possible qu'une cyberattaque constitue une agression armée dès lors que ses effets et son ampleur atteignent une gravité comparable à ceux d'un emploi de la force physique. C'est par exemple le cas d'une cyberattaque qui causerait des pertes humaines, des dommages physiques ou économiques considérables avec de graves conséquences pour l'intégrité territoriale, politique ou la souveraineté de l'État.

De même, des cyberattaques qui, isolément, n'atteignent pas le seuil de l'agression armée, pourraient être qualifiées comme telles si l'accumulation de leurs effets atteignait un seuil de gravité suffisant, ou si elles étaient menées de manière conjointe à des opérations menées dans le champ physique constitutives d'une agression armée. Ces cyberattaques doivent néanmoins être coordonnées et émaner de la même entité ou de différentes entités agissant de concert.

Enfin, pour être qualifiée d'agression armée, une cyberattaque doit avoir été perpétrée directement ou indirectement par un État. Un État est responsable des actes commis par des acteurs non étatiques sur son territoire si ces derniers ont agi sur ses instructions, ses directives ou sous son contrôle.

4. Les grands principes du droit international s'appliquent dans le domaine de la cyberdéfense

a. La caractérisation d'un conflit

Des opérations dans le cyberespace qui seraient constitutives d'hostilités entre deux ou plusieurs États peuvent caractériser l'existence d'un conflit armé international. De même, les opérations prolongées dans le cyberespace opposant des forces armées gouvernementales aux forces d'un ou de plusieurs groupes armés ou opposant plusieurs groupes armés entre eux, peuvent constituer un conflit armé non international dès lors que ces groupes font preuve d'un minimum d'organisation et que les effets de ces opérations atteignent un degré de violence suffisant.

Lorsque ces opérations militaires sont combinées avec des opérations militaires conventionnelles, il n'est pas difficile de qualifier la situation de conflit armé. En revanche, s'il est possible théoriquement que des opérations cyber caractérisent à elles seules un conflit armé, il faudrait que celles-ci atteignent un seuil de violence spécifique.

b. La participation d'un État à un conflit armé

Les règles applicables dans le domaine physique s'appliquent pleinement au domaine cyber. Ainsi, un État devient partie à un conflit dès qu'il a « *recours à la force armée* » (TPIY, Tadic, 1995) contre les forces armées, le territoire ou la population d'un autre État. Il s'agit d'une évaluation *in concreto* reposant d'une part sur le seuil d'intensité du recours à la force armée. Si ce seuil n'est pas déterminé, il implique une certaine intensité de la violence. Ainsi, des cyber-opérations menées par les forces françaises à l'encontre d'un autre État et qui produiraient des dommages physiques, ou rendraient des systèmes inopérants, pourraient être qualifiées de recours à la force armée.

Il est aussi possible de considérer qu'un État devient partie à un conflit si son implication correspond à un contrôle effectif (Cour internationale de Justice) ou global (Cour pénale internationale et Tribunal pénal international pour l'ex-Yougoslavie) des forces armées d'un autre État. Le contrôle global peut par exemple être caractérisé si un État est impliqué dans l'organisation, la coordination ou la planification des actions militaires de forces armées d'un autre État, en plus de financer celui-ci, de l'entraîner, de l'équiper ou de lui apporter son soutien opérationnel. Le contrôle global va au-delà de la simple aide financière, de la fourniture d'équipements militaires ou même de la formation.

c. Le respect de la souveraineté des États

L'applicabilité du principe de souveraineté a été reconnue par le Groupe d'experts gouvernementaux cyber de l'ONU dans ses deux rapports de 2013 et de 2015. Il est notamment admis que les États exercent leur souveraineté sur les infrastructures situées sur leur territoire. Le droit international interdit les atteintes à certains principes qui dérivent du principe de souveraineté (intégrité territoriale,

non-intervention dans les affaires intérieures, non-recours à la force), et ces interdictions s'étendent au cyberespace. Ainsi, toute cyberattaque menée à l'encontre de systèmes d'information ou toute production d'effets hostiles par le biais de moyens cybernétiques par un organe étatique, une personne ou entité exerçant des prérogatives de puissance publique, ou agissant sur les instructions, directives ou contrôle d'un État tiers sont susceptibles de constituer une violation de souveraineté.

d. Le principe de non-intervention dans les affaires intérieures

L'ingérence par le biais d'un moyen cyber dans le domaine réservé d'un État, ou bien les atteintes au système politique, économique et social d'un État par une cyber-opération peuvent constituer une violation du principe de non-intervention dans les affaires intérieures. De telles violations peuvent être, par exemple, des cyber-opérations qui viendraient perturber la capacité d'un État à mener ses processus électoraux ou en altéreraient les résultats. En ce sens, la ministre des armées Florence Parly a rappelé en octobre 2021, au sujet de la L2I, que les armées n'avaient pas vocation à s'immiscer dans les affaires électorales d'un autre État.

En tout état de cause, les cyber-opérations qui violeraient les principes d'intégrité territoriale, de non-intervention, de souveraineté ou encore d'interdiction du recours à la force pourraient conduire à l'engagement de la responsabilité internationale pour fait internationalement illicite de l'État auquel elles seraient imputées.

e. L'application du principe de distinction

Le principe de distinction impose aux parties à un conflit armé de faire, en tout temps, la distinction entre civils et combattants, biens civils et objectifs militaires. Ainsi, dans un contexte de conflit armé, si les cyberattaques ne sont pas dirigées contre un objectif militaire déterminé ou si leurs effets ne peuvent être limités, elles sont interdites. En cas de doute sur la nature d'un individu, celui-ci doit être considéré comme civil. Pour les biens, de manière similaire, s'il existe un doute sur la qualification, un bien normalement affecté à un usage civil sera présumé ne pas être utilisé en vue d'apporter une contribution physique à l'action militaire.

Dans cette perspective, les opérations de LIO et L2I sont planifiées et coordonnées en prenant toutes les mesures possibles pour vérifier que les objectifs ciblés ne sont pas des personnes civiles ou des biens à caractère civil. Le commandement doit ainsi réunir les renseignements nécessaires pour identifier l'objectif, puis choisir le moyen le plus adapté pour mettre en œuvre le principe de distinction. L'intégration de cyberarmes dans la manœuvre opérationnelle repose sur une planification longue et spécifique qui permet de recueillir toutes les informations nécessaires à l'identification de la nature du système visé afin de garantir le respect de ce principe de distinction. Si la cible examinée se révèle ne pas être un objectif militaire, alors l'attaque est annulée.

f. La qualification d'objectifs militaires cyber

Les équipements ou systèmes informatiques, les données, les processus ou flux d'échanges qui les composent peuvent constituer un objectif militaire. Cependant, cette qualification nécessite que ces outils contribuent à l'action militaire par leur nature (par exemple : postes informatiques des forces armées, réseaux de communication militaire), par leur emplacement (lieux depuis lesquels sont menées des cyberattaques), leur destination (utilisation de réseaux informatiques à des fins militaires), et que leur destruction, totale ou partielle, leur capture ou neutralisation confèrent un avantage militaire précis.

g. La qualification de biens civils

A contrario, tous les biens qui ne sont pas des objectifs militaires sont considérés comme civils. On ne peut donc pas mener une opération cyber contre des systèmes informatiques utilisés par des services exclusivement civils (école, établissements médicaux), sauf si ces derniers sont utilisés à des fins militaires. Les opérations cyber doivent également respecter des régimes de protection spécifiquement prévus par le DIH comme ceux relatifs aux biens culturels, à l'environnement naturel, aux biens de secours humanitaires, entre autres.

h. L'application du principe de distinction à des infrastructures servant à la fois des fins civiles et militaires

Une infrastructure dite « duale » peut être considérée, après analyse minutieuse et au cas par cas, comme un objectif militaire (pour peu que les conditions évoquées plus haut soient respectées : contribution à l'action militaire et avantage conféré par leur destruction/capture/neutralisation). Ces infrastructures qualifiées comme objectifs militaires peuvent être ciblées à condition que soient respectés également les principes de proportionnalité et de précaution. Ainsi, compte tenu des caractéristiques intrinsèques au cyberespace le commandement militaire doit se montrer particulièrement vigilant afin de minimiser les effets incidents sur les civils et les biens à caractère civil. En effet, en application du principe de proportionnalité, ces effets ne doivent pas être disproportionnés par rapport à l'avantage militaire direct et concret attendu de l'attaque.

i. L'article 5 de l'OTAN

L'article 5 du Traité de Washington consacre le principe de la défense collective. La défense collective implique qu'une attaque contre un membre de l'Alliance est considérée comme une attaque dirigée contre tous les Alliés. Pour que l'article 5 soit applicable, une attaque armée doit avoir eu lieu sur le territoire d'un membre de l'OTAN. Selon l'article 6, l'attaque armée doit donc avoir lieu contre l'un des membres se trouvant en Europe ou en Amérique du Nord, contre le territoire de la Turquie ou contre les îles placées sous la juridiction de l'une des parties dans la région de l'Atlantique Nord au nord du Tropique du Cancer. En ce sens, lors du Sommet de Madrid en 2022, les dirigeants de l'OTAN ont confirmé que l'article 5 s'appliquait au domaine cyber et qu'un acte isolé de cyber-

malveillance pourrait atteindre le seuil correspondant à une attaque armée qui conduirait le Conseil de l'OTAN à invoquer l'article 5.

Toutefois, il faut noter qu'invoquer l'article 5 est une décision politique de solidarité en réponse à une atteinte à l'intégrité d'un État membre de l'Alliance. Ce n'est pas un processus automatique. En effet, ce n'est que par consensus et après une évaluation des circonstances, des renseignements à disposition et de la caractérisation de l'attaque que le recours à une réponse collective pourra être décidé par le Conseil.

j. L'article 42.7 TUE

La clause de défense mutuelle peut être utilisée dans les cas où un État membre serait l'objet d'une agression armée sur son territoire. Elle impose aux autres États membres de lui apporter aide et assistance par tous les moyens en leur pouvoir. Néanmoins, elle est relativement souple dans sa mise en œuvre car l'article 42.7 n'apporte aucune indication quant à la forme, aux critères, aux conditions ou aux modalités pratiques de la solidarité qui doit se manifester entre les États membres dans l'hypothèse d'une « agression armée » sur le territoire de l'un d'eux. La clause de défense mutuelle laisse aux États membres le soin de décider de la nature de l'aide qu'ils apporteront à l'État ayant besoin de leur assistance (militaire ou civil).

Tout comme pour l'article 5 de l'OTAN, et au regard des termes de l'article 42.7 TUE, il ne fait aucun doute qu'une cyberattaque doit constituer une agression armée pour que les États membres puissent y répondre en légitime défense collective en application de l'article 42.7 TUE. Pour prendre part à l'exercice d'une légitime défense collective en application de cet article, en cas d'agression armée cyber sur un autre État membre par exemple, la France ne doit pas nécessairement attribuer elle-même, mais elle doit valider avec certitude le processus d'attribution réalisé par l'État victime.

k. L'article 51 de la Charte des Nations Unies

En vertu de l'article 51, une agression armée ouvre le droit de l'État victime à faire usage de la légitime défense individuelle ou collective. Une cyberattaque peut constituer une agression armée pour peu qu'elle atteigne un certain seuil de gravité. Ce seuil sera déterminé de manière politique, au cas par cas, en fonction d'un certain nombre de critères : contexte politique ou diplomatique, existence de dommages, origine de l'instigateur, intention hostile caractérisée, degré de l'impact, conséquences pour la sécurité nationale, atteinte à des fonctions critiques, etc.

Il est possible de réagir au titre de la légitime défense à une agression armée menée dans le cyberespace, par des moyens physiques ou numériques. En tout État de cause, l'emploi de la force dans le cadre de la légitime défense devra respecter les principes de proportionnalité et de nécessité tels qu'établis par la CIJ.

Par ailleurs, la France considère que dans le cas d'attaques cyber non déclenchées mais sur le point de l'être de façon imminente et certaine (pourvu que l'impact de cette agression soit suffisamment grave), le droit à la légitime défense préemptive pourra être légitimement invoqué. Néanmoins, au même titre que pour les opérations dans le monde « physique » la légitime défense préventive (1) n'est pas reconnue.

5. La prise en compte des spécificités des opérations militaires dans le cyberespace dans le processus d'élaboration des normes

Sur le plan européen et international, le ministère des Armées conduit une stratégie d'influence juridique complète, d'une part en participant aux différents forums concernant la régulation des activités étatiques dans le cyberespace (participation à l'élaboration du *UE Cybersecurity Act* en lien avec l'ANSSI, participation aux travaux de l'ENISA, échanges dans le cadre du réseau CyberCo, participation aux travaux de la NATO CCDCOE) afin d'y diffuser et d'y défendre ses positions juridiques, et d'autre part en diffusant ces mêmes positions par le truchement de publications dédiées et détaillées telles que le Manuel de droit des opérations militaires et l'interprétation de la France concernant le droit international applicable aux cyber opérations, lesquelles seront ou sont d'ores et déjà traduites en langue anglaise afin de faciliter leur diffusion.

Ainsi la position de la France est aujourd'hui largement connue et partagée : les normes du droit international existantes s'appliquent au cyberespace, lorsqu'elles sont considérées au regard des spécificités du cyberespace tout en étant interprétées à la lumière du but et de l'objet du droit international, et suffisent à encadrer les activités dans le cyberespace aussi bien en temps de paix qu'en contexte de conflit armé.

Par ailleurs, l'élaboration des divers documents précisant la position française sur le droit international applicable au cyberespace a nécessité une étroite collaboration avec d'autres services tels que le COMCYBER.

Au niveau national, les spécificités des activités du ministère des armées sont prises en compte au travers de l'articulation entre la compétence générale de l'ANSSI en matière de sécurité des systèmes d'information et la compétence propre du chef d'état-major des armées dans la défense des systèmes d'information militaires qui relèvent de sa responsabilité.

Ces spécificités trouvent également une traduction dans les dispositions relatives aux militaires qui mènent des actions numériques au soutien des opérations extérieures des forces armées, lesquels bénéficient d'un cadre pénal spécifique.

---

(1) En réponse à une potentielle agression armée, c'est-à-dire latente et plus ou moins susceptible de se produire dans le futur.

6. Le cadre juridique de l'action des cybercombattants du ministère des Armées

Le ministère des armées a pris des mesures pour mieux encadrer les activités des cybercombattants dans le cyberespace. Ainsi, la loi du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense a modifié le II de l'article L. 4123-12 du code de la défense pour inclure « les actions numériques » dans la liste déjà existante qui prévoit une excuse pénale pour les opérations mobilisant les capacités militaires se déroulant à l'extérieur du territoire français ou des eaux territoriales.

Cette précision visait à lever toute ambiguïté sur le fait que ce type d'opérations entre bien dans le champ de cette excuse pénale. Ainsi, le COMCYBER peut bénéficier de ce régime protecteur dès lors que les actions qu'il conduit sont rattachables à une opération mobilisant des capacités militaires se déroulant à l'extérieur du territoire national et sous réserve d'un strict respect des règles d'engagement opérationnel conformes au droit international. Sont ainsi prises en compte les spécificités du milieu cyber dématérialisé, global et transfrontières dans lequel ces militaires opèrent : même mobilisés dans le cadre d'une OPEX, ces cybers combattants sont en mesure d'agir depuis le territoire national.

Elle est justifiée par la nécessité d'offrir aux cybercombattants une protection identique à celles des militaires engagés physiquement dans une opération extérieure.

7. Les fondements juridiques des techniques de recueil du renseignement

Il n'existe pas de cadre juridique propre pour le recours aux techniques de recueil de renseignement (TRR) dans le cyberespace et le cadre juridique de droit commun prévu par les dispositions du livre VIII du code de la sécurité intérieure (CSI) trouve à s'appliquer en la matière.

Ainsi, chaque recours à une TRR suppose le respect des principes de nécessité et de proportionnalité. Doit également être pris en compte le droit au respect de la vie privée, au sens de l'article L. 801-1 du CSI.

Seuls les services de renseignement peuvent demander la mise en place d'une TRR. S'agissant du périmètre du ministère des Armées, il s'agit de la DGSE, de la DRSD et de la direction du renseignement militaire (DRM).

Le recours à une TRR suit une procédure particulière :

1/ Une demande écrite et motivée devant préciser la technique à mettre en œuvre, le service demandeur, les finalités poursuivies, les motifs, la durée de validité de l'autorisation, les personnes, lieux ou véhicules concernés ;

2/ La Commission nationale de contrôle des techniques de renseignement (CNCTR) émet un avis conforme dans les 24 heures ;

3/ Le Premier ministre autorise ou non la mise en œuvre de la TRR.

Pour obtenir des renseignements sur les risques d'attaques cyber au moyen d'une technique de recueil, la finalité invoquée par les services de renseignement est celle visée au 1° de l'article L. 811-3 du CSI (« *l'indépendance nationale, l'intégrité du territoire et la défense nationale* »). Les demandes de TRR présentées sur ce fondement représentent 3 % du total des demandes adressées à la CNCTR.

Les TRR susceptibles d'être mises en œuvre à ce titre sont les suivantes :

1/ Le recueil de données informatiques (article L. 853-2 du CSI, technique qui consiste par exemple à procéder à des copies de disque dur ou de serveurs informatiques) ;

2/ L'interception de sécurité (article L. 852-1 du CSI, captation des correspondances échangées depuis ordinateur ou un smartphone) ;

3/ Le dispositif technique de proximité (article L. 851-6 du CSI du type IMSI-Catchers, toujours en vue d'une intrusion dans un support informatique) ;

4/ L'exploitation des données interceptées dans le cadre de mesures de surveillance internationale (articles L. 853-1 et suivants du CSI, exploitation des données interceptées sur les réseaux internationaux de communications électroniques).

Pour le ministère des Armées, ces mesures sont essentiellement mises en œuvre par la DGSE et ne peuvent en tout État de cause l'être que pour une durée limitée (d'un, deux ou quatre mois selon la technique en cause). Les données recueillies ne peuvent elles-mêmes être exploitées que pendant une durée limitée (de 1 à 4 mois selon la technique et jusqu'à six années pour l'exploitation des données de connexion issues de la surveillance internationale).

Ces dispositions, validées par le Conseil constitutionnel, n'ont pas été remises en cause par la Cour de Justice de l'Union européenne (arrêt La Quadrature du Net du 6 octobre 2020).

8. L'absence de cadre juridique relatif à l'hygiène numérique

a. Les règles applicables en matière d'hygiène numérique

Aucune disposition légale ne fixe les règles applicables en matière d'hygiène numérique. Toutefois, sujet d'actualité par essence, le ministère est pleinement mobilisé et la sensibilisation des acteurs concernés passe par l'instauration de règles de droit souple.

Ainsi, un guide du bon usage des réseaux sociaux a été adopté en 2021 pour les agents du ministère des Armées. Il rappelle le principe de discrétion professionnelle des agents du ministère, militaires comme civils, en précisant :

1/ les erreurs à ne pas commettre (séparation de la vie privée et professionnelle sur les réseaux sociaux, ne pas faire mention de son unité, de son grade, de son nom et ne pas faire de photo en tenu de militaire…) ;

2/ les bons réflexes afin de se protéger sur les réseaux sociaux (sécuriser les adresses mails et les terminaux comme les ordinateurs portables ou smartphones, limiter les informations privées comme les adresses postales, utiliser un pseudonyme, choisir un mot de passe complexe, utiliser une authentification à deux facteurs) ;

3/ et les règles qui s'imposent aux agents (devoir de discrétion, secret professionnel et devoir de réserve, être garant de l'image des armées).

Ce guide précise également les principes à adopter en opération extérieure afin d'assurer la sécurité des missions. Par exemple, la géolocalisation doit être désactivée, les paramètres de sécurité doivent être activés et il est interdit de filmer les opérations militaires, de diffuser des photos ou vidéos informant sur le camp et les missions sans l'accord de l'État-major des armées.

Par ailleurs, une fiche de vigilance à destination des officiers de sécurité a été rédigée par la DPID sur les réseaux sociaux, l'internet de loisir et les agents de la défense.

b. Des sanctions en cas de révélation d'informations sensibles

Plusieurs leviers existent pour sanctionner sur un plan disciplinaire ou professionnel (retrait notamment partiel ou total, temporaire ou définitif d'une qualification professionnelle, prononcée par décret en Conseil d'État pour les militaires) la divulgation d'informations sensibles ou protégées. Le cas échéant, les agents encourent cumulativement des sanctions pénales.

i. L'obligation de discrétion, sanctionnée disciplinairement, s'applique à tout agent du ministère

Conformément aux dispositions de l'article L. 121-7 du code général de la fonction publique (CGFP), l'agent public doit faire preuve de discrétion professionnelle pour tous les faits, informations ou documents dont il a connaissance dans l'exercice ou à l'occasion de l'exercice de ses fonctions. Le statut général prévoit la même obligation pour les militaires. En dehors des cas expressément prévus par la loi, les militaires ne peuvent être déliés de cette obligation que par décision expresse de l'autorité dont ils dépendent (article L.4121-2 du code de la défense).

ii. Le non-respect du devoir de réserve peut également être sanctionné disciplinairement

Les agents publics sont soumis conformément à l'article 121-2 du CGFP à une obligation de neutralité. Pour les militaires, l'article L. 4121-2 du code de la

défense dispose que « *les opinions ou croyances, notamment philosophiques, religieuses ou politiques, sont libres. Elles ne peuvent cependant être exprimées qu'en dehors du service et avec la réserve exigée par l'État militaire. Cette règle s'applique à tous les moyens d'expression (…).* »

L'ensemble des agents publics est astreint par le CGFP au secret professionnel, sous peine des sanctions prévues par l'article 226-13 du code pénal (CP) en cas de révélation des informations couvertes par ce secret. *A contrario*, aucune disposition du statut général ne soumet par une obligation générale, en raison de son seul statut, le militaire au secret professionnel, le code général de la fonction publique ne lui étant pas non plus applicable (article L.6 du CGFP). Des statuts, fonctions ou missions particuliers résultant d'une disposition spéciale peuvent néanmoins astreindre un militaire à une telle obligation et lui faire encourir les sanctions prévues à l'article 226-13 du code pénal. Cela concerne par exemple les agents disposant d'un accès à des informations personnelles sur la santé ou la situation familiale ou les agents habilités en charge du contrôle *a posteriori* des exportations d'armement.

iii. Les atteintes au secret de la défense nationale

Toute personne qui divulgue des informations classifiées, soit directement, soit en les transmettant à des personnes qui les communiqueront dans les médias commet le délit de compromission énoncé par les dispositions de l'article 413-10 du code pénal (« *est puni de sept ans d'emprisonnement et 100 000 euros d'amende le fait pour toute personne dépositaire, (…) d'un procédé, objet, document, information, réseau informatique, donnée informatisée ou fichier qui a un caractère de secret de la défense nationale (…) de le porter à la connaissance du public ou d'une personne non qualifiée. En cas d'imprudence ou de négligence, l'infraction est punie de 45 000 euros d'amende et de 3 ans d'emprisonnement*. »). Est dépositaire du secret de la défense nationale l'agent civil ou militaire qui, par son état, sa profession, sa fonction ou sa mission, est habilité à avoir accès à une information classifiée et, cumulativement, a le besoin d'en connaître.

iv. L'application de la protection pénale de l'anonymat ou appartenance à certains services ou unités spécialisés

Les agents des services de renseignement et les membres des unités des forces spéciales bénéficient d'un dispositif de protection pénale de leur anonymat, prévu aux articles 413-13 et 413-14 du code pénal, sanctionnant la révélation de toute information susceptible de permettre la découverte de l'identité d'emprunt ou réelle d'un agent de renseignement, de sa fausse qualité ou de son appartenance au service. Les peines encourues sont cinq ans d'emprisonnement et 75 000 euros d'amende. Ce même article précise que la révélation commise par imprudence ou négligence, par une personne dépositaire, de l'information citée ci-dessus est puni de trois d'emprisonnement et 45 000 euros d'amende.

Enfin, le ministère des Armées élabore un projet de rédaction d'une politique ministérielle visant à encadrer et à maîtriser les risques de l'utilisation des outils numériques dans un cadre privé par les agents du ministère des Armées, leurs proches et leurs familles.

9. Les affaires dites Pegasus et Predator Files, révélatrices de l'impératif de régulation du marché des armes cyber offensives

a. L'affaire dite Pegasus

En octobre 2019, Amnesty International a publié un rapport sur l'utilisation de Pegasus en vue de cibler des défenseurs des droits humains. En juin 2020, Amnesty International a mis au jour d'autres éléments similaires. Une synthèse des différentes enquêtes a été publiée sur le site internet d'Amnesty International (1) .

Lors de ces enquêtes, le Security Lab a identifié des attaques par « injection réseau ». Ce type d'attaque permet à ses auteurs de surveiller, d'intercepter et de manipuler les données de trafic Internet de la personne ciblée. Le navigateur Internet du téléphone est redirigé vers un site malveillant, sans aucune intervention de son ou sa propriétaire. Le logiciel espion Pegasus est alors installé de façon invisible sur le téléphone à partir de ce site. Une attaque par injection réseau nécessite soit de se situer à proximité des personnes ciblées, soit d'avoir accès aux réseaux mobiles du pays – ce que seuls les pouvoirs publics pourraient autoriser.

En mai 2021, Amnesty International a publié, conjointement avec Privacy International et le Centre for Research on Multinational Corporations (SOMO), un briefing visant à mettre en lumière la structure complexe et opaque de l'entreprise NSO Group.

En juillet 2021, l'enquête sur le Projet Pegasus a révélé que le logiciel espion de NSO Group est utilisé contre des militants, des journalistes et des dirigeants politiques partout dans le monde. Amnesty International a été le partenaire technique de cette enquête. Le Security Lab a réalisé l'analyse technique des téléphones portables des personnes susceptibles d'être victimes de Pegasus. Cette analyse technique permet de déterminer si un appareil a été visé ou s'il contient des traces d'intrusion de Pegasus. Amnesty International a publié un document technique indiquant les moyens, les outils et la méthodologie employés par le Security Lab, ainsi que des annexes techniques concernant les cas individuels mentionnés dans l'enquête.

Un appareil peut être visé de plusieurs façons (à noter que toutes les tentatives d'attaques ne se traduisent pas systématiquement par l'infection de l'appareil visé) :

1/ envoyer à la personne ciblée un lien qui, si elle l'ouvre, la dirige vers une URL malveillante qui fait partie du système Pegasus (attaque dite « un clic »).

---

(1) *https://www.amnesty.fr/actualites/projet-pegasus-revelations-sur-un-systeme-mondial-de-surveillance.*

2/ et exploiter les vulnérabilités inconnues dans le code de certaines applications telles que WhatsApp, iMessage, iTunes, *etc*., sans que la personne soit invitée à cliquer sur un lien (attaque dite « zéro clic »). Dans le cadre du Projet Pegasus, ce sont ces attaques « zéro clic » qui ont été mises en lumière.

Une fois installé dans le téléphone d'une personne, Pegasus permet à l'auteur de l'attaque d'avoir entièrement accès au contenu de ce téléphone (SMS, courriels, activité sur Internet, micro, appareil photo, appels téléphoniques et contacts).

Le Projet Pegasus a révélé que parmi les personnes désignées comme des cibles potentielles figurent des dirigeants politiques (14 chefs d'États et plus de 600 responsables politiques de 34 pays potentiellement ciblés), des militants et des journalistes (180 journalistes de 20 pays potentiellement ciblés). Au moment des révélations de juillet 2021, des clients potentiels de NSO ont été identifiés dans 11 pays.

Suite au Projet Pegasus, Amnesty International a publié un rapport relevant les principaux enseignements du point de vue du droit international et en particulier du droit international relatif aux droits humains qui ressortent des révélations et des analyses techniques. Des recommandations ont été formulées aux différents acteurs. En particulier, Amnesty International demande aux États :

1/ d'instaurer un moratoire immédiat sur l'exportation, la vente, le transfert et l'utilisation des logiciels et technologies de surveillance jusqu'à la mise en place d'un cadre réglementaire conforme aux droits humains ;

2/ de mener une enquête indépendante, transparente et impartiale sur toutes les licences d'exportation accordées pour des technologies de surveillance numérique et résilier les autorisations de mise sur le marché et d'exportation dès lors qu'il existe un risque substantiel que ces technologies contribuent à des atteintes aux droits humains ;

3/ et de s'assurer de la conformité de leurs pratiques de surveillance numérique avec les normes internationales.

b. L'affaire dite des Predator Files

Le Security Lab d'Amnesty International a fourni une assistance technique dans le cadre de l'enquête des Predator Files [(1)] menée par l'European Investigative Collaborations (EIC), concernant l'alliance Intellexa, basée en Europe, et Predator, son logiciel espion extrêmement invasif. Le Security Lab a analysé des brochures et des documents techniques ainsi que l'infrastructure technique d'Intellexa. Predator est un logiciel espion qui peut être installé sur un appareil mobile au moyen d'une attaque « un clic » ou « zéro clic ». L'alliance Intellexa propose aussi

(1) https://www.mediapart.fr/journal/international/dossier/predator-files-toutes-nos-revelations.

différentes techniques pour installer le logiciel espion via des « attaques tactiques », qui permettent de prendre pour cible les appareils situés à proximité.

L'enquête des journalistes a révélé la présence de produits de l'alliance Intellexa dans au moins 25 pays en Europe, en Asie, au Moyen-Orient et en Afrique. L'analyse réalisée par Amnesty International d'une récente infrastructure technique liée au système de logiciel espion Predator indique que des activités connexes, sous une forme ou une autre, ont été menées dans plusieurs pays.

L'alliance Intellexa compte des entreprises implantées dans différents États. L'enquête sur les Predator files met en évidence que des produits de surveillance extrêmement invasifs sont vendus à une échelle presque industrielle et peuvent librement fonctionner dans l'ombre sans qu'ils soient contrôlés, ni soumis à une quelconque forme de reddition de comptes.

Dans le cadre des Predator Files, Amnesty International a publié un rapport révélant que des membres de la société civile, des journalistes, des personnalités politiques et des universitaires dans l'Union européenne (UE), aux États-Unis et en Asie ont été les cibles d'attaques révoltantes menées au moyen du logiciel espion Predator. Le rapport établi qu'entre février et juin 2023, au moins 50 comptes appartenant à 27 personnes et 23 institutions ont été publiquement pris pour cible, avec Predator, sur les plateformes de réseaux sociaux X (anciennement Twitter) et Facebook. Parmi les personnes visées par le logiciel espion Predator figurent des responsables des Nations unies, un sénateur et un député américains, un eurodéputé français, la présidente du Parlement européen ainsi que celle de Taiwan.

c. Un rôle important de l'ANSSI pour se protéger contre les armes cyber offensives

Interrogée sur l'affaire dite Pegasus, l'ANSSI a indiqué qu'elle ne peut commenter le dossier du fait de sa judiciarisation. L'ANSSI constate cependant que, malgré les révélations sur le programme Pegasus de NSO Group en 2021, le secteur des entreprises privées de LIO reste très actif. Si aucun ciblage récent de la France ou de personnalités françaises à l'aide d'espiogiciels n'est connu, le dévoiement potentiel de ce type d'outil justifie le suivi de ces entreprises et de leurs capacités.

Parallèlement à ces acteurs offrant des solutions d'espiogiciels, des entreprises, telles que BellTrox InfoTech Services, fournissent des prestations apparentées à de la LIO, moins sophistiquées mais persistantes, comme de l'expertise humaine (*hacker for hire*). Elles mènent des activités intenses d'espionnage économique et politique au profit de clients variés qui peuvent porter atteinte au secret des affaires et à la défense nationale. Les récentes révélations du journal The Sunday Times et de l'organisation non gouvernementale The Bureau of Investigative Journalism à propos de campagnes d'espionnage de personnalités ayant critiqué l'attribution de la coupe du monde de football de 2022 au Qatar en sont une nouvelle illustration. Quatre personnalités françaises feraient partie des cibles présumées. Les publications régulières sur les capacités cyber offensives

privées soulignent la nécessité de renforcer les capacités de détection et d'investigation.

Afin de répondre à ces enjeux, l'ANSSI est très impliquée dans la protection des communications téléphoniques des autorités publiques françaises. Pour cela, elle agit sur plusieurs plans :

1/ elle apporte un accompagnement à l'Opérateur des systèmes d'information interministériels classifiés (OSIIC) dans la sécurisation des moyens téléphoniques mis à disposition des autorités dans le cadre de leurs fonctions ;

2/ et en lien avec ses partenaires du C4 TechOps, elle assure un suivi des techniques utilisées par des entreprises privées fournissant des solutions d'espiogiciel contre des téléphones. Si la menace le justifie, l'ANSSI peut notamment mettre en œuvre les articles L. 2321-2-1 du code de la défense ou l'article L. 33-14 du code des postes communications électroniques afin de détecter des victimes de ses solutions sur le territoire national.

d. Que penser des révélations relatives aux affaires Pegasus et Predator ?

S'il est délicat d'avoir une opinion arrêtée sur les affaires Pegasus et Predator compte tenu de l'impossibilité de connaître de ces affaires eu égard à leur caractère judiciarisé, il n'en demeure pas moins qu'elles sont révélatrices de la nécessité de mieux régulier, à l'échelle internationale, l'usage et la commercialisation des armes cyber offensives. Ainsi, sans se prononcer sur le fond de ces affaires, une meilleure régulation de l'utilisation par les États et de la commercialisation des armes cyber offensives apparaît souhaitable.

En outre, les rapporteurs estiment qu'il est nécessaire de procéder à une évaluation juridique afin de déterminer la capacité de la France et, plus largement, de la communauté internationale, à répondre par le corpus juridique national et international actuel au mercenariat dans le domaine de la cyberdéfense. Ils ne sont pas convaincus que le droit, et singulièrement le droit international, réponde à l'émergence de cette nouvelle catégorie d'acteurs, mise en lumière par la guerre en Ukraine, notamment. La clarification du cadre juridique en la matière semble indispensable, eu égard à la multiplication de ces acteurs et à leur potentielle nuisance.

IV. LE DÉFI CAPACITAIRE : DOTER NOS ARMÉES DE CAPACITÉS TECHNIQUES POUR FAIRE FACE AUX MENACES

1. La cyberdéfense est une priorité forte de la LPM 2024-2030

La LPM pour les années 2024 à 2030 prévoit un effort financier conséquent de 4 milliards d'euros sur la période de la programmation pour la cyberdéfense, érigée en domaine prioritaire au même titre, entre autres, que l'espace, le renseignement ou la défense sol-air. À titre de comparaison, le budget dédié à la

cyberdéfense dans la loi de programmation militaire pour les années 2019 à 2025 s'élevait à 1,6 milliard d'euros, soit une hausse de 150 % dans la LPM.

Ce budget inédit est le fruit d'un travail conduit par le ministère pour tracer les orientations capacitaires dans le domaine de la cyberdéfense à l'horizon 2030 sur la base d'un schéma directeur mis à jour en juin 2021 et d'une programmation des ressources jusqu'en 2027. L'état-major des armées, en s'appuyant sur le commandement de la cyberdéfense, a déterminé les besoins opérationnels, tandis que le cadrage physico-financier a été élaboré conjointement avec la Direction générale de l'armement.

Ce budget permettra au ministère des Armées de renouveler ses capacités cyber existantes et d'en acquérir de nouvelles. À cet égard, sur les 4 milliards d'euros, environ 3,7 milliards d'euros seront consacrés aux programmes à effet majeur, qui relèvent du programme 146 « Équipement des forces ». Plus précisément, l'effort financier total se répartit principalement entre trois catégories de domaines :

– le domaine de la cyberprotection, à hauteur de 1,6 milliard d'euros, pour, d'une part, le renouvellement des chiffreurs militaires afin de garantir l'inviolabilité des données, notre souveraineté numérique et faire face à l'arrivée du quantique, et, d'autre part, le développement de systèmes de communication sécurisés permettant l'échange d'informations sensibles et classifiées entre les différents sites du ministère et avec ses partenaires. Ces efforts constitueront le socle de sécurité rendant possible la réalisation d'opérations interarmées et interalliées ;

– le domaine de la LID, à hauteur de 1 milliard d'euros, pour l'extension des capacités de surveillance à l'ensemble du périmètre du ministère par le développement et l'acquisition de sondes pour tous les systèmes d'information et les systèmes d'armes, ainsi que pour l'acquisition de capacités de détection et d'investigation dans une optique d'entraînement des personnels spécialisés et de capacités de réponse aux incidents informatiques. En outre, ce budget permettra de mettre en cohérence les pratiques, les procédures et les équipements des trois armées en ce domaine, afin de garantir au chef d'état-major des armées une liberté d'action et de renforcer le pilotage au niveau stratégique ;

– et les nouveaux domaines de lutte que sont la LIO et la L2I, à hauteur de 1,4 milliard d'euros, pour la diversification des capacités militaires en vue de leur intégration par les armées en opérations.

Il ne faut toutefois pas se limiter au budget du patch cyber pour apprécier l'effort global du ministère. À titre d'exemple, le budget dédié à la transformation numérique du ministère, à hauteur de 8 milliards d'euros, contribuera au renforcement de la résilience des systèmes d'information. Il en ira de même pour l'innovation de défense, dont le budget contribuera à la cyberdéfense.

En outre, il y a des synergies entre la cyberdéfense et d'autres domaines, tels que, par exemple, la guerre électronique. Les composantes de surveillance et de

protection du domaine de la guerre électronique sont majoritairement portées par l'incrément n° 1 du programme interarmées ROEM tactique lancé en réalisation en 2018, par le programme BARAGE lancé en réalisation en 2008 et par les programmes d'armement des équipements. La composante d'attaque électronique du domaine guerre électronique, qui vise à agir dans le spectre à des fins offensives, n'est portée par aucun PEM pour la période 2024-2030. Elle est néanmoins traitée sur cette période par des expérimentations et des études de montée en maturité technologique qui permettront, dans le contexte d'engagement actuel, de tirer parti des actions combinées et complémentaires de la guerre électronique et de la cyber défense.

2. L'équilibre entre l'efficacité et la cybersécurité

La cybersécurité d'un système, quand elle est considérée comme une obligation de conformité à des réglementations, peut en effet être vue comme un ensemble de contraintes pesant fortement sur l'expérience utilisateur. La recherche du meilleur compromis entre le niveau de service et le niveau de sécurité des systèmes dont elle assure la maîtrise d'ouvrage est au cœur des préoccupations de la DGA. Les méthodes de conception de type « agile » qui mettent l'utilisateur final dans la boucle tout au long du développement permettent d'améliorer l'acceptabilité de ces contraintes, par exemple en travaillant sur l'ergonomie ou les interfaces homme-machine.

Par ailleurs, les approches nouvelles qui traitent la cybersécurité comme une performance système à part entière, et donc sujette à compromis comme toute autre performance, doivent aussi permettre de dimensionner la cybersécurité au juste nécessaire et ici encore d'améliorer l'acceptabilité des contraintes.

Ainsi, le SIC du ministère doit concilier deux réalités très différentes. D'une part, les outils de fonctionnement courant, au bénéfice des usagers du ministère des Armées, doivent répondre aux nouveaux usages, en perpétuelle évolution, ainsi qu'aux attentes des utilisateurs. D'autre part, les outils nécessaires aux opérations (parmi lesquels des moyens de fonctionnement courant), doivent faire preuve de résilience pour ne pas constituer un moyen d'entrave de l'action militaire française et doivent être en mesure de garantir la souveraineté de l'action militaire française en protégeant ses informations les plus sensibles. L'équilibre trouvé en mutualisant certains moyens d'usage dual, permet de disposer de moyens communs performants posés sur un socle internalisé et résilient.

Les systèmes d'information développés par le ministère sont globalement efficaces et sécurisés par nécessité de robustesse et de résilience. Toutefois, comme l'a indiqué la DIRISI, la sécurisation de ces systèmes peut entraîner un allongement de délais et une dépense d'énergie importante en termes de personnels qui peut conduire à des retards et ainsi diminuer l'efficacité recherchée. Ainsi l'équilibre est difficile à atteindre et il est nécessaire de faire preuve d'une gestion du risque dynamique, d'adaptabilité et de souplesse plus que d'un simple respect statique des normes.

Le ministère a également par construction un parc de SI et de systèmes de communications très diversifié. Ainsi, la dette technique est importante au ministère et les systèmes les plus anciens peuvent avoir des écarts avec les normes actuelles. Toutefois, la culture de la gestion du risque et la systématisation de l'homologation compensent ces éventuelles vulnérabilités.

3. La sécurisation des systèmes d'information au défi des spécificités des armées

Chaque armée a ses spécificités et ses modalités d'action sur les théâtres d'opération. Or, pour permettre à l'ensemble des unités de communiquer, il est nécessaire de définir un réseau et des outils communs. À cette fin, la DGNUM définit un socle numérique ministériel mutualisé dans le cadre d'un comité dédié en lien avec la DIRISI et les trois armées. Cette ambition peut se heurter parfois aux spécificités de milieu et aux exigences de chaque entité. Le ministère des Armées doit parfois fournir des efforts importants pour forcer les acteurs à se passer d'outils achetés sur étagère. Beaucoup de solutions sur étagère correspondent aux besoins des armées, mais le ministère doit trouver un équilibre avec l'impératif de sécurité, quitte à dégrader l'efficacité de l'outil si besoin. S'il parvient en général à imposer un standard ministériel pour les outils utilisés par les trois armées, c'est parfois plus compliqué. Chaque armée souhaite qu'on prenne en compte ses spécificités, ce qui complique ipso facto le processus de sécurisation et peut parfois être très coûteux.

Ainsi, la DGNUM est garante de l'homogénéité des SIC utilisés par les armées et, plus généralement, de la cohérence de l'urbanisation des SIC du ministère. Cette doctrine est fixée dans le cadre d'un document relatif à la cohérence technique qui fixe un nombre maximal de technologiques utilisables, qui ne peut être dépassé qu'avec dérogation. Si la DGNUM ne vérifie pas chaque projet un à un, une validation de son besoin fonctionnel sous la forme d'un visa d'architecture est nécessaire pour son déploiement, ce qui constitue un filtre. À chaque fois qu'une armée exprime de nouveaux besoins, le ministère des Armées analyse la liste des logiciels requis et détermine s'il y a des failles de sécurité ; auquel cas, ils sont bannis. Ce faisant, le ministère essaie de faire converger les pratiques. Mais si cette technique fonctionne bien sur les nouveaux systèmes d'information, elle fonctionne moins bien sur les anciens. Toutefois, le ministère ne fait pas que refuser les projets insatisfaisants en termes de sécurité et veiller à l'homogénéisation : il propose des solutions en cas de blocage et peut promouvoir certains projets, voire les appuyer. Le ministère des Armées accompagne également l'émergence d'entreprises nationales en vue de travailler avec elles de manière sécurisée et fait de la veille technologique au bénéfice des armées, au travers de l'Agence de l'innovation de défense (AID), sur des domaines d'avenir nécessitant une expertise forte comme l'intelligence artificielle ou le calcul intensif. Enfin, il veille ce que les financements prennent en compte les priorités du chef d'état-major des armées (CEMA).

4. La sécurisation des systèmes d'armes

La surface numérique des systèmes d'armes est de plus en plus importante, d'une part car les systèmes d'armes embarquent de plus en plus de composants numériques et d'autre part car les systèmes d'armes sont très massivement interconnectés entre eux *via* des solutions numériques. Cette augmentation de la surface d'attaque impose de prendre en compte la menace cyber afin de les protéger contre ces nouvelles menaces. Les programmes comme le SCAF ou SCORPION, qui comprennent non seulement des systèmes d'armes mais aussi des solutions de connectivité entre les différents composants les constituant, embarquent une forte dimension cyber dans leur processus d'ingénierie et de développement.

La prise en compte de la cybersécurité des systèmes d'armes n'est toutefois pas nouvelle. Les enjeux de cyberprotection, et de cyberdéfense étaient déjà bien pris en compte dans plusieurs programmes d'armement par le passé. On peut citer par exemple les capacités de LID intégrées au périmètre des programmes SIA (système d'information des armées) ou DESCARTES (réseaux fixes de télécommunications), lancés dans la dernière décennie. Les systèmes à composantes numériques du ministère doivent respecter un corpus documentaire fourni, en particulier condensé dans le « cadre de cohérence technique », actualisé annuellement sous le pilotage de DGNUM, auquel contribue la DGA, qui fixe l'ensemble des normes, standards et exigences à appliquer dans le domaine numérique.

Concernant l'usage des technologies de *cloud*, le ministère des Armées décline la doctrine Cloud de l'État qui fixe des contraintes et restrictions à l'usage d'hébergement informatique chez des tiers industriels comme Amazon. De plus, le recours à des services logiciels en mode locatif (*Software as a Service*, Saas) est soumis de manière systématique à un visa de la DGNUM. La réglementation relative à la protection des informations sensibles ou classifiées permet d'interdire le recours à des solutions de *cloud* non maîtrisées. Pour le niveau « DR », l'absence de pénalisation en cas d'infraction constitue cependant une limite. Par ailleurs, pour les données soumises au contrôle export, le recours à un *cloud* étranger peut être considéré comme une exportation et doit donc être traité en tant que tel.

S'agissant de la sécurisation des systèmes d'armes, l'industriel est en charge de l'informatique embarquée. Le défi auquel le ministère des Armées est confronté aujourd'hui est celui relatif aux ambitions qui peuvent être fixées aux industriels en termes de sécurité. La DGA a, conjointement avec l'EMA, mis en place dès 2019 un cercle de confiance avec les huit principaux industriels de la BITD afin de définir avec eux des exigences techniques fortes de sécurité à intégrer dans les documents de spécification des systèmes d'armes. À titre d'exemple, il est demandé aux industriels d'identifier, de sécuriser et d'homologuer les systèmes d'information dits « névralgiques » qui sont à la fois critiques d'un point de vue cyber et exposés vers l'extérieur. Ces SI sont considérés comme « névralgiques » si par exemple leur piégeage pouvait conduire à une perte d'intégrité ou de disponibilité du système d'arme final.

De manière plus générale, la DGA se transforme aujourd'hui afin d'être capable d'exercer un rôle, nouveau, de maître d'œuvre étatique du système de défense. Cela va la conduire à renforcer son pouvoir prescriptif vis-à-vis des maîtres d'œuvre industriels de défense en matière de standards et d'outils de développement logiciel et en matière de modèle de données. En outre, la cyberprotection fait partie des critères d'appréciation de l'opportunité d'acquérir une solution ou un système d'arme étrangers. Dans la majorité des cas, les systèmes sont achetés en l'état. Afin de maîtriser le risque cyber, la DGA étudie systématiquement avec les armées l'éventuelle mise en place de mesures de protection complémentaires « autour » de ces systèmes.

Toutefois, jusqu'où le ministère peut-il pousser la prescription si, par exemple, Dassault voulait recourir à l'architecture d'Amazon pour le stockage des données du Rafale ? Si le service des affaires industrielles et de l'intelligence économique (S2IE) de la DGA a fixé une doctrine pour l'achat des systèmes d'armes au sens strict (par exemple pour les chiffreurs ou les réseaux radios), pour l'informatique embarquée ou pour le numérique qui « gravite » autour du système d'armes, c'est essentiellement à la main des industriels aujourd'hui. Jusqu'ici, la doctrine consistait à privilégier les constructeurs que le ministère des Armées connait déjà et qui étaient en adhérence avec la BITD. Désormais, le ministère réfléchit à l'élaboration d'une doctrine orthogonale consistant à exiger le recours à des technologies souveraines lorsqu'il estime que c'est nécessaire et à ne tolérer le recours à des technologies non-souveraines que lorsque le risque est faible ou nul.

5. Le recours aux solutions des GAFAM, le chiffrement des données et la souveraineté numérique

Il convient de distinguer les domaines dans lesquels le recours à des solutions fournies par les GAFAM est possible ou non. Pour des domaines de souveraineté absolue comme, par exemple, la dissuasion nucléaire, le recours à des solutions étrangères est exclu, y compris pour les puces électroniques, qui ne sont pas fournies par les GAFAM. En revanche, s'agissant, par exemple, des serveurs et des systèmes d'exploitation, il n'y a quasiment rien sur le sol européen : il n'existe pas, à ce jour, de système d'exploitation souverain, ce qui contraint le ministère des Armées à recourir à des solutions extra-européennes, et singulièrement celles des GAFAM. La stratégie du ministère des Armées consiste alors à miser sur des couches de chiffrement ; de sorte que, certes, le système d'exploitation a été édité par Microsoft et n'est donc, de ce fait, pas souverain, mais les données ne peuvent pas être lues grâce au chiffrement. Ainsi, l'architecture de sécurité qui a été pensée pour les terminaux et les centres de données du ministère limite, en cas de compromission, l'accès aux données en clair : dans ce cas, seules des données chiffrées seront captées en cas d'attaque informatique ou de cyber-espionnage. Si des données chiffrées ont été captées, le ministère des Armées indique que cela ne sera pas grave car il ne sera pas possible de les déchiffrer, et donc de les lire. Microsoft n'a donc, de ce fait, pas accès aux données du ministère des Armées.

Sur les réseaux classifiés, l'ensemble des données sont chiffrées et sont déconnectées vis-à-vis de l'extérieur. C'est, par exemple, l'outil utilisé par le COMCYBER : il travaille sur un réseau qui fonctionne sur Windows mais qui n'est pas connecté à internet. L'outil de travail au ministère est le réseau Intradef, lequel est au niveau « diffusion restreinte » et sur lequel rien ne transite en clair. Ainsi, si des données sont interceptées, elles seront illisibles.

En revanche, pour les systèmes d'information de fonctionnement courant au bénéfice des usagers hébergeant des données non-sensibles, notamment celles que le ministère des Armées peut collecter ou mettre à la disposition du public dans le cadre des processus de recrutement ou les outils dédiés à la communication de la délégation à l'information et à la communication de la défense (DICOD), les systèmes doivent, par définition, être reliés à Internet. Pour ces systèmes d'information, le ministère des Armées envisage d'exiger *a minima* le label SecNumCloud de l'ANSSI. Par exemple, l'outil utilisé aujourd'hui par la DICOD pour faire des montages vidéos est performant mais est hébergé aux États-Unis. Le ministère des Armées s'est donc fixé pour objectif de trouver une meilleure alternative d'ici un an, et à défaut, il ne recourra plus à cette solution. La DGNUM aborde ces questions ouvertement avec la DIRISI, le COMCYBER et la DGA. Il s'agit de données qui ne sont pas sensibles au sens de la classification, mais le ministère des Armées est dans une zone grise, qui nécessite une appréciation fine au cas par cas pour déterminer s'il est tout de même nécessaire d'acquérir un outil souverain, le coût induit par une telle acquisition étant un des facteurs d'appréciation. Le ministère des Armées se pose constamment la question : que fera une armée adverse avec l'information renseignée dans un outil de requête non-souverain ?

6. Le piège Microsoft

Le système d'information du ministère repose sur de nombreux constituants matériels et logiciels. Le système d'exploitation n'est qu'un des constituants logiciels et ce n'est pas le seul nécessaire pour garantir la souveraineté de nos SIC. Pour obtenir un SI entièrement souverain, il faudrait également une filière souveraine pour les composants matériels et leurs logiciels (processeurs, microcontrôleurs, *etc*.) ainsi qu'une filière pour les applications logicielles (suite bureautique, navigateurs, *etc*.). Aussi, le développement d'un système d'information entièrement souverain paraît inatteignable et d'un coût prohibitif.

Afin de maîtriser le risque en matière de souveraineté, la DGA fait développer des équipements souverains sur les constituants du SI qu'elle estime sensibles afin d'en garantir la sécurité tout en atteignant un niveau de confiance élevé. Elle recherche systématiquement le meilleur équilibre entre coût, maintenabilité, sécurisation et efficacité. Sans se prononcer sur la règle d'extraterritorialité du droit américain, la DGA a indiqué qu'elle lui semblait impossible de reconcevoir et de maintenir, en France ou en Europe, tous les logiciels étrangers que le ministère des Armées utilise dans ses SIC. Cette orientation

induirait pour le ministère des coûts de développement spécifiques conséquents, avec un gain sécuritaire difficile à évaluer.

La doctrine sécuritaire raisonnable selon la DGA est de considérer, dans l'analyse de risques des systèmes concernés, que l'utilisation d'un « produit sur étagère » étranger facilite, pour le pays correspondant, la réalisation d'attaques informatiques avancées. Il s'agit dès lors pour la DGA d'atteindre le meilleur équilibre entre coût, maintenabilité, sécurisation et efficacité, en cherchant à garantir la non-compromission des données sensibles *via* une maîtrise fine des entrées et sorties des SIC. Cette approche procède d'une maîtrise fine des systèmes d'information pour ajuster le choix des solutions et le degré de souveraineté associé au niveau de sécurité recherché. L'utilisation des logiciels étrangers fait dans ce cadre l'objet d'une attention particulière dès lors qu'ils sont utilisés dans des systèmes impliqués dans des activités présentant un risque d'espionnage. Dans ces cas, les dispositions architecturales (sécurité périmétrique, chiffrement gouvernemental) permettent de couvrir le risque induit.

S'agissant par exemple de Microsoft, son rôle se limite à fournir des logiciels. Les infrastructures sur lesquelles ces logiciels tournent sont propriété de l'État et les tâches de configuration et d'administration sont assurées entièrement par des personnels étatiques ou des sociétés de confiance de la BITD nationale (modèle de « *cloud* privé *on-premise* »). À date, il n'est pas envisagé d'apporter de changement majeur à cette doctrine.

Mais le passage de Windows à une logique de service présente le risque d'une réduction graduelle de la capacité du ministère des Armées à exploiter en propre des réseaux basés sur des technologies Microsoft. Cela étant, il semble que Microsoft revient peu à peu sur cette logique devant la résistance des institutions et des entreprises privées. Le risque existe néanmoins. En cas de survenance de ce risque et en fonction de la criticité des usages, il faudrait alors, soit :

1/ migrer vers d'autres systèmes d'exploitation avec les délais et les coûts associés ;

2/ rester sur les anciennes versions logicielles avec les problématiques de maintien en condition de sécurité associées ;

3/ décider d'assumer le risque du SaaS.

7. Le recours aux systèmes d'exploitation et aux logiciels libres est-il pertinent ?

Face au piège dans lequel se trouve le ministère des Armées s'agissant du recours à Microsoft, une solution serait de préconiser le recours au système d'exploitation Linux et aux logiciels libres. Or, une analyse à grande échelle resterait nécessaire pour identifier les coûts, délais, et impacts d'un passage à Linux et aux logiciels libres, et en particulier l'impact du changement des outils de

bureautique sur les utilisateurs et les différents métiers du ministère d'une part, et sur les opérateurs SIC du ministère, dont la DIRISI au premier chef, d'autre part. En effet, l'enjeu d'une telle migration n'est pas seulement technique : il implique la formation, la reconversion et le recrutement de profils dans tous les domaines d'expertises impactés par cette bascule. Interrogée à ce sujet, la DIRSI a indiqué que, contrairement à certaines idées reçues, libre ne veut pas dire gratuit et l'utilisation qui est faite aujourd'hui à la DIRISI des logiciels libres a un coût. Réduire la dépendance à Microsoft poserait des problèmes de compatibilité, aurait un coût équivalent et serait chronophage en termes de formation et de maintien en compétence des administrateurs. Cela demanderait surtout de disposer d'un minimum de ressources humaines internes dédiées et expertes sur un large panel de logiciels libres, ce qui semble inaccessible à court ou moyen terme compte tenu des tensions actuelles en termes de ressources humaines dans le domaine du numérique.

Par ailleurs, pour garantir la souveraineté des SI du ministère des Armées, changer le système d'exploitation ne suffit pas. Il faudrait disposer de versions maîtrisées de nombreux autres logiciels utilisés pour conduire les missions du ministère. Il faudrait également disposer de matériel maîtrisé, construit en France ou en Europe. Or, aujourd'hui, ces logiciels et ces matériels n'existent pas pour l'essentiel, et leur développement, dans le cadre d'une souveraineté nationale ou européenne, semble très difficilement accessible au moins à moyen terme, sans une impulsion politique forte qui dépasserait très largement le périmètre du ministère des Armées.

Enfin, si la décision de changer le système d'exploitation des postes utilisateur était prise, il n'est pas acquis que toutes les fonctionnalités actuelles du socle et des systèmes métiers pourraient être préservées en l'état. Cette décision aurait des répercussions sur la capacité du ministère à faire évoluer l'architecture de sécurité de son socle et donc à assurer la sécurité de ce dernier. Elle retarderait également les travaux nécessaires pour s'assurer de notre interopérabilité avec nos alliés et la capacité de la France à être nation cadre.

8. La cybersécurité de la BITD

La cybersécurité des entreprises de la BITD relève de la responsabilité directe de la DRSD. Le maillage territorial et les actions de la DRSD auprès des entreprises de défense de toutes tailles et activités permettent d'avoir une vision assez claire du niveau de maturité cyber de celles-ci. Le point positif est qu'il est en progression. À l'instar du reste de la société, les entreprises de défense prennent conscience qu'elles sont soumises à un risque croissant de subir une cyberattaque sur leurs systèmes, dont les conséquences seraient potentiellement incompatibles avec leur survie. Cependant, il demeure une très forte hétérogénéité de connaissance des menaces et des risques, des moyens consentis à la prévention et la protection, mais surtout des pratiques d'hygiène informatique, particulièrement au sein des TPE et PME. Le premier vecteur d'infection demeure en priorité la mauvaise hygiène informatique des utilisateurs. Les grands groupes, très ciblés, sont en capacité de se protéger eux-mêmes. La DRSD observe depuis plusieurs années, un report du

ciblage vers leur chaîne de sous-traitance, plus vulnérable. Comme l'a indiqué la DRSD, les attaques sur les entreprises de la chaîne d'approvisionnement ont été multipliées par 4 en un an.

Ainsi, si le risque de cyber espionnage est réel et ne doit pas être négligé car il contribue à la fuite du potentiel scientifique et technique de la nation et au rattrapage technologique des compétiteurs de la France, la cybercriminalité est le principal vecteur d'ingérence cyber et cause de lourdes pertes économiques aux entreprises de défense. L'exfiltration des données puis leur publication sur internet est un phénomène que la DRSD suit de près et prend en compte dans ses actions de sensibilisation et de prévention.

En matière d'ingérence informationnelle, là encore, le niveau est hétérogène. Ce sont principalement les grands groupes qui se dotent de capacités permettant de détecter les éventuelles attaques.

9. La question des exportations d'armes cyber offensives et du rapport aux brokers de vulnérabilités informatiques

S'agissant de la cyberdéfense, la DGA a indiqué que la France n'exporte pas d'autres systèmes que :

- les produits sur étagère proposés par des sociétés duales, dans le cadre du régime de contrôle de l'exportation de biens à double usage, qui s'appuie sur un règlement européen spécifique ;

- et les systèmes de cyberprotection et de LID en tant que constituants d'un système d'armes (aériens ou navals par exemple), dont l'export relève du régime de contrôle des matériels de guerre.

Elle a également indiqué que la France n'exporte aucun système ou sous-système cyber offensif.

S'agissant de ses relations avec les brokers de vulnérabilités informatiques, la DGA a indiqué que le niveau de confiance envers ceux-ci est extrêmement faible. Il est en effet quasiment impossible de connaître le cycle de vie d'une vulnérabilité ou d'un code exploitant celle-ci (qui l'a trouvé ? à combien de personne il a été vendu ? est-ce qu'il contient des marquants ?). Dans le domaine de la LIO, la stratégie de la DGA est donc aujourd'hui de privilégier le recours à des études réalisées par des entreprises de la BITD. Cette approche permet d'avoir une confiance forte dans les vulnérabilités nécessaires à la réalisation d'armes numériques, car, ce faisant, il n'y a pas de risque d'intoxication et de vente à de multiples acteurs.

En l'état, le principal risque que les brokers font peser sur la DGA est lié à leur positionnement sur le marché de l'emploi. L'extrême technicité des travaux à mener fait exploser les prix des vulnérabilités sur le marché, qui peuvent atteindre jusqu'à plusieurs millions d'euros pour une chaîne complète. Ainsi, le risque est

non négligeable de voir un ingénieur expérimenté quitter la DGA ou les sociétés de la BITD pour des sociétés étrangères qui offrent des salaires difficilement atteignables dans les services de l'État et des conditions de travail extrêmement souples.

10. Trois enjeux à relever à court terme sur le plan technique

Le ministère des Armées devra relever trois enjeux à court terme sur le plan technique.

a. L'architecture des réseaux et la défense en profondeur

Le premier enjeu a trait à l'architecture des réseaux. Si le ministère des Armées a bâti des forteresses, il souhaite, demain, bâtir des villes. Aujourd'hui, il y a un périmètre de sécurité fort autour de l'ensemble des systèmes d'information du ministère. L'enjeu est d'empêcher que, demain, quelqu'un qui a réussi à pénétrer la forteresse puisse avoir accès à tout ; ce que le COMCYBER appelle « la défense en profondeur », dont l'objectif est d'affiner les accès. Cela implique de mieux sécuriser les accès afin d'empêcher que n'importe quelle personne ait tous les droits d'accès. En fonction, par exemple, de l'identifiant et du lieu de connexion, attribués selon les fonctions occupées au ministère, une personne donnée ne pourra pas avoir accès à l'ensemble des informations qu'elle souhaite, y compris sur la durée, ce qui n'est pas le cas aujourd'hui. Le ministère des Armées souhaite également pouvoir couper tous les accès en un clic si nécessaire, ce qui n'est pas possible aujourd'hui car il faut les couper un à un. Cela impliquera de mettre en œuvre un processus de transition important pour changer l'architecture numérique du ministère, ce qui ne sera pas simple et prendra beaucoup de temps. L'objectif est de faire une partie de la transition sur la période de la loi de programmation militaire pour les années 2024 à 2030, car le ministère des Armées estime que la manœuvre ne sera pas achevée avant 2031.

La DIRISI contribue d'ores et déjà à la défense en profondeur, qui permet de s'assurer que si l'une des mesures de sécurité est compromise ou défaillante, d'autres assurent la protection des informations sensibles ou classifiées. En particulier, la DIRISI est en charge du déploiement et de l'exploitation des systèmes d'information mais aussi du transport et du routage de ces informations, ce qui permet précisément cette défense en profondeur. Pour atteindre cet objectif, la DIRISI utilise ses infrastructures maîtrisées, en respectant les règles de sécurité qui leur sont attachées, maîtrise les interconnexions des réseaux locaux, configure de manière adéquate les équipements de réseau actifs et configure les mécanismes de commutation et de routage pour se protéger des attaques.

b. L'hébergement des données en nuage

Le deuxième enjeu a trait à l'hébergement en nuage. Actuellement, le ministère des Armées met en œuvre une stratégie visant à exploiter tout le potentiel des technologies d'hébergement en nuage. Afin de satisfaire les besoins des

systèmes d'information non éligibles à une migration dans des *clouds* externes, le ministère des Armées développe et exploite plusieurs *clouds* privés, selon divers niveaux de sensibilité et de classification (non protégé, diffusion restreinte, secret). Des solutions de stockage de données différenciées en fonction des performances attendues sont déployées ou en cours de construction sur ces divers *clouds*.

Cet enjeu a été entamé mais il faut aujourd'hui faire basculer les systèmes d'information un à un sur des systèmes d'hébergement en nuage. Or, le ministère des Armées ayant 1 500 systèmes d'information en son sein, ce processus prendra du temps. La première manœuvre devrait être achevée d'ici 2027 ou 2028. D'ici 2030, entre 50 et 60 % de l'architecture de réseau du ministère aura basculé sur un système de stockage en nuage, en se concentrant sur les principaux systèmes d'information et sur les informations sensibles.

Cet impératif ne se limite d'ailleurs pas aux données du ministère des Armées. En réalité, il conviendrait de se doter de moyens de sauvegarder les données de l'ensemble des acteurs en lien avec les armées, y compris, donc, des entreprises de la BITD et, plus largement, des OIV et des OSE.

c. L'épée de Damoclès des logiciels en tant que service

Enfin, le troisième et dernier enjeu a trait à l'émergence des logiciels en tant que services (*Software as a Service* (SaaS)), qui constituent une véritable épée de Damoclès qui pèse sur les services de l'État. Il s'agit d'une vraie question pour demain en termes de souveraineté car le modèle émergent est celui de l'achat de droits d'utilisation de logiciels hébergés ailleurs. Cette crainte vaut par exemple pour la solution Office 365 de Microsoft. Si, demain, Office 365 n'est disponible que sous forme de SaaS, le ministère des Armées ne pourra plus l'utiliser. Microsoft a d'ailleurs indiqué que d'ici 2030, voire 2027, il n'y aura plus que des logiciels sous forme de SaaS. Pour le ministère des Armées, compte tenu de ses exigences de sécurité et de souveraineté, cela est inacceptable. Il devra donc trouver une alternative si cela arrivait, mais aujourd'hui, il n'y a pas de vision claire de la cible qu'il doit viser.

V. LE DÉFI PROSPECTIF : PRÉPARER LES ARMÉES AUX RUPTURES TECHNOLOGIQUES DE DEMAIN

1. Une politique de soutien à l'innovation dans le domaine de la cyberdéfense par l'Agence de l'innovation de défense

Le soutien de l'innovation dans le domaine cyber conjugue plusieurs canaux pour bénéficier du dynamisme du domaine civil tout en s'assurant de la disponibilité des solutions spécifiques indispensables au ministère des Armées. Le soutien à l'innovation est ainsi notamment porté par :

1/ des projets de technologie de défense (PTD), dans le cadre du domaine d'innovation « CYBER et NAVWAR », s'appuyant sur le programme 144 « Environnement et prospective de la politique de défense » ;

2/ des projets d'accélération de l'innovation (PAI), notamment pour accélérer le développement de nouveaux produits d'intérêt dual ;

3/ des travaux de recherche (PR) s'appuyant sur le financement de thèses, en particulier dans le cadre de l'Accord général de partenariat (qui regroupe 12 universités, écoles ou centres de recherche), sur le dispositif ASTRID, et sur les travaux en lien avec le CEA dans le cadre du programme 191 « Recherche duale (civile et militaire) » ;

4/ des dispositifs *ad hoc* tels que la Cyberdéfense Factory, qui offre aux PME et *start-ups* un accès aux opérationnels du COMCYBER et aux expertises de pointe détenues par la DGA, ainsi qu'à des données d'intérêt cyber détenues par le ministère ;

5/ et une implication dans la définition des appels à projets, la sélection et le suivi des entreprises innovantes accompagnées par l'État dans le cadre de la stratégie nationale cyber.

Plus précisément, l'action de l'AID permet de préparer le futur et de traiter les enjeux suivants.

a. Préparer les futurs produits de sécurité gouvernementaux

Cet enjeu comprend l'anticipation des futures menaces, l'étude de nouveaux mécanismes ou briques de sécurité et la meilleure sécurisation des systèmes.

Par ailleurs, pour appréhender la cybersécurité au niveau d'un macro-système et la prendre en compte comme une performance opérationnelle, un ensemble de PTD sont réalisés ou planifiés afin d'adresser les principaux systèmes d'armes dans les différents milieux (véhicules terrestres, navires armes, hélicoptères, avions de combat, missiles, satellites, ...). En effet, les enjeux cyber de ces différents milieux n'étant pas similaires, il est nécessaire d'avoir une approche dédiée pour chacun de ceux-ci.

Pour explorer de nouvelles techniques afin de détecter des menaces avancées et outiller la LID, notamment en prenant en compte les ruptures apportées par l'intelligence artificielle, plusieurs projets sont en cours. On peut citer par exemple une thèse sur la détection d'intrusion réseau, basée sur une approche par intelligence artificielle non supervisée de détection d'anomalies dans des graphes d'objets de sécurité, avec un accent mis sur l'exploitabilité des alertes remontées par l'intelligence artificielle. On peut citer également un PAI pour automatiser la détection et l'analyse de malwares avec une technologie innovante de conceptualisation de code à base d'intelligence artificielle. On peut citer enfin un projet de la Cyberdéfense Factory pour le développement d'une solution de

cartographie 3D permettant d'offrir une vision intelligible de l'état général de cybersécurité d'un système.

b. Améliorer la confiance dans le niveau de cybersécurité atteint

Afin d'atteindre cet objectif, des études sont conduites pour explorer de nouvelles approches pour les processus d'ingénierie, d'évaluation de sécurité *hardware* et *software*, d'évaluation de sécurité des produits et systèmes. On peut citer par exemple des thèses afin d'étudier l'apport de l'intelligence artificielle pour l'évaluation des implémentations de fonctions cryptographiques avec attaques par canaux auxiliaires, ou encore un projet d'innovation interne pour développer un moyen compact de détection des émissions électromagnétiques non intentionnelles pouvant faire fuiter des informations sensibles, avec une approche mettant en œuvre des technologies de radio logicielle ainsi que des techniques d'intelligence artificielle pour traiter le signal.

D'autres études sont conduites pour outiller la LIO en apportant des outils d'aide à la rétro-ingénierie et à la recherche de vulnérabilités et explorer l'apport de l'intelligence artificielle.

Enfin, des études sont conduites pour outiller la L2I en identifiant et en soutenant des produits avec des fonctions innovantes via l'intelligence artificielle. Peut être cité par exemple un projet de recherche sur la détection de vidéos hyper-truquées.

L'AID travaille en coordination avec l'ensemble des services de l'État concernés. La coordination avec l'ANSSI et l'interministériel se fait principalement dans le cadre d'une implication dans la sélection et le suivi des entreprises innovantes accompagnées par l'État dans le cadre de la stratégie nationale de cyberdéfense de France 2030. Pour donner un exemple de la complémentarité des dispositifs, le ministère des Armées a lancé en fin 2018 un défi sur l'investigation à distance des cyberattaques, remporte par la société HarfangLab. Ce défi a ensuite donné lieu au financement d'une expérimentation conduite par le CALID du COMCYBER.

2. L'intelligence artificielle générative, porteuse de menaces et d'opportunités pour les armées

Les avancées récentes significatives de l'intelligence artificielle générative sont à la fois une opportunité et une menace dans le domaine cyber. Elles peuvent constituer une opportunité notamment pour la LID (par exemple pour l'analyse et la caractérisation de malwares ou la détection de scénarios d'attaque) ou la L2I pour aider à détecter des manœuvres informationnelles (par exemple pour l'aide à la formulation de contre-arguments face à une campagne de désinformation). II y a aussi des opportunités classifiées pour la LIO. Un enjeu important, en cas d'utilisation d'IA générative pour la sécurité, est de s'assurer que les données

utilisées pour l'apprentissage n'ont pas été empoisonnées, s'assurer de la robustesse de l'IA et s'assurer de la qualité des défenses de l'IA.

Elle peut également constituer une menace dans le sens où elle apporte une capacité décuplée à l'attaquant, notamment dans les domaines de la LIO et de la L2I. Elle peut aider les outils existants à devenir plus rapides et plus sophistiqués. Elle peut par exemple aider un attaquant à générer des courriels pour du *phishing*, usurper une identité ou encore faire de la simulation de vie. L'intelligence artificielle offre ainsi le potentiel de simplifier la complexité à créer une attaque, donnant la capacité à des personnes moins expérimentées d'en créer, d'automatiser des attaques, de générer des fausses informations (images, audio, vidéo) ou encore de faciliter des attaques informationnelles massives.

Si les menaces de l'intelligence artificielle générative et des technologies quantiques ne sont pas comparables, on peut néanmoins souligner que les grandes avancées récentes sur l'IA générative en font une technologie beaucoup plus mature que les technologies quantiques.

3. L'irruption des technologies quantiques fait peser un risque réel sur la robustesse des protocoles actuels de chiffrement

La DGA pilote la feuille de route du ministère des Armées sur les technologies quantiques. Plus précisément, la DGA anticipe l'émergence des technologies quantiques en :

1/ finançant des projets de recherche et technologie (R&T) sur les technologies quantiques ;

2/ évaluant la menace que ces technologies prévisibles ou probables feront porter sur les systèmes du ministère des Armées ;

3/ et en développant ses compétences techniques et scientifiques sur les technologies quantiques.

Dans le cas particulier du chiffrement souverain, l'existence ininterrompue de travaux sur les chiffreurs souverains permet à la DGA de disposer d'équipes reconnues dans le domaine de la crypto-mathématique. Les équipes concernées étudient l'état de l'art des attaques quantiques sur les algorithmes de chiffrement et intègrent ces connaissances dans la spécification des algorithmes utilisés dans les chiffreurs souverains.

D'un point de vue algorithmique, des travaux ont été entrepris au niveau international pour remplacer les algorithmes menacés par des algorithmes résistants au quantique (algorithmes dits post-quantiques). En particulier, le NIST (organisme américain de standardisation) a lancé un premier appel à projet en 2017. Toutefois, des travaux parallèles ont été entrepris dès le lancement de la procédure américaine en 2017.

Des choix, inspirés de ceux du NIST, mais en tenant compte des spécificités des armées, ont été effectués. Les premiers algorithmes ont été spécifiés et sont en évaluation à l'ANSSI. Ils répondent à l'essentiel des besoins et seront complétés par d'autres algorithmes, en cours de développement, pour couvrir l'intégralité du périmètre de la cryptographie.

S'agissant toutefois de l'ordinateur quantique, les rapporteurs n'ont pas pu obtenir de détails quant aux coûts, moyens et délais nécessaires pour son élaboration. Ils estiment donc nécessaire de procéder à une évaluation technique en la matière, afin de déterminer la capacité de la France à s'en doter en propre ou s'il y a nécessité d'un partenariat européen pour y arriver.

4. Se préparer à l'émergence de la 6G

Le déploiement de la 5G et, demain, de la 6G, présente un intérêt pour la défense, avec un double objectif de tirer profit, pour les systèmes militaires, des investissements dans les technologies à usage civil, et d'élargir l'offre de service en complément des systèmes militaires résilients actuels.

La réalisation de ces objectifs passe par l'examen des cas d'usages opérationnels militaires de la 5G pour permettre d'identifier les captations d'opportunité de technologies pour les programmes d'armement ou les intégrations dans les systèmes de communication des armées (hybridation de moyens militaires et civils).

La DGA participe directement à la stratégie nationale d'accélération de la 5G de France 2030 en étant membre des comités d'orientation et de sélection des projets qui sont soumis par les industriels en vue de disposer de solutions 5G souveraines et matures à un horizon de 2 à 3 ans. La montée en puissance de la 5G puis de la 6G s'accompagne d'une augmentation des bandes de fréquences utilisées pour ces technologies pouvant impacter celles utilisés dans les télécommunications du ministère des Armées. Dans ce cadre, la DGA apporte son expertise en support de la DGNUM et de l'Agence nationale des fréquences (ANFR) pour les travaux liés aux conférences mondiales des radiocommunications (CMR).

Du côté de la DGNUM, le déploiement de la 5G sur des réseaux d'opérateurs, ou dans le cadre de réseaux privés industriels, pose les mêmes problèmes de coexistence, principalement spectrale, avec les systèmes opérés par le ministère des Armées, que ceux précédemment rencontrés pour permettre le déploiement des générations antérieures (2G, 3G, 4G). En effet, ces technologies, dans les bandes de fréquences qu'elles utilisent, ne permettent pas la coexistence avec d'autres usages du spectre radioélectrique, notamment ceux intéressant la défense (radars, liaisons de données, satellite), sauf à assurer des distances de séparation très importantes (jusqu'à plusieurs centaines de kilomètres). La 5G peut également sévèrement affecter les usages dans les bandes adjacentes si la réglementation 5G n'inclut pas des dispositions contraignantes (cas des radioaltimètres, par exemple).

Ces enjeux de préservation de l'accès au spectre des équipements actuels et futurs des armées, qui conditionnent *in fine* leur capacité à opérer, sont bien identifiés. La DGNUM dispose d'un bureau de la gouvernance des fréquences, coiffé par un officier général en charge de ce domaine qui est le représentant du ministère des Armées au conseil d'administration de l'ANFR. La DGNUM agit, en étroite coordination avec l'ANFR, au niveau de la réglementation internationale dans les instances mondiales (dans le cadre de l'UIT : Union Internationale des Télécommunications) ou au niveau de l'organisation régionale d'appartenance de la France sur laquelle l'UIT s'appuie pour conduire ces travaux (CEPT : Conférence Européenne des Postes et Télécommunications), ainsi que dans les comités de l'OTAN dédiés aux questions d'utilisation du spectre radioélectriques, qui sont fondamentales pour l'interopérabilité des armées de l'Alliance ou encore, plus rarement, au niveau de la Commission européenne.

Les actions menées consistent notamment à orienter l'identification mondiale des bandes de fréquences pour les usages 5G vers celles les plus aptes à permettre un déploiement avec le minimum de contraintes réciproques et de participer activement au choix des critères techniques réglementaires à mettre en œuvre dans le déploiement de la 5G, protégeant les usages de défense actuels et futurs (dans la mesure de ce qu'il est possible d'anticiper) partout où ils seraient susceptibles d'être activés.

À ces fins, la DGNUM participe régulièrement aux groupes de travail élaborant les réponses aux points d'agenda traitant, entre autres, des sujets relatifs à la 5G et à la 6G de la conférence mondiale des radiocommunications (CMR). La CMR, qui se réunit tous les quatre ans, est chargée de réviser le règlement des radiocommunications, traité international ratifié par la France, pour l'adapter aux évolutions des technologies et des usages des fréquences.

En collaboration avec la DGA, la DGNUM informe et oriente les choix des industriels de l'armement dans l'intégration de la technologie 5G et la prise en compte des contraintes afférentes dans les programmes et opérations d'armement. En support de l'AID, la DGNUM apporte son expertise dans l'évaluation et le suivi des projets qui lui sont soumis.

VI. LE DÉFI DE LA TRANSPARENCE : MIEUX ASSOCIER LE PARLEMENT AU SUIVI DE LA POLITIQUE DE CYBERDÉFENSE

Enfin, le dernier défi est celui de la transparence. Ce défi est avant tout le résultat de l'expérience des rapporteurs dans le cadre de leur mission. Le sujet de la cyberdéfense, et singulièrement dans les domaines offensif et informationnel, est d'une sensibilité particulière. Les rapporteurs ont pu le mesurer lors de leurs auditions, au cours desquelles les questions relatives à la LIO et à la L2I se sont très vite heurtées à une absence de réponse compte tenu du fait que les informations relatives à ces deux domaines de lutte informatique sont classifiées et revêtent une sensibilité forte.

Cette précaution peut s'entendre. Mais il n'en demeure pas moins que l'absence de transparence vis-à-vis des Parlementaires sur les activités des armées et des services de renseignement en matière de LIO / active et de L2I pose question. Si les Parlementaires votent la loi – y compris, donc, les lois de finances –, ils doivent logiquement disposer d'un niveau d'information suffisamment élevé pour pouvoir consentir ou non, de manière éclairée, à l'adoption de dispositions législatives relatives à la politique de cyberdéfense. Or, à l'heure actuelle, ce n'est pas le cas.

Le ministère des Armées a fait un effort de transparence salutaire en 2019 en assumant publiquement de conduire des actions offensives dans le cyberespace. Par ailleurs, si les doctrines de lutte informatique sont classifiées, des éléments publics de doctrine ont été mis à la disposition du grand public, ce qui ne peut qu'être salué. Il n'en demeure pas moins indispensable de franchir une nouvelle étape dans ce domaine, et singulièrement vis-à-vis des Parlementaires, représentants de la Nation.

LISTE DES RECOMMANDATIONS DES RAPPORTEURS

Le défi de la gouvernance : adapter l'organisation de la cyberdéfense de l'État pour une nation cyber résiliente

1/ Repenser la gouvernance selon une approche globale et plus lisible pour renforcer la résilience de la Nation ;

2/ Renforcer les relations entre l'ANSSI et les armées en cas de crise cyber majeure dans le secteur civil ;

3/ Pouvoir faire bénéficier aux entités du secteur civil (collectivités territoriales et leurs établissements publics, établissements de santé et OIV/OSE) des savoir-faire des armées en cas de crise cyber majeure ;

4/ Instaurer l'obligation de diligenter, à intervalles réguliers, des « contrôles techniques » en cybersécurité aux collectivités territoriales et leurs établissements publics ainsi qu'aux établissements de santé, notamment en lien avec le ministère de l'Intérieur et le COMCYBER-MI (ex-COMCyberGEND) et sous la responsabilité des préfets de zones de défense et des préfets de région ;

5/ Poursuivre le mouvement de décentralisation des compétences en matière de cyberdéfense au sein des trois armées ;

6/ Augmenter les effectifs du CERT de l'ANSSI ;

7/ Renforcer l'éducation à la cybersécurité à l'école en vue de diffuser une culture de l'hygiène numérique au sein de la population à même de contribuer à la cyber-résilience de la Nation ;

8/ Élaborer une feuille de route précise pour renforcer la féminisation des agents numériques et cyber de l'État afin d'élargir le vivier de compétences et de talents ouvert au recrutement ;

9/ Élaborer une stratégie spécifique pour renforcer la cybersécurité dans les DROM-COM ;

10/ Encourager les armées à participer davantage aux exercices internationaux et en organiser à destination de nos partenaires ;

11/ Augmenter la formation en préparation opérationnelle par la réalisation d'exercices en conditions réelles (par exemple dans une centrale électrique), tant en interne que dans le cadre de coopérations bilatérales avec des États alliés.

Le défi des ressources humaines : recruter, former et fidéliser

12/ Renforcer les dispositifs de recrutement des agents cyber par la voie de l'apprentissage ;

13/ Décliner la feuille de route relative à la féminisation des agents cyber de l'État pour le ministère des Armées ;

14/ Encourager les parcours croisés au sein des services de l'État pour mieux fidéliser les agents cyber ;

15/ Assurer un suivi du mécanisme prévu à l'article 42 de la LPM 2024-2030 ;

16/ Développer l'offre de formation dans les établissements d'enseignement supérieur, au-delà des grandes écoles ;

17/ Augmenter le nombre de réservistes de cyberdéfense au sein des trois armées.

Le défi juridique : sécuriser les actions de nos armées par le droit

18/ Veiller à la prise en compte des spécificités des actions des armées dans le cyberespace dans le processus d'élaboration des normes ;

19/ Réfléchir aux voies juridiques envisageables pour mieux encadrer le recours aux réseaux sociaux des personnels du ministère des Armées ;

20/ Mieux encadrer le processus d'exportation des biens à double usage dans le domaine cyber, et singulièrement des armes cyber offensives et des logiciels à base d'intelligence artificielle dans le domaine informationnel ;

21/ Procéder à une évaluation juridique pour déterminer notre capacité à répondre par notre corpus juridique national et international actuel au mercenariat dans le domaine de la cyberdéfense.

Le défi capacitaire : doter nos armées de capacités techniques pour faire face aux menaces

22/ Limiter au strict nécessaire le recours aux solutions étrangères dans les systèmes d'armes ;

23/ Élaborer une feuille de route pour réduire l'empreinte des GAFAM au sein du ministère des Armées ;

24/ Explorer la piste d'un recours plus accru aux systèmes d'exploitation et aux logiciels libres ;

25/ Fixer des critères de cybersécurité aux entreprises de la BITD et leurs sous-traitants pour l'obtention de marchés publics ;

26/ Encadrer de manière très stricte les relations entre le ministère des Armées et les entreprises qui vendent des armes cyber offensives ;

27/ Poursuivre la feuille de route relative à la défense en profondeur ;

28/ Accélérer la feuille de route relative à l'hébergement informatique en nuage ;

29/ Élaborer une feuille de route dressant des alternatives aux systèmes d'exploitation et logiciels de type SaaS ;

30/ Se doter de moyens de sauvegarder les données de l'ensemble des acteurs de la BITD, des OIV et des OSE dans des *clouds* souverains.

Le défi prospectif : préparer les armées aux ruptures technologiques de demain

31/ Poursuivre la politique d'investissement dans les technologies quantiques ;

32/ Procéder à une évaluation technique des coûts, moyens et délais nécessaires à la dotation d'un ordinateur quantique, en identifiant la capacité de la France à s'en doter en propre ou s'il y a nécessité d'un partenariat européen pour y arriver ;

33/ Explorer les opportunités offertes par l'intelligence artificielle et élaborer une feuille de route relative aux influences mutuelles entre l'intelligence artificielle et la cyberdéfense.

Le défi de la transparence : mieux associer le Parlement au suivi de la politique de cyberdéfense

34/ Associer davantage le Parlement au suivi de la politique de cyberdéfense des armées en matière de lutte informatique offensive et de lutte informatique d'influence ;

35/ Créer une commission parlementaire chargée du suivi de la politique de cyberdéfense de l'État dont les membres seraient autorisés ès qualités à connaître des informations classifiées relatives à ladite politique.

TRAVAUX DE LA COMMISSION

Au cours de sa séance du mercredi 17 janvier 2024, la commission examine le présent rapport.

M. le président Jean-Pierre Cubertafon. Madame la rapporteure, Monsieur le rapporteur, mes chers collègues, nous sommes réunis ce matin pour entendre les conclusions des rapporteurs de la mission flash sur les défis de la cyberdéfense.

Avant toute chose, je tiens à excuser M. le Président Thomas Gassilloud pour son absence. Il est en effet actuellement en déplacement en Afrique avec nos collègues Benoît Bordat, François Piquemal et Anna Pic.

La commission de la Défense nationale et des forces armées a créé une mission flash sur les défis de la cyberdéfense le 15 mars 2023. Elle en a désigné rapporteurs Mme Anne Le Hénanff et M. Frédéric Mathieu, ici présents.

Dans le cadre de leur mission flash, les rapporteurs ont conduit 25 auditions, à l'occasion desquelles ils ont auditionné des représentants du ministère des Armées mais également de l'ANSSI, du SGDSN, du ministère de l'Intérieur, du ministère de l'Éducation nationale et du ministère de l'Enseignement supérieur et de la Recherche. Ils ont également pu s'entretenir avec des journalistes, des représentants d'ONG ainsi que des représentants d'entreprises de la BITD.

Par ailleurs, les rapporteurs ont effectué trois déplacements sur le territoire national et un déplacement à l'étranger. Sur le territoire national, ils se sont rendus à la DGA-MI, à Bruz, au groupement de la cyberdéfense des armées, à Saint-Jacques-de-la-Lande, à la 807e compagnie de transmissions de l'armée de Terre, à Saint-Jacques-de-la-Lande également, au commandement des systèmes d'information et de la communication de l'armée de Terre, à Cesson-Sévigné, ainsi qu'au Centre Support Cyberdéfense de la Marine nationale, à Brest. Ils se sont également rendus en Finlande et en Estonie.

Je souhaite d'emblée féliciter nos deux rapporteurs pour la très grande qualité de leur travail et pour leur investissement. Il s'agit d'un sujet majeur pour nos armées, consacré d'ailleurs comme tel dans la LPM, le cyberespace étant en effet un des nouveaux champs de conflictualité avec l'espace et les fonds marins. Nous avons hâte d'entendre vos conclusions qui, au regard de votre programme de travail, promettent d'être particulièrement riches et denses. Sans plus attendre, je vous cède la parole.

Mme Anne Le Hénanff, rapporteure. Merci Monsieur le Président, mes chers collègues, je suis très heureuse de vous présenter les conclusions de notre mission flash sur les défis de la cyberdéfense. Mon collègue et moi souhaitons d'emblée remercier le président Thomas Gassilloud de nous avoir confié cette

mission flash, sur un sujet dont nous estimons qu'il est à la fois capital et encore trop peu estimé à sa juste valeur. Je souhaite également remercier mon collègue co-rapporteur Frédéric Mathieu, avec lequel j'ai pris plaisir à travailler. Nos relations de travail ont été excellentes tout le long de la mission, et j'espère qu'il en dira autant !

Avant de rentrer dans le vif du sujet, nous souhaitions d'emblée faire quelques remarques d'ordre méthodologique.

Dans le cadre de notre mission flash, nous nous sommes intéressés aux défis de la « cyberdéfense ». Cette notion a été entendue au sens des trois doctrines de lutte informatique du ministère des Armées que sont la lutte informatique défensive, dite LID, la lutte informatique offensive, la LIO et la lutte informatique d'influence, L2I.

Nous avons également inclus dans le périmètre de notre mission flash la cybersécurité, la cyberprotection et, surtout, la cyber-résilience ; notion qui nous est particulièrement chère.

En tant que membres de la commission de la Défense, nous avons bien entendu orienté nos travaux avec un prisme « défense », toutefois, convaincus que nous sommes de la nécessité d'appréhender cette question au-delà du seul périmètre du ministère des Armées, nous avons également fait le choix de nous intéresser à cette question à l'échelle interministérielle, et en l'occurrence, à l'échelle du SGDSN, autorité de tutelle de l'ANSSI.

Comme l'a indiqué le président, nous avons conduit 25 auditions, à l'occasion desquelles nous nous sommes entretenus avec des représentants des états-majors, directions et services du ministère des Armées bien sûr, mais également avec des représentants de l'ANSSI, du SGDSN et du ministère de l'Intérieur. En vertu de cette approche globale, nous avons choisi d'élargir notre prisme d'analyse en auditionnant des représentants du ministère de l'Éducation nationale et du ministère de l'Enseignement supérieur et de la Recherche. Nous nous sommes également entretenus avec des journalistes, avec des représentants d'ONG, et, bien sûr, des représentants d'entreprises de la BITD.

En complément des auditions conduites à l'Assemblée nationale, nous avons effectué trois déplacements sur le territoire national et un déplacement à l'étranger. Nous étions en effet convaincus qu'il était absolument indispensable de nous rendre sur le terrain pour appréhender la cyberdéfense de manière concrète, opérationnelle, au plus près des acteurs concernés. Sur le territoire national, nous nous sommes rendus à la DGA-MI, à Bruz, au groupement de la cyberdéfense des armées du COMCYBER et à la 807e compagnie de transmissions de l'armée de Terre, à Saint-Jacques-de-la-Lande, au commandement des systèmes d'information et de la communication de l'armée de Terre, à Cesson-Sévigné, ainsi qu'au Centre Support Cyberdéfense de la Marine nationale, à Brest.

Nous avons également souhaité nous rendre à l'étranger pour nous enquérir de la manière dont la cyberdéfense est appréhendée par d'autres États. Nous nous sommes ainsi rendus en Finlande et en Estonie, deux États particulièrement avancés dans les domaines de la cyber-résilience et de la cyberdéfense, qui peut s'expliquer par leur situation géographique et le contexte géopolitique, je pense notamment à la guerre en Ukraine.

Fruit de ces travaux qui, comme vous pouvez vous en douter, ont été particulièrement denses, nous formulons 35 recommandations, regroupées en 6 défis que nous nous attellerons à vous présenter dans le cadre de ce propos introductif. Ces recommandations sont évidemment le résultat des échanges nourris que nous avons pu avoir avec l'ensemble de nos interlocuteurs mais ils ont également le fruit de nos propres expériences. En ce qui me concerne, de par mon expérience d'élue locale à Vannes en charge du numérique depuis de nombreuses années, j'ai toujours gardé à l'esprit l'importance de ce sujet pour nos territoires.

Nous tenons à remercier l'ensemble des personnes que nous avons rencontrées lors de nos travaux. Les échanges que nous avons eus, les réflexions qu'ils ont partagées, leur investissement pour nous accueillir lors de nos déplacements et leur disponibilité nous ont permis de vous présenter aujourd'hui nos conclusions. Merci à eux pour le temps qu'ils nous ont consacrés.

M. Frédéric Mathieu, rapporteur. Je souhaite, en préambule, remercier également ma collègue Anne Le Hénanff pour la qualité de notre coopération et le travail fourni. Ce fut un vrai plaisir de travailler à vos côtés, chère collègue. Je m'associe pleinement aux remerciements formulés vis-à-vis des personnes avec lesquelles nous avons travaillé.

Avant de vous présenter les défis de la cyberdéfense que nous avons identifiés et les recommandations associées, permettez-nous de vous présenter brièvement l'écosystème de cyberdéfense ; prérequis indispensable à la bonne compréhension de nos conclusions.

Le cyberespace se structure en trois couches indissociables, d'où procèdent toutes les menaces :

1/ une couche physique, constituée des équipements, des systèmes informatiques et de leurs réseaux ayant une existence matérielle (et donc une territorialité qui ouvre sur un droit national, voire international) ;

2/ une couche logique, constituée de l'ensemble des données numériques, des logiciels, des processus et outils de traitement, de gestion et d'administration de ces données, ainsi que de leurs flux d'échanges, implantés dans les matériels pour leur permettre de rendre les services attendus ;

3/ et une couche cognitive, également appelée couche informationnelle, constituée des informations et des interactions sociales de toutes sortes qui se

trouvent dans le cyberespace et des personnes qui peuvent déclarer plusieurs identités numériques.

Au-delà de la notion de « défendabilité » des systèmes, la cyberdéfense au sein du ministère des Armées est déclinée en cohérence avec les six missions définies par la revue stratégique de cyberdéfense publiée en février 2018 :

1/ prévenir : il s'agit de faire prendre conscience aux utilisateurs du risque représenté par la numérisation des organisations ou des équipements qu'ils servent ;

2/ anticiper : il s'agit d'évaluer en permanence les probabilités de cyberattaques et prendre des mesures préventives lorsque la menace paraît suffisamment forte. Cette mission incombe à l'Agence nationale de sécurité des systèmes d'information (ANSSI), en coordination avec les services de renseignement et le Commandement de la cyberdéfense (COMCYBER) sur le périmètre du ministère des Armées ;

3/ protéger : il s'agit de diminuer la vulnérabilité de nos systèmes informatiques, à la fois en compliquant la tâche des attaquants potentiels et en facilitant la détection des cyberattaques ;

4/ détecter : il s'agit de rechercher des indices d'une éventuelle cyberattaque en cours. Cette mission relève de la responsabilité du COMCYBER et des unités subordonnées au ministre des Armées. Pour compléter ses informations, il sollicite ses partenaires nationaux et internationaux ;

5/ réagir : il s'agit de résister à une cyberattaque afin qu'elle n'empêche pas la poursuite de notre activité. Dans la plupart des cas, le COMCYBER déclenche alors une opération de lutte informatique défensive, en liaison avec l'ANSSI. Elle peut entraîner l'emploi de moyens qui sortent du domaine de la cyberdéfense, voire du ministère des Armées (par exemple, la saisie de la justice, une action diplomatique ou une mesure de rétorsion économique) ;

6/ attribuer : il s'agit de préciser l'auteur d'une cyberattaque par des preuves ou un faisceau d'indices. Les services de renseignement sont au cœur de ce processus de recueil d'indices d'attribution ; la décision d'attribution appartenant, *in fine*, aux plus hauts responsables politiques.

Ainsi, les actions de prévention et de protection concernent les systèmes informatiques du ministère des Armées, tandis que les missions d'anticipation, de détection et de réaction s'intéressent aux systèmes informatiques appartenant aux autres catégories d'acteurs.

Mme Anne Le Hénanff, rapporteure. Par ailleurs, les opérations dans le cyberespace reposent sur trois doctrines : la lutte informatique défensive (LID), qui regroupe l'ensemble des actions, techniques ou non, conduites pour faire face à un risque, une menace ou à une cyberattaque réelle ; la lutte informatique offensive (LIO), qui regroupe l'ensemble des actions entreprises dans le cyberespace,

conduites de façon autonome ou en combinaison des moyens militaires conventionnels, pour produire des effets à l'encontre d'un système adverse afin d'en altérer la disponibilité ou la confidentialité des données et la lutte informatique d'influence (L2I), qui désigne les opérations militaires conduites de façon autonome ou en combinaison avec d'autres opérations dans la couche informationnelle du cyberespace afin de détecter, caractériser et contrer les attaques, appuyer la communication stratégique, renseigner ou faire de la déception.

Le cyberespace constitue donc désormais un espace de manœuvre et de confrontation à part entière, au même titre que les milieux terrestres, maritime, aérien, et extra-atmosphérique. Le cyberespace est un milieu transverse dont les activités sont nécessairement en interaction avec les milieux conventionnels : terre, mer, air, espace, notamment en matière de champs électromagnétique et informationnel.

L'action dans ou depuis le cyberespace peut ainsi produire des effets dans l'ensemble des milieux et des champs. Par exemple, une attaque cyber peut faire dévier de sa route un satellite. Réciproquement, une action dans ces milieux et champs peut produire des effets dans le cyberespace, comme la destruction physique d'un serveur.

Dans ce contexte, le cyberespace a acquis une valeur stratégique permettant de garantir la liberté d'action des forces dans les autres milieux et champs. Or, la menace est multiforme, permanente, non territorialisée et peut avoir des conséquences à tous les niveaux tactiques, à l'avant comme à l'arrière. Ce milieu doit par conséquent être pris en compte dans la manœuvre pour se protéger et pour saisir les opportunités d'agir. Surtout, il doit être pris en compte dès la phase de compétition du *continuum* « compétition-contestation-affrontement », au quartier comme en mission.

En outre, il existe des spécificités de milieu évidentes dans l'exploitation du volet cyber par les trois armées. Un sous-marin n'est pas soumis à la même menace cyber qu'un PC de division installé en zone industrielle d'une ville ou qu'un avion militaire posé sur une base aérienne de théâtre. De même, l'environnement numérique adverse d'une force navale, terrestre ou aérienne est intimement lié à son milieu.

Les trois volets de la politique de cyberdéfense du ministère des Armées (LID, LIO et L2I) permettent aux trois armées de prendre en compte ces dimensions (se protéger, se défendre et agir) de manière adaptée et complémentaire grâce à une organisation assurant la cohérence d'ensemble du modèle cyber du ministère tout en respectant les spécificités des armées.

Mais si les doctrines sont une référence, elles ne constituent pas un carcan. Elles définissent les principes et les responsabilités et doivent s'adapter à l'emploi. Dans un domaine aussi jeune que les opérations dans le cyberespace, il est pertinent qu'elles soient revues régulièrement avec l'ensemble de la communauté cyber mais

aussi plus largement la communauté militaire des opérations car tout évolue très rapidement. L'apparition dans le champ doctrinal du concept des opérations multi milieux multi champs dans le concept d'emploi des forces de 2021 traduit d'ailleurs bien cet état de fait.

M. Frédéric Mathieu, rapporteur. Le schéma qui s'affiche derrière nous vous présente une version simplifiée de l'écosystème de la cyberdéfense à l'échelle de l'État.

S'agissant des acteurs de la cyberdéfense au sein du ministère des Armées, l'acteur central est le commandement de la cyberdéfense (COMCYBER). Placé sous l'autorité directe du CEMA, le COMCYBER est un commandement opérationnel qui rassemble l'ensemble des forces de cyberdéfense sous une autorité interarmées déployé sur plusieurs emprises à Paris et à Rennes. Le COMCYBER effectue ses missions par délégation de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), qui est responsable de la cyberdéfense et de la cybersécurité des administrations publiques, des entreprises et, singulièrement, des opérateurs d'importance vitale (OIV) et des opérateurs de services essentiels (OSE).

Créé en mai 2017, le COMCYBER est en charge de la conception, de la planification et de la conduite des opérations de cyberdéfense, ainsi que de la défense des systèmes d'information des armées, directions et services du ministère des Armées (à l'exception de ceux de la DGSE et de la DRSD) ; de la stratégie de cyberdéfense par la coordination des contributions des armées et organismes interarmées à la politique nationale et internationale de cyberdéfense et par la mise en cohérence du modèle de cyberdéfense du ministère des Armées ; de la dimension capacitaire de la politique de cyberdéfense par l'élaboration de la politique des ressources humaines de cyberdéfense, par la coordination de la définition des besoins techniques spécifiques à la cyberdéfense et par la gestion de la réserve de cyberdéfense.

Autre acteur de la cyberdéfense au sein du ministère des Armées, la DGA constitue l'expert technique référent du ministère des Armées.

De manière générale, la DGA est responsable de la conception et de la réalisation des systèmes permettant de garantir aux forces, dans la durée, la résilience cyber des capacités qu'elles opèrent, et d'acquérir et de conserver leur liberté d'appréciation et d'action dans le cyberespace.

Cette mission se décline selon quatre axes :

1/ porter à un niveau adapté au niveau de la menace la cybersécurité des systèmes numériques et des systèmes d'armes afin d'être résilient face aux agressions cyber ;

2/ équiper nos forces armées de systèmes leur permettant d'acquérir et de conserver leur liberté d'appréciation et d'action dans le cyberespace, c'est-à-dire de conduire des actions dans les trois domaines de lutte informatique ;

3/ orienter, maintenir et développer les capacités technologiques et industrielles nécessaires, en cohérence avec la stratégie nationale de cyberdéfense ;

4/ accroître la cybersécurité de la BITD et contribuer à la cyberdéfense de la Nation.

Enfin, le troisième acteur principal du ministère des Armées dans le domaine de la cyberdéfense est la DGSE. Elle participe à la protection des intérêts fondamentaux de la France par des actions de renseignement ainsi qu'à la compréhension et à la réduction de la menace cyber (criminelle ou d'État).

Au titre de cette mission, la DGSE est membre du centre de coordination des crises cyber (C4), qui regroupe l'ANSSI, la DGA, le COMCYBER et la DGSI, et partage ses renseignements au sein de cette comitologie interministérielle. Sur le territoire national, sur autorisation du Premier ministre après avis de la CNCTR, la DGSE met en œuvre toutes les techniques de recueil du renseignement autorisées par le code de la sécurité intérieure, selon le principe de proportionnalité. À l'étranger, la DGSE utilise tous types de techniques de recueil du renseignement dont elle dispose.

Par anticipation sur une action hostile pouvant toucher la France, le renseignement sur la menace cyber cherche à informer sur les acteurs, étatiques ou criminels, connus pour nourrir des projets agressifs dans l'espace numérique ainsi que sur les outils et les services commercialisés pour mettre en œuvre ces projets. En complément, par réaction à une action hostile ayant touché la France, le renseignement sur la menace aura pour mission d'identifier l'auteur de l'action et son donneur d'ordre.

Mme Anne Le Hénanff, rapporteure. D'autres acteurs au sein du ministère des Armées jouent un rôle prépondérant en matière de cyberdéfense : la DIRISI, la DRSD, la DPID ou encore la DGNUM sont autant d'entités qui participent, directement ou indirectement, aux capacités de cyberdéfense du ministère. Les trois armées sont évidemment également parties prenantes de la cyberdéfense du ministère des Armées, selon des modalités en cours d'évolution, mais nous y reviendrons.

Au-delà du ministère des Armées, l'ANSSI est l'acteur principal de la cyberdéfense au sein de l'État. Créée en 2009 et rattachée au Secrétariat général de la défense et de la sécurité nationale (SGDSN), la principale mission de l'ANSSI est d'assurer la sécurité des systèmes d'information de l'État et de veiller à celle des administrations, des opérateurs d'importance vitale (OIV) et des opérateurs de services essentiels (OSE), auprès desquels elle exerce par ailleurs une mission de conseil et de soutien.

De son côté, la DGSI, membre du premier cercle des services de renseignement, est la seule entité qui peut exercer sa mission de cyberdéfense sur le territoire national aussi bien dans un cadre judiciaire que de renseignement. Lorsqu'une cyberattaque menace les intérêts fondamentaux de la Nation, la DGSI,

agissant au titre de ses missions de contre-ingérence, de contre-espionnage et de contre-terrorisme, peut mettre en œuvre des techniques de recueil du renseignement dans le cadre de ses investigations.

Plus spécifiquement, la DGSI suit les modes opératoires de nos attaquants cyber susceptibles de porter atteinte aux intérêts fondamentaux de la Nation et agit, de manière proactive ou réactive, pour contrer ces menaces.

Après cette présentation des concepts, de la doctrine et des acteurs de la cyberdéfense, venons-en aux défis que nous avons identifiés et que le ministère des Armées, et plus largement, l'ensemble des services de l'État, devra relever pour doter la France d'une puissance cyber de tout premier rang. Ces défis sont au nombre de six : premièrement, le défi de la gouvernance ; deuxièmement, le défi des ressources humaines ; troisième défi : le défi juridique ; quatrième défi : le capacitaire ; le cinquième défi concerne la prospective et enfin le défi de la transparence.

Le premier défi est le défi de la gouvernance. À l'issue de nos travaux, nous avons acquis la conviction que la politique de cyberdéfense de l'État gagnerait à être plus lisible et devrait être appréhendée de manière globale pour renforcer la cyber-résilience de la Nation. Nous avons en effet la conviction que la culture de la cybersécurité ne peut pas se décréter depuis un sommet… et diffuser au sein de la société sans cette approche globale. Cela impliquera notamment de renforcer les relations entre l'ANSSI et les armées, en cas de crise cyber majeure dans le secteur civil. Ce rapprochement est en cours, avec la perspective des Jeux olympiques et paralympiques de 2024, mais il devra encore être renforcé pour faire face aux défis de demain. Au demeurant, au-delà de la seule ANSSI, c'est bien l'ensemble des entités du secteur civil (collectivités territoriales et leurs établissements publics, établissements de santé, mais également opérateurs d'importance vitale et opérateurs de services essentiels) qui devraient pouvoir bénéficier des savoir-faire des armées en cas de crise cyber majeure.

Ce rapprochement est d'autant plus pertinent de notre point de vue que les effectifs de l'ANSSI sont limités, et singulièrement ceux de son centre de veille et d'alerte, et que la charge de travail qui pèsera sur elle ne fera qu'augmenter avec la directive NIS 2. Le recours par l'ANSSI à des prestataires privés de réponse aux incidents de sécurité est d'ailleurs la preuve qu'elle ne peut répondre seule à l'ensemble des cyberattaques qui frappent notre pays, cyberattaques qui ne vont cesser de se multiplier. Nous sommes d'ailleurs favorables à une augmentation des effectifs de ce centre d'alerte et de veille de l'ANSSI.

M. Frédéric Mathieu, rapporteur. De leur côté, les armées sont en train d'acquérir des compétences nouvelles en matière de cyberdéfense grâce à la mise en place de la communauté cyber des armées. Annoncée en filigrane lors des débats sur la LPM, la création d'une « communauté cyber des armées » a été officialisée en novembre 2023. En effet, au-delà des moyens financiers et humains, le COMCYBER indiquait en avril 2023 devant notre commission qu'un effort

particulier serait fait pour adapter les modalités et les niveaux d'action de la cyberdéfense. Si certaines actions peuvent être conduites de loin dans le cyberespace, d'autres nécessitent d'être à proximité des cibles. Cette diffusion de la cyberdéfense au sein des trois armées, au plus près des bases et des régiments, contribuera sans doute au renforcement de la cyber-résilience du ministère et, plus globalement, de la Nation.

S'agissant plus spécifiquement des collectivités territoriales, de leurs établissements publics et des établissements de santé, nous estimons qu'il est temps de franchir un nouveau cap en matière de cybersécurité. Les trop nombreux exemples de cyberattaques ayant frappé des collectivités territoriales et des établissements de santé prouvent qu'il est désormais urgent de rehausser le niveau d'ambition en la matière. Concrètement, nous estimons qu'il faut instaurer l'obligation de diligenter, à intervalles réguliers, des « contrôles techniques » en cybersécurité, notamment en lien avec le ministère de l'Intérieur et le commandement du ministère de l'Intérieur dans le cyberespace – nouveau nom du commandement de la Gendarmerie dans le cyberespace – sous la responsabilité des préfets des zones de défense et des préfets de région. Nous avons pu apprécier concrètement les compétences et les savoir-faire des gendarmes en matière de cyberdéfense. Nous savons ce qu'ils peuvent apporter à ces entités et, ce faisant, contribuer à la cyber-résilience de la Nation.

Mme Anne Le Hénanff, rapporteure. Mais la cyber-résilience de la Nation impliquera également de renforcer l'éducation à la cybersécurité à l'école en vue de diffuser une culture de l'hygiène numérique au sein de la population. De ce point de vue, l'école a un rôle primordial à jouer. En formant les jeunes au risque cyber dès l'école, un très grand nombre de cyberattaques pourraient être évitées. Il n'est en effet plus à démontrer que la sensibilisation accompagnée de l'adoption de réflexes simples avant, pendant et après une attaque de nature cyber permet d'en limiter les impacts, voire d'éviter celle-ci. Le ministère de l'Éducation nationale devra donc prendre toute sa part à cet effort global de la Nation.

En outre, renforcer la cyber-résilience de la Nation impliquera de féminiser les recrutements des agents numériques et cyber de l'État afin d'élargir le vivier de compétences et de talents ouvert au recrutement. Cela vaut évidemment pour les services de l'État mais également dès l'école secondaire, en luttant efficacement contre les stéréotypes de genre et en incitant les jeunes filles à s'engager dans cette voie professionnelle.

M. Frédéric Mathieu, rapporteur. Par ailleurs, afin d'améliorer le niveau de cyber-résilience de la Nation, la participation à des exercices est indispensable. Dans le cadre de nos travaux, nous avons été alertés sur la faible participation des armées et des services de l'État aux exercices cyber organisés à l'échelle internationale. Nous n'avons par ailleurs pas eu connaissance d'exercices cyber organisés par la France et en France à destination de nos partenaires. Nous estimons pourtant cela indispensable. D'ailleurs, s'agissant de la nature de ces exercices, nous avons acquis la conviction qu'il était nécessaire d'organiser des exercices en

conditions réelles, à la fois à l'échelle interministérielle mais également avec des États alliés dans le cadre de coopérations bilatérales. Nous pensons d'ailleurs que cela permettait de renforcer utilement le lien armées – Nation et que les populations seraient d'autant plus sensibilisées face au risque cyber si les conséquences d'une cyberattaque – par exemple l'arrêt d'une centrale électrique pendant quelques heures – sont ressenties *in concreto* par les populations dans le cadre de ces exercices.

Enfin, lorsque nous appelons de nos vœux un renforcement de la cyber-résilience de la Nation, nous pensons évidemment à l'ensemble du territoire national, et y compris, donc, les territoires ultra-marins. De ce point de vue, nous pensons qu'il est impératif d'élaborer une stratégie spécifique pour renforcer la cybersécurité dans les DROM-COM, qui sont particulièrement vulnérables face au risque de cyberattaques.

Mme Anne Le Hénanff, rapporteure. Venons-en désormais au deuxième défi : le défi des ressources humaines. Les difficultés de recrutement et de fidélisation du ministère des Armées dans le domaine de la cyberdéfense sont connues. Toutefois, le ministère des Armées possède de nombreux atouts pour attirer les talents et plusieurs pistes permettraient de mieux recruter, former et fidéliser les agents cyber du ministère.

Tout d'abord, même si cela peut paraître évident, il convient de rappeler que le ministère des Armées est en concurrence avec les secteurs publics et privés dans le cadre du recrutement des talents cyber. De ce fait, les difficultés de recrutement du ministère ne lui sont pas exclusivement imputables. Il est notamment tributaire du manque d'offre de formations dans les établissements d'enseignement supérieur, même si on note ces dernières années un développement accru de ces offres et une ouverture à un panel plus large d'étudiants. J'en veux pour preuve la création par le COMCYBER d'un parcours universitaire entre l'École Polytechnique et l'EPITA dédié à la cyberdéfense. Toutefois, au-delà des seules grandes écoles, il est absolument indispensable que l'offre de formation en matière de cybersécurité et de cyberdéfense soit étendue. Cette mission incombera en premier lieu au ministère de l'Enseignement supérieur et de la Recherche.

Par ailleurs, les études démontrent que le recours à l'apprentissage est un moyen très efficace pour recruter et fidéliser les agents cyber. Le ministère des Armées est pleinement engagé dans cette voie avec la création d'un BTS à Saint-Cyr l'École et au lycée Naval à Brest. Cette politique doit être renforcée.

Une seconde piste pour améliorer le recrutement et la fidélisation est celle relative au développement des parcours croisés au sein des services de l'État. Si le critère de la rémunération est souvent mis en avant pour justifier les difficultés de recrutement et de fidélisation, l'absence de visibilité sur la carrière joue également. Aujourd'hui, ces parcours croisés restent encore trop peu développés et la concurrence entre les services reste de mise. Ces derniers peuvent également s'effectuer sous la forme d'aller et retour entre les armées et le secteur privé, dans

le respect des règles déontologiques qui encadrent ces départs et de l'article 42 de la loi de programmation militaire qui a mis en place un mécanisme pour lutter contre les ingérences étrangères dans le cadre de recrutements.

M. Frédéric Mathieu, rapporteur. En outre, la feuille de route relative à la féminisation des agents cyber de l'État que nous appelons de nos vœux gagnerait à être déclinée au sein du ministère des Armées. Celui-ci prend d'ores et déjà des initiatives dans le cadre du plan relatif à l'égalité professionnelle entre les femmes et les hommes, qui doivent être poursuivies.

Les agents cyber comprennent également les réservistes de cyberdéfense, qui peuvent jouer un rôle fondamental à la fois pour le ministère des Armées mais aussi pour la cyber-résilience de la Nation dont ils pourraient être de véritables ambassadeurs. Dans le plan réserve 2035, la trajectoire est fixée à 500 réservistes de cyberdéfense. Le ministère des Armées indique qu'elle sera consolidée en fonction des besoins et, si elle est soutenue, par la création de postes permanents dédiés à l'animation ou à la formation. Cette trajectoire nous semble insuffisante pour irriguer l'ensemble des armées. Nous estimons donc qu'il est indispensable de recruter davantage de réservistes cyber.

Venons-en désormais au troisième défi : le défi juridique. Même si cela est peu connu, la cyberdéfense comprend une dimension juridique relativement forte, en particulier s'agissant du cadre juridique des opérations militaires dans le cyberespace. Nous avons identifié quatre enjeux dans ce domaine.

Le premier enjeu a trait à la prise en compte des spécificités des armées dans le cyberespace dans le processus d'élaboration des normes. Il s'agit là d'un impératif absolu, notamment à l'échelle européenne, qui doit être pleinement pris en considération.

Le deuxième enjeu a trait au recours par les agents du ministère des Armées aux réseaux sociaux. Nous ne nous étendrons pas sur les exemples précis qui ont été portés à notre attention dans le cadre de nos travaux à cet égard. Toutefois, nous sommes en mesure de vous indiquer qu'il s'agit d'un véritable enjeu, et singulièrement parmi les plus jeunes recrues. Sans rentrer dans les détails, nous déplorons qu'une utilisation trop légère des réseaux sociaux ait pu parfois aboutir, involontairement, à une divulgation d'informations protégées par le secret de la défense nationale. Un guide du bon usage des réseaux sociaux a été adopté en 2021 pour les agents du ministère des Armées. Il rappelle le principe de discrétion professionnelle des agents du ministère, militaires comme civils. Une interdiction pure et simple ne serait ni possible, ni souhaitable. En revanche, la conduite d'une réflexion sur les voies juridiques envisageables pour mieux encadrer le recours aux réseaux sociaux, singulièrement en OPEX ou lors des exercices de préparation opérationnelle, nous apparaît souhaitable.

Le troisième enjeu a trait à notre politique d'exportation des biens à double usage dans le domaine cyber, et singulièrement des armes cyber offensives et des

logiciels à base d'intelligence artificielle dans le domaine informationnel. Deux affaires ont défrayé la chronique ces dernières années, s'agissant des logiciels de cyber-espionnage : l'affaire Pegasus et l'affaire Predator. Sans rentrer dans les détails, ces deux affaires montrent qu'il est indispensable de réfléchir à une meilleure régulation des armes cyber offensives et de leurs exportations. S'agissant de la cyberdéfense, la DGA a indiqué que la France n'exporte pas d'autres systèmes que les produits sur étagère proposés par des sociétés duales, dans le cadre du régime de contrôle de l'exportation de biens à double usage d'une part, et les systèmes de cyberprotection et de lutte informatique défensive en tant que constituants d'un système d'armes (aériens ou navals par exemple), dont l'export relève du régime de contrôle des matériels de guerre, d'autre part. Elle a également indiqué que la France n'exporte aucun système ou sous-système cyber offensif.

Enfin, nous estimons nécessaire de procéder à une évaluation juridique afin de déterminer notre capacité à répondre par notre corpus juridique national et international actuel au mercenariat dans le domaine de la cyberdéfense. Nous ne sommes pas convaincus que le droit, et singulièrement le droit international, réponde à l'émergence de cette nouvelle catégorie d'acteurs. Nous ne sommes toutefois pas en mesure d'arrêter clairement notre position, et reconnaissons que le débat est ouvert. La clarification de cette situation nous semble indispensable, eu égard à la multiplication de ces acteurs et à leur potentielle nuisance.

Mme Anne Le Hénanff, rapporteure. Le quatrième défi est le défi capacitaire. Un premier ensemble d'enjeux a trait à notre souveraineté numérique.

Vous n'êtes pas sans ignorer les risques que fait peser le recours à des logiciels étrangers dans nos systèmes d'information et nos systèmes d'armes, et singulièrement eu égard aux règles d'extraterritorialité du droit américain – mais pas que – ou encore des dispositions législatives adoptées par des États comme les États-Unis ou la Chine pour collecter, en toute légalité, nos données. À ce jour, le ministère des Armées n'exclut pas le recours à des solutions étrangères, y compris sur étagère, et ce tant pour ses systèmes d'armes que pour ses systèmes d'information, dès lors qu'elle estime que le risque est maîtrisé. En ce qui nous concerne, nous pensons qu'il est absolument indispensable de limiter au strict nécessaire le recours aux solutions étrangères dans nos systèmes d'armes. La présence de portes dérobées dans des solutions étrangères permettant à l'État fournisseur d'espionner l'État client n'est un secret pour personne. Les mesures prises pour réduire les risques sont salutaires. Mais cela suppose d'être en mesure de détecter les éventuelles portes dérobées installées sur les solutions étrangères. Or, comme nous avons pu l'entendre en audition, si on estime qu'il n'y a pas de cyberattaque, cela peut vouloir dire deux choses : soit il n'y en a effectivement pas, et tout va bien ! soit il y en a une que nous ne détectons pas, et c'est beaucoup plus gênant … !

Nous pensons donc qu'il est nécessaire de limiter autant que possible le recours à des solutions étrangères.

Cette ambition va de pair avec l'élaboration d'une feuille de route pour réduire l'empreinte des GAFAM au sein du ministère des Armées. Nous nous sommes particulièrement intéressés au recours par celui-ci du système d'exploitation Windows. Nous sommes parvenus à la conclusion que le ministère des Armées est aujourd'hui piégé : aucune alternative crédible n'existe à ce système d'exploitation, et le recours aux logiciels libres présente de nombreuses limites, même si l'exploration d'un recours plus accru à Linux nous semble souhaitable.

En outre, compte tenu de l'incapacité actuelle du ministère des Armées à assumer, seul, le maintien en condition de sécurité d'un système d'exploitation alternatif, il est directement tributaire de Microsoft. Ce qui signifie qu'elle est dépendante pour la correction des vulnérabilités informatiques potentiellement exploitées par des acteurs malveillants. Cette dépendance sera d'autant plus grave si, demain, cette entreprise décidait de fournir ses services sur le mode dit de « logiciels en tant que services » (*Software as a Service* (SaaS)).

Ce risque est une véritable épée de Damoclès qui pèse sur la protection des données des services de l'État mais surtout sur notre souveraineté. Cela est dû au fait que le modèle émergent consiste au seul achat de droits d'utilisation de solutions hébergées à l'étranger. D'ailleurs, Microsoft a indiqué que d'ici 2030, voire 2027, il n'y aura plus que des logiciels sous forme de SaaS.

Le ministère des Armées, compte tenu de ses exigences en matière de sécurité et de souveraineté, ne peut accepter cette situation, et aujourd'hui, il est difficile d'estimer l'ampleur des risques…

En outre, la feuille de route du ministère des Armées en matière de défense en profondeur des systèmes d'information doit être poursuivie. Comme entendu en audition, si le ministère a bâti des forteresses, il s'agit désormais de bâtir des villes. Aujourd'hui, il y a un périmètre de sécurité fort autour de l'ensemble des systèmes d'information du ministère.

L'enjeu est d'empêcher que, demain, quelqu'un qui a réussi à pénétrer la forteresse puisse avoir accès à tout. Ce qu'on appelle « la défense en profondeur », dont l'objectif est d'affiner les portes d'entrée. Cela implique de mieux les sécuriser afin d'empêcher que n'importe quelle personne ait tous les droits d'accès. En fonction, par exemple, de l'identifiant et du lieu de connexion, attribués selon les fonctions occupées au ministère, une personne donnée ne pourra pas avoir accès à l'ensemble des informations qu'elle souhaite, y compris sur la durée, ce qui n'est pas le cas aujourd'hui. Pour cela, il faudrait mettre en œuvre un processus de transition important afin de changer l'architecture numérique du ministère, ce qui ne sera a priori pas le cas avant 2031. Ce que nous regrettons…

M. Frédéric Mathieu, rapporteur. Un autre sujet de préoccupation majeur est celui relatif à l'hébergement informatique en nuage. Actuellement, le ministère des Armées met en œuvre une stratégie visant à exploiter tout le potentiel des technologies d'hébergement en nuage. Afin de satisfaire les besoins des systèmes

d'information non éligibles à une migration dans des clouds externes, le ministère des Armées développe et exploite plusieurs clouds privés, selon divers niveaux de sensibilité et de classification (non protégé, diffusion restreinte, secret). Des solutions de stockage de données différenciées en fonction des performances attendues sont déployées ou en cours de construction sur ces divers clouds. Cet enjeu a été entamé mais il faut aujourd'hui faire basculer les systèmes d'information un à un sur des systèmes d'hébergement en nuage. Or, le ministère des Armées comprenant plus de 1 500 systèmes d'information, ce processus prendra du temps et on estime que d'ici 2030, entre 50 et 60 % de l'architecture de réseau du ministère seulement aura basculé sur un système de stockage en nuage. Nous estimons qu'il est nécessaire d'accélérer cette feuille de route relative à la migration vers un hébergement informatique en nuage souverain. Nous insistons sur « souverain ». Cet impératif vaut également pour les entreprises de la BITD, les OIV et les OSE, dont les données sont au moins aussi stratégiques que celles des services du ministère des Armées et au-delà.

D'ailleurs, s'agissant, des entreprises de la BITD, nous estimons qu'il est nécessaire de franchir une nouvelle étape pour renforcer leur cyber-résilience, et singulièrement les entreprises de la chaîne de sous-traitance. Lors de nos auditions, il nous a clairement été indiqué que les entreprises de la BITD sont les cibles régulières des cyberattaquants. Plus encore que les rançongiciels, qui frappent aussi les entreprises de la BITD, ce sont les logiciels de cyber-espionnage qui frappent en premier lieu ces entreprises. Il s'agit là d'un enjeu capital : quel est l'intérêt d'investir des milliards d'euros pour se doter de systèmes d'armes performants à même de donner à nos armées une supériorité opérationnelle sur le terrain si les entreprises qui conçoivent ces systèmes d'armes se font piller leurs savoir-faire ? La DRSD est en charge de la sensibilisation des entreprises de la BITD face à ce risque, et notamment le centre de veille et d'alerte dédié aux entreprises de défense créé récemment. Toutefois, nous estimons qu'il est désormais nécessaire d'aller plus loin. C'est pourquoi nous pensons qu'il faudra fixer des critères de cybersécurité aux entreprises de la BITD et à leurs sous-traitants en contrepartie de l'obtention de marchés publics.

Enfin, nous estimons qu'il faudra à l'avenir encadrer de manière très stricte les relations entre le ministère des Armées et les entreprises qui vendent des armes cyber offensives. S'agissant de ses relations avec les *brokers* de vulnérabilités informatiques, la DGA a indiqué que le niveau de confiance envers ceux-ci est extrêmement faible. Il est en effet quasiment impossible de connaître le cycle de vie d'une vulnérabilité ou d'un code exploitant celle-ci ; par exemple : qui l'a trouvé ? à combien de personne il a été vendu ? est-ce qu'il contient des marquants ? Dans le domaine de la LIO, la stratégie de la DGA est donc aujourd'hui de privilégier le recours à des études réalisées par des entreprises de la BITD. Cette approche permet d'avoir une confiance forte dans les vulnérabilités nécessaires à la réalisation d'armes numériques, car, ce faisant, il n'y a pas de risque d'intoxication et de vente à de multiples acteurs. Nous estimons que cette ligne est la bonne et qu'elle devra être tenue à l'avenir.

Mme Anne Le Hénanff, rapporteure. Le cinquième défi porte sur l'innovation et la prospective. Deux domaines en particulier ont retenu notre attention : les technologies quantiques et l'intelligence artificielle.

S'agissant de l'émergence des technologies quantiques, c'est la DGA qui pilote la feuille de route du ministère des Armées :

1/ en finançant des projets de recherche et technologie (R&T) ;

2/ en évaluant la menace que ces technologies, prévisibles ou probables, feront porter sur les systèmes à l'avenir ;

3/ et en développant ses compétences techniques et scientifiques.

Si l'identification des enjeux et la feuille de route semblent claires, nous nous sommes cependant heurtés à la question spécifique de l'ordinateur quantique. Personne n'a été en mesure de nous indiquer si l'avènement de cette nouvelle technologie était imminent, ni si les budgets pour son développement étaient nécessaires !

C'est pourquoi nous estimons indispensable de procéder à une évaluation des coûts, moyens et délais nécessaires à cette nouvelle technologie, ainsi qu'à une estimation de la capacité de la France à s'en doter en propre ou si nous avons besoin d'un partenariat européen pour y parvenir.

Par ailleurs, nous avons été alertés lors de nos travaux sur l'influence croissante de l'intelligence artificielle, et singulièrement de l'intelligence artificielle générative, dans le domaine de la cyberdéfense. Les avancées récentes significatives sont à la fois une opportunité et une menace dans le domaine cyber. Elles peuvent constituer une opportunité notamment pour la LID, par exemple pour l'analyse et la caractérisation de malwares ou la détection de scénarios d'attaque ou la L2I pour aider à détecter des manœuvres informationnelles (par exemple pour l'aide à la formulation de contre-arguments face à une campagne de désinformation).

Un enjeu important, en cas d'utilisation d'IA générative pour la sécurité, est de s'assurer que les données utilisées pour l'apprentissage n'ont pas été empoisonnées, s'assurer de la robustesse et de la qualité des défenses de l'IA. Mais elle peut également constituer une menace dans le sens où elle apporte une capacité décuplée à l'attaquant, notamment dans les domaines de la LIO et de la L2I. Elle peut par exemple aider un attaquant à générer des courriels pour du *phishing*, usurper une identité ou encore simplifier la création d'une cyberattaque, pourtant complexe, (donnant ainsi la capacité à des personnes moins expérimentées d'en créer), d'automatiser des cyberattaques, de générer des fausses informations ou encore de faciliter des attaques informationnelles massives. Or, tous ces apports et toutes ces menaces sont encore exploratoires, quoique plus tangibles que les technologies quantiques. L'élaboration d'une feuille de route relative aux influences mutuelles entre l'intelligence artificielle générative et la cyberdéfense nous paraît indispensable.

M. Frédéric Mathieu, rapporteur. Enfin, le dernier défi est celui de la transparence. Ce défi est avant tout le résultat de notre expérience dans le cadre de notre mission. Le sujet de la cyberdéfense, et singulièrement dans les domaines offensif et informationnel, est d'une sensibilité particulière. Nous avons pu le mesurer lors de nos auditions, au cours desquelles les questions relatives à la LIO et à la L2I se sont très vite heurtées à une absence de réponse compte tenu du fait que les informations relatives à ces deux domaines de lutte informatique sont classifiées et revêtent une sensibilité forte.

Cette précaution peut s'entendre. Mais il n'en demeure pas moins que le défaut de transparence vis-à-vis des Parlementaires que nous sommes sur les activités des armées et des services de renseignement en matière de LIO et de L2I pose question. Si les Parlementaires votent la loi – y compris, donc, les lois de finances –, ils doivent logiquement disposer d'un niveau d'information suffisamment élevé pour pouvoir consentir ou non, de manière éclairée, à l'adoption de dispositions législatives relatives à la politique de cyberdéfense. Or, à l'heure actuelle, ce n'est pas le cas.

Le ministère des Armées a fait un effort de transparence salutaire en 2019 en assumant publiquement de conduire des actions offensives dans le cyberespace. Par ailleurs, si les doctrines de lutte informatique sont classifiées, des éléments publics de doctrine ont été mis à la disposition du grand public, ce qui ne peut qu'être salué. Il n'en demeure pas moins indispensable de franchir une nouvelle étape dans ce domaine, et singulièrement vis-à-vis des Parlementaires, représentants de la Nation. Nous estimons donc nécessaire d'associer davantage le Parlement au suivi de la politique de cyberdéfense du ministère des Armées en matière de LIO et de L2I, et suggérons, pour ce faire, de créer une commission parlementaire chargée du suivi de la politique de cyberdéfense de l'État dont les membres seraient autorisés ès qualités à connaître des informations classifiées relatives à ladite politique.

Voici, chers collègues, les conclusions de nos travaux. Nous nous tenons désormais à votre disposition pour répondre à toutes vos questions.

L'exposé des rapporteurs a été suivi d'un débat.

M. Mounir Belhamiti (RE). Au nom du groupe Renaissance, je tiens à vous remercier pour la qualité de votre travail et la pertinence de vos recommandations. Ce n'est sûrement pas un hasard que deux Députés originaires de Bretagne soient mobilisés sur le sujet de la cyberdéfense. Le grand ouest est le fer de lance de la cyberdéfense en France, ce qu'on ne peut que saluer, car cela reflète le dynamisme et la mobilisation de nos territoires.

Des défis, il y en a. Ce domaine est en évolution constante et les menaces de plus en plus sophistiquées. J'imagine les difficultés que vous avez dû éprouver tout au long de vos travaux pour suivre les évolutions dans ce domaine. C'est un champ de conflictualité en tant que tel. La France et l'Europe sont confrontés à des

enjeux complexes tels que celui de la coordination des efforts entre les États, le partage efficace des renseignements, la capacité à anticiper et à répondre aux menaces d'origine nationale ou internationale, les lacunes de la collaboration entre les entités publiques et privées, le besoin d'investissement significatif en matière de formation, la question de la régulation des technologies émergentes… autant de défis que vous avez pu dresser. La LPM répond en partie à ce nouveau paradigme car 4 milliards d'euros sont programmés pour la cyberdéfense. Cela s'inscrit dans la démarche d'économie de guerre souhaitée par le président de la République et le ministre des Armées.

Ma question porte sur la prise en compte de critères de cybersécurité applicables aux entreprises de la BITD. Cela concerne évidemment la chaîne de sous-traitants. À votre avis, les marchés publics sont-ils sur ce point à la hauteur des enjeux ? Sommes-nous assez vigilants vis-à-vis des entreprises de la chaîne d'approvisionnement ? Est-ce qu'on accompagne suffisamment ces entreprises ? A-t-on les outils nécessaires pour protéger ces entreprises en cas de crise cyber massive sur le sol français ?

Mme Anne Le Hénanff, rapporteure. En préambule, je souhaite préciser que notre cyberdéfense est une cyberdéfense d'excellence. Nous avons pu le mesurer notamment lors de notre déplacement en Finlande et en Estonie. Il y a une vraie admiration pour le modèle de cyberdéfense français.

Les marchés publics sont un vrai frein aujourd'hui, et pas uniquement dans le domaine de la cyberdéfense. On nous dit souvent que la remise à plat des procédures de marchés publics est un travail colossal. Le code des marchés publics est aujourd'hui un obstacle en matière de cybersécurité et de cyberdéfense. Il devrait être possible d'introduire des critères spécifiques liés à l'achat dans le domaine de la cybersécurité. Le code des marchés publics n'est plus adapté à l'environnement et aux nouvelles menaces. La cyber-résilience ne peut passer que par l'accompagnement des acteurs du territoire. Les collectivités achètent les logiciels, et aujourd'hui, la facilité, c'est d'acheter sur étagère. Le code des marchés publics est donc aujourd'hui un vrai frein à la cybersécurité et à la cyber-résilience.

M. Frédéric Mathieu, rapporteur. Je ne sais pas si les organisations criminelles ou étatiques qui font du cyber-espionnage sur les entreprises de la BITD ont lu la mythologie grecque mais ils connaissent bien le principe du cheval de Troie, et notamment de porter l'effort sur les entreprises les plus petites et les plus faibles, c'est-à-dire sur les entreprises de la chaîne de sous-traitance. C'est une question qui est bien prise en compte par les gros acteurs de la BITD, qui savent très bien que leurs chaînes d'approvisionnement peuvent présenter des faiblesses.

La fixation de critères de cybersécurité nous semble essentielle. On nous dit que cela induit des coûts supplémentaires pour l'entreprise. Certes, mais c'est peut-être la question du modèle économique de ces entreprises qui doivent prendre en compte, comme coût d'entrée sur un marché, le fait d'être à la hauteur en termes de cyberdéfense. Nous avons espoir qu'une évolution sur le code des marchés publics

pourra influencer favorablement les pratiques dans ce domaine et la responsabilisation des acteurs. Le ministère des Armées et l'ANSSI ne peuvent pas arriver systématiquement en secours curatif, au demeurant aux frais du contribuable, pour compenser des moyens qu'une entreprise n'a pas voulu mettre pour garantir sa cybersécurité alors que ses activités sont sensibles. Cela nous a été dit par l'ANSSI, et nous approuvons.

Mme Caroline Colombier (RN). Nous souhaitons saluer le travail de grande qualité présenté ce matin, fort de nombreuses auditions menées ces derniers mois.

La cyberdéfense constitue une nouvelle dimension complexe de la conflictualité moderne, impactant tant le domaine civil que le domaine militaire. Face à cela, une mutation psychologique, capacitaire et opérationnelle doit s'imposer. Le développement du numérique et de l'IA nécessite un renforcement des moyens dévolus à la cyberdéfense. Ainsi, les armées génèrent une masse de données toujours plus conséquente, dont la maîtrise et la protection sont souvent déléguées à des prestataires privés. Or, il est essentiel qu'elle conserve une maîtrise tant de leurs données que de leurs SI dans un intérêt évident de souveraineté. Quelles sont donc vos pistes de réflexion pour aider nos armées à reprendre la main sur leurs SI ?

Par ailleurs, nous souhaitons recueillir votre avis sur la crise actuelle que traverse l'entreprise Atos. Endettée de plus de 5 milliards d'euros, cette entreprise doit en rembourser la moitié avant 2025. Ces derniers jours, son action a totalement plongé. Atos est non seulement un prestataire technologique de premier ordre dans le cadre des JOP 2024, mais elle joue également un rôle essentiel dans notre dissuasion dans la mesure où elle fournit les supercalculateurs nécessaires aux simulations d'essais nucléaires. Or, pour renflouer sa dette, Atos souhaite vendre sa branche « cybersécurité et infogérance ». Cette crise traversée par ce fleuron français vous inquiète-t-elle ? Quelles mesures envisageriez-vous pour la remettre à flots afin qu'il poursuive le rôle qu'il occupe depuis 1997 dans la défense et la souveraineté nationale ?

Mme Anne Le Hénanff, rapporteure. S'agissant des SI des armées, le ministère des Armées travaille beaucoup sur ce sujet dont ils ont conscience. Ceci dit, s'agissant, par exemple, de Linux, on nous a aussi indiqué qu'en l'état, il n'était pas possible de transposer les SI utilisés aujourd'hui sur Windows vers Linux en peu de temps – cela demanderait des années – et par ailleurs, il faudra travailler sur Linux, car il ne pourrait pas être mis en place en l'état. Il faudrait donc conduire des travaux de sécurisation, ce qui induira un coût et prendra du temps. Mais le ministère des Armées a bien conscience de cette dépendance. On nous a aussi indiqué que ces SI sont utilisés dans des domaines non-sensibles, et qu'à partir du moment où des actions sont considérées comme sensibles ou secrètes, il y a, au sein des armées, les compétences et l'expertise qui permettent de sécuriser les SI et éviter l'intrusion par des personnes extérieures dans des domaines que les armées ne souhaitent pas rendre accessibles ; et heureusement ! Il y a plusieurs cercles concentriques : un

premier cercle pour le tout-venant, un cercle plus fermé, et un cercle très fermé. Mais cela ne retire rien à notre constat.

M. Frédéric Mathieu, rapporteur. S'agissant d'Atos, vous avez décrit la situation de l'entreprise. Ce sujet mériterait en réalité une commission d'enquête. Que dire ? Nous avons un fleuron industriel, qui est l'hériter de l'engagement de la France de longue date dans le domaine de l'informatique et des technologies de communication. Nous sommes très préoccupés par la question de la souveraineté, notamment pour les matériels informatiques. L'exemple d'Atos ne fait que confirmer la nécessité que l'État redevienne un État stratège dans ce domaine. Des députés ont déposé des amendements sur le PLF pour nationaliser Atos de manière provisoire et préventive. J'ai moi-même déposé une PPL pour que l'État participe durablement au capital d'Atos. Je ne vais pas faire la publicité de ma PPL ! Mais cette question nous préoccupe tous. Au-delà d'Atos, la question en filigrane est celle de la vision stratégique de l'État : est-ce que la France peut se permettre d'être dépouillée de nos capacités industrielles ? J'espère que nous arriverons à faire comprendre dans le débat public que le numérique n'est plus une simple fonction support : c'est devenu une fonction stratégique, qui peut être une arme en soi. Le sentiment que nous avons aujourd'hui, c'est que cela n'est pas bien pris en compte en termes de vision stratégique.

M. Aurélien Saintoul (LFI-NUPES). Votre travail a un mérite particulier : il est quasiment exhaustif. Je dis « quasiment » car il met un peu de côté la question de la dissuasion, au sujet de laquelle personne ne vous donnera de réponses dans le domaine de la défense. Mais je pense qu'il faut avoir à l'esprit que la question de la cyberdéfense dans le domaine de la dissuasion devra nous faire réfléchir. Je n'en dirai pas davantage, mais nous devons connecter ces deux sujets. Je me permets de répondre à notre collègue Mounir Belhamiti, qui a évoqué le fait que la LPM répond « en partie » aux défis de la cyberdéfense : répondre en partie aux défis, c'est ne pas y répondre.

Néanmoins, je note que votre rapport dresse l'ensemble des perspectives et montre qu'il y a un enjeu de dépendance extrêmement fort. Il n'y a pas d'autre façon d'y répondre qu'en ayant une ambition à la hauteur des enjeux. J'entends dans votre travail des choses qui consonnent énormément avec le programme de La France insoumise, et singulièrement avec la valorisation que nous accordons à la notion de planification, ce dont je me réjouis.

Vous avez évoqué le quantique. Vous suggérez un audit de nos politiques. Avez-vous quand même un aperçu de la stratégie mise en œuvre jusqu'à présent ? Avez-vous perçu une cohérence dans l'appréciation que l'État a de ce sujet ? Ou avez-vous eu le sentiment d'une approche plutôt impressionniste ?

Ensuite, s'agissant des ressources humaines, qui sont un des grands défis, est-ce qu'une école comme Polytechnique fournit les contingents nécessaires ? Ou pourrait-on faire mieux ? D'autres écoles pourraient être mobilisées, mais s'agissant de Polytechnique, nous avons peut-être un sujet la concernant.

J'avais également une question sur Atos, à laquelle vous avez globalement répondu, qui portait sur l'idée que c'est en réalité l'ensemble de l'écosystème qui devrait être consolidé. C'est notre conviction. Nous manquons de profondeur de vue si nous ne savons pas que Atos a sauvé Bull, et que Bull était pourtant public et qu'il a été privatisé. C'est peut-être l'ensemble de ces mouvements de capitaux et de ces stratégies erratiques au fil des années que nous devrions interroger.

Enfin, la dernière question porte sur la L2I. Avez-vous pu avoir des éléments tangibles sur les restrictions éthiques que nous appliquons ? C'est une question que je pose souvent. Avez-vous pu rentrer dans la machine ?

M. Frédéric Mathieu, rapporteur. S'agissant de la L2I, c'est compliqué de rentrer dans la machine, comme vous dites ! Il s'agit d'un domaine très sensible. On sait que les armées mènent des actions dans le champ informationnel. Mais il s'agit d'informations classifiées. Cela est en rapport avec notre proposition de créer une commission *ad hoc*, qui permettrait à une délégation de notre assemblée d'avoir une vision claire sur ce sujet, selon les mêmes modalités et le même type de fonctionnement que la DPR.

S'agissant du quantique, on nous dit qu'il faut lancer des études sérieuses sur la question. Je vais vous confier une anecdote sans vous dévoiler les acteurs concernés. En l'espace d'une matinée, au sujet de la dotation par l'État d'un ordinateur quantique, on a rencontré deux hauts décideurs qui auraient dû avoir les idées claires sur cette question. Lors de la première audition, on nous a dit que les investissements nécessaires pour se doter d'un ordinateur quantique seraient très élevés. Lorsqu'on a demandé combien, on nous a indiqué que cela coûterait au moins 100 millions d'euros. Pourtant, 100 millions d'euros, ce n'est pas si cher… et au même moment, nous apprenions que le surcoût du projet immobilier de la DGSE au Fort Neuf de Vincennes était de 185 millions d'euros… lors de la seconde audition, nous avons reposé la question. La personne que nous auditionnions nous a dit que le coût afférent était tellement élevé qu'on ne peut pas le chiffrer. Donc, dans la même matinée, nous avons eu une fourchette allant de 100 millions d'euros à l'infini en dilatation constante… on est dans le quantique cela dit, donc on passe de l'infiniment petit à l'infiniment grand !

Plus sérieusement, cela est triste car nous sommes persuadés qu'il y a des gens au sein des services qui savent très bien ce qu'il en est car nous avons la capacité en interne de faire ce type d'évaluations. Mais ce que cette anecdote montre, c'est qu'il y a deux options : soit l'information ne remonte pas au bon niveau, soit on ne se pose pas la question en haut lieu. Cela m'inquiète quant aux conseils politiques prodigués aux grands décideurs politiques. On préconise donc la conduite d'une étude pour connaître le coût, les délais et les partenaires européens éventuels avec lesquels cela pourrait être fait.

J'ai le sentiment que, s'agissant du quantique, on est à une époque similaire à celle du milieu des années 1930 avec l'atome : on sait que ça existe, on sait qu'il y a des potentialités, on sait qu'on pourrait en faire une arme… mais tout cela, on

ne le saura que si on décide de se lancer dans le Projet Manhattan. Aujourd'hui, la France et l'Europe en sont à ce point-là. Il faut donc travailler ce sujet. Si le quantique s'affirme comme une réalité dans les années qui viennent, on est face à quelque chose en potentiel offensif qui est de l'ordre de la dissuasion nucléaire. La question est donc de savoir si on veut passer à côté ou non.

Mme Anne Le Hénanff, rapporteure. Sur les ressources humaines, nous ne sommes jamais mieux servis que par soi-même. Le partenariat entre l'École Polytechnique et l'EPITA a l'avantage de répondre aux besoins. La première promotion ne sera que de 30 étudiants, mais c'est un bon début. La conclusion de partenariats entre le ministère des Armées et des écoles d'ingénieurs ou la création de BTS et d'IUT a l'avantage d'aboutir à des formations adaptées aux besoins du ministère des Armées. Nous croyons également à une approche sectorielle dans ce domaine, en adaptant la formation aux besoins des armées. C'est ce vers quoi le ministère des Armées tend. Mais cela ne suffira pas : il faudra aller plus loin. Le COMCYBER est pleinement engagé dans cette voie.

S'agissant de la L2I, les armées agissent dans un cadre déontologique national et international : ils ne font pas n'importe quoi ! Il y a un cadre, et la démarche est essentiellement défensive dans le domaine informationnel. Lorsque des vagues de désinformation en provenance, par exemple, du Sahel, il s'agit de rectifier ces fausses informations, en prouvant leur caractère fallacieux. On ne fait pas de la désinformation gratuite ou des actions pour décrédibiliser des États.

M. Jean-Louis Thiériot (LR). Je tiens à vous dire à quel point votre exposé était absolument passionnant, clair et surtout très pédagogique. Pour quelqu'un qui ne vient pas forcément de ce secteur, c'était d'une clarté exceptionnelle. Je tenais à vous en remercier.

Vous nous avez présenté l'architecture et la doctrine française. Avez-vous procédé à des comparaisons internationales ? Quelle est la doctrine de l'OTAN en termes de cyberdéfense ? Enfin, des leçons de la guerre en Ukraine peuvent-elles être tirées en matière de cyberdéfense ? La question du quantique est majeure. J'ai beaucoup aimé votre référence à la rupture épistémologique potentielle entre l'atome et le quantique. Que font nos compétiteurs stratégiques ?

Ensuite, s'agissant du SaaS, c'est un sujet de préoccupation qui m'inquiète beaucoup depuis très longtemps. Quelles solutions pourrait-on avoir à moyen terme et à quels coûts ? Et comment ferait-on pour la dissuasion ? J'ai la faiblesse de croire, s'agissant de la dissuasion, qu'on a réussi à élaborer une architecture numérique totalement souveraine.

Enfin, le COMCYBER n'est-il qu'un commandement opérationnel ? Si oui, existe-t-il par ailleurs un commandement organique ?

Mme Anne Le Hénanff, rapporteure. S'agissant du SaaS, les armées ne pourront pas répondre seules à ce défi. C'est logique, car cette problématique concerne tous les ministères sans exception. Ce ne sont pas aux armées de trouver

des solutions. Les échanges que nous avons eus nous prouvent qu'ils ont conscience de cela. À l'échelle interministérielle, c'est la DINUM qui est responsable. La solution ne pourra venir que du plus haut niveau, y compris à l'échelon politique, et en l'occurrence, celui du Premier ministre. C'est à lui de s'emparer de ce sujet. Cela étant dit, exclure tous les logiciels extraterritoriaux, ce n'est pas sérieux. Il faut trouver un juste équilibre, ce qui prendra du temps mais nous devons nous y atteler au plus haut niveau de l'État, qui est celui du Premier ministre. Nous devons nous emparer de ce sujet.

S'agissant des comparaisons internationales, la sensibilité à la cyberdéfense et à la cybersécurité est très loin de ce qu'on a pu constater en Finlande et en Estonie. Pour nous, ce sont des modèles. Pourquoi ? L'Estonie est vraiment la référence en matière de numérique, car ils ont franchi une étape sur l'identité numérique du citoyen que nous n'avons pas encore franchi. Nous avons été impressionnés dans ces deux pays par le fait que dès l'école primaire, les élèves entendent parler d'hygiène numérique ou de désinformation. Les enfants sont parties prenantes de la cyber-résilience dans ces pays. En France, ce que nous constatons, c'est que la cybersécurité est un sujet d'experts, très fermé. Avec ce rapport, nous souhaitons que ce sujet s'ouvre à la nation tout entière. La révision de la Revue stratégique de cyberdéfense en cours peut être l'occasion d'aller plus loin.

S'agissant de l'Ukraine, la Finlande et l'Estonie sont en cyber guerre. Ils subissent régulièrement des cyberattaques depuis le déclenchement de la guerre en Ukraine. Nous avons des leçons à tirer de cela. Mais ils sont aussi demandeurs vis-à-vis de la France, notamment en matière d'exercices. On a donc beaucoup à apprendre d'eux, mais ils sont aussi en attente vis-à-vis de nous.

M. Frédéric Mathieu, rapporteur. Le COMCYBER assure à la fois un commandement organique et un commandement opérationnel. Toutefois, avec la création de la communauté cyber des armées, l'objectif est bien de donner des marges de manœuvre aux armées sur les échelons tactique et opératif, sous le contrôle du COMCYBER.

Sur la guerre en Ukraine, beaucoup d'aspects sont confidentiels. Mais notre recommandation sur la nécessité de réfléchir au cadre juridique du mercenariat cyber est liée aux enseignements que nous avons pu tirer de la guerre en Ukraine. La nécessité de conduire des exercices en situation réelle est également un autre enseignement de la guerre en Ukraine.

S'agissant du quantique à l'étranger, les États-Unis et la Chine sont les deux acteurs les plus en avance. Mais peu d'informations circulent. Quand on a évoqué le sujet du quantique avec des autorités nationales, on nous a indiqué qu'on ne pourra rien faire sans le secteur privé, notamment pour des raisons de coûts. De notre point de vue, il faudra s'émanciper de réflexes dogmatiques car lorsqu'on nous a parlé d'une nécessaire participation du secteur privé qui devra avoir l'assurance qu'il pourra exporter la technologie quantique, dont on ne connaît pas encore les implications, on a toussé ! Or, comme je le disais en audition, je n'ai pas le

souvenir que le général de Gaulle ait fait un appel à projets sur les marchés financiers pour la dissuasion nucléaire… ce qui donnait lieu à un silence poli, mais gêné ! Il faut donc avancer et aller à un niveau de maturité supérieure s'agissant du quantique. On ne peut pas rester dans le niveau d'obscurité actuel.

M. Christophe Blanchet (Dem). Je vous remercie sincèrement pour votre exposé vivant, passionnant, éduquant mais très inquiétant !

S'agissant de l'organisation de la cyberdéfense en millefeuilles, j'ai l'impression qu'on s'y perd rapidement… et il ne s'agit que d'une version simplifiée ! Est-ce que la gouvernance de la cyberdéfense ne serait pas plus performante si, comme pour les millefeuilles administratifs, on opérait quelques coupes ?

Par ailleurs, vous avez parlé des cyberattaques mais vous avez élargi à l'ensemble de la population. Avez-vous quantifié le nombre de cyberattaques que la France a subies ? Cela me semble important de quantifier la menace pour embarquer la population dans cette démarche de cyber-résilience.

Pendant votre intervention, j'ai pu voir le nombre de personnes à proximité sur WhatsApp. Il y avait 10 profils chinois connectés à moins de 500 mètres d'ici. Quel regard portez-vous sur les applications telles que Telegram et WhatsApp ? Est-ce que Tchap est une solution viable ?

Enfin, comment ne pas parler des réserves ? Vous avez évoqué les réservistes opérationnels dans votre propos. Je suis d'accord pour dire qu'il faudrait davantage de réservistes opérationnels. Mais s'agissant des réservistes citoyens, c'est une manne utile et nécessaire. Comment la politique de défense nationale s'opère-t-elle à ce sujet ? Est-ce qu'il y a une ambition ? Lors des débats sur la LPM, nous avions vu qu'il n'y avait pas de compréhension sur l'utilité de la réserve citoyenne. Pourtant, il s'agit de personnes passionnées qui pourraient transmettre ces messages sur la cybersécurité, notamment dans les écoles.

Mme Anne Le Hénanff, rapporteure. La réserve citoyenne est un sujet stratégique pour la cyberdéfense. C'est un sujet utile et indispensable car il contribue au renforcement du lien armées-Nation ! On a un objectif sur la réserve opérationnelle. Ces réservistes opérationnels jouent un rôle stratégique pour la cyberdéfense française. Mais s'agissant de la réserve citoyenne dans le domaine de la cyberdéfense, sujet dont j'ai souvent parlé avec le COMCYBER, elle a existé. Il y a une volonté de la remettre en œuvre. C'est vrai que la priorité était la réserve opérationnelle. La réserve citoyenne est plutôt active avec la Gendarmerie. Il y a aussi des réservistes dans la Police nationale. Il y en a moins dans les armées. Je formule le vœu qu'on réarme – si je puis dire ! – les armées en réservistes citoyens car ceux-ci ont des vraies compétences. La volonté de redéployer la réserve citoyenne fait partie des ambitions des armées, et nous serons là pour les accompagner dans l'atteinte de cet objectif.

S’agissant du millefeuille, il ne faut couper aucune compétence. Mais on a un point majeur : au niveau de la gouvernance, il faudra réorganiser la cyberdéfense en France. L’organisation est encore trop silotée. Il y a des chasses gardées, ce qui est inacceptable. Par ailleurs, cette organisation est trop pyramidale : du haut vers le bas. Nous pensons au contraire que l’organisation de la cyberdéfense doit être transversale.

M. Frédéric Mathieu, rapporteur. Nous vous avions présenté la version simplifiée de l’organisation de la cyberdéfense, mais l’organisation est en réalité beaucoup plus complexe, comme le soulignait notre collègue Mounir Belhamiti.

M. Mounir Belhamiti (RE). Et il n’y a même pas de ministre !

Mme Anne Le Hénanff, rapporteure. C’est vrai !

M. Frédéric Mathieu, rapporteur. Tout à fait. La question de la création d’un ministère chargé de la cybersécurité est d’ailleurs régulièrement évoquée dans les cercles qui réfléchissent à la réorganisation de cette politique. En tout cas, force est de constater que chaque service s’est doté de ses capacités propres. La création de la communauté cyber des armées va dans le bon sens. Mais nous sommes attachés au *continuum* de cybersécurité et de cyber-résilience de la Nation. On ne va pas pouvoir rester très longtemps dans le modèle actuel, et tant pis si cela heurte certains conservatismes dans certaines administrations publiques : il va falloir avoir une approche globale. Si cette ambition arrive à maturité, il y aura des changements dans l’organigramme. Mais comme le disait ma collègue, on ne peut pas couper des compétences.

S’agissant des messageries cryptées, nous savons qu’il y a un sujet. On ne sait pas ce qu’il en est spécifiquement pour chaque application, mais au sein des armées, des consignes sont passées pour sensibiliser au risque encouru par le recours à des messageries au quotidien, même lorsqu’elles prétendent être parfaitement cryptées.

Enfin, s’agissant du nombre de cyberattaques, il y a des statistiques dans les rapports d’activité de l’ANSSI. Toutefois, il ne s’agit que des cyberattaques connues : il y a des cyberattaques qui ont pu toucher la France au sujet desquelles aucune publicité n’est faite pour des raisons évidentes de confidentialité.

Mme Mélanie Thomin (SOC). Au nom du groupe Socialistes et apparentés, je vous remercie pour ce rapport qui est force de propositions et qui fait honneur à l’audace du travail parlementaire. Bravo à tous les deux !

Nous partageons le fait que l’anticipation et la lutte contre les menaces cyber sont primordiales dans notre approche des conflits modernes et doivent être un élément structurant de notre politique de défense nationale. Les attaques cyber sont discrètes et ont une portée sans limite, comme vous l’avez très bien dit. Nos services publics et l’économie du pays sont devenus des cibles de choix.

S'agissant du travail parlementaire qui pourrait émerger en réaction à votre rapport, ma première question portera sur les logiciels. Pour reprendre votre raisonnement concernant les logiciels en tant que service, comment peut-on encadrer juridiquement cette pratique pour contrer leur expansion ? Pourrait-on, par exemple, contraindre par la loi chaque éditeur de logiciel proposant un logiciel en tant que service par abonnement à obligatoirement proposer une version sous licence propriétaire ?

Par ailleurs, s'agissant de l'IA générative, un aspect intéressant soulevé dans la LIO et la L2I est que les cyberattaques peuvent avoir pour cibles des bases de données. Comment garantir la protection de ces bases de données ? Faudrait-il imposer aux éditeurs un stockage physique en France ou *a minima* en Europe ?

M. Frédéric Mathieu, rapporteur. S'agissant de l'IA générative, il faut avoir en tête que la localisation géographique n'est pas un critère pertinent. Les règles d'extraterritorialité de certains États, notamment des États-Unis, sont telles que le fait d'avoir un serveur de Microsoft sur le sol français ne prémunit en rien de toute ingérence du département d'État américain sur nos données. La question n'est donc pas celle de la localisation géographique. Il s'agit d'un sujet de conflits de lois, entre la loi nationale et la loi extraterritoriale.

S'agissant du travail parlementaire, le rapport vous appartient désormais ! Ce n'est plus uniquement notre œuvre. On peut imaginer beaucoup de choses. L'acquisition de logiciels sous licence propriétaire peut s'étudier mais elle ne réglera pas la question des portes dérobées dès lors que ce logiciel n'est pas souverain. L'enjeu est de se prémunir de la mise en place de portes dérobées. On peut tout à fait acheter un système propriétaire et en être victime. On a ressenti un malaise lorsqu'on évoquait le sujet de Windows. En insistant, on finissait par nous répondre que les Américains sont nos alliés. Pourtant, ce sont ceux qui nous ont le plus espionnés ces dernières années… en tout cas de manière connue. *A contrario*, on nous a dit que l'État est propriétaire de ces logiciels et que, par conséquent, il a la main dessus. Je répondais systématiquement à cet argument que le recours à des matériels ou à des logiciels chinois comme Huawei ne posait donc aucun problème ; et là, on nous disait que si, cela posait problème, et les raisons invoquées s'appliquaient en réalité totalement à Microsoft. Donc, en effet, la question est d'avoir des solutions souveraines sur lesquelles on a pleinement la main.

Mme Anne Le Hénanff, rapporteure. Avec mon collègue, nous n'avons jamais travaillé dans l'optique d'un travail législatif. Nous avons vécu cette mission. Désormais, nous partageons nos conclusions. Nous avons nos recommandations mais nous n'avions pas d'objectif législatif.

S'agissant de la protection de notre souveraineté, je crois beaucoup au travail de l'Europe. On a voté le projet de loi « sécuriser et réguler l'espace numérique » à l'Assemblée nationale. L'IUCS permettra de fixer le niveau de cybersécurité imposé en Europe. L'ANSSI est très impliquée à ce sujet. On souhaite que la France donne le ton quant au niveau de cybersécurité exigé en Europe.

J'espère qu'on atteindra cet objectif. L'examen à venir de la directive NIS 2 permettra aussi de renforcer notre cybersécurité.

Enfin, comme mon collègue l'a dit, la localisation géographique des serveurs n'entre pas en ligne de compte. Ce qui compte, c'est la cybersécurité et l'extraterritorialité. Pour vous rassurer, le ministère des Armées détient en propre son centre de données.

M. Loïc Kervran (HOR). Je remercie nos deux co-rapporteurs et saluer quelques points qui me semblent importants. L'importance de votre travail est perceptible dans la qualité du rendu. L'expérience de Mme Le Hénanff, en tant qu'élue locale, se reflète aussi dans vos travaux et préconisations. Je salue aussi votre bonne entente et votre capacité à dépasser les différences politiques, ce qui est toujours le cas, du reste, dans cette commission. Votre approche globale qui dépasse les seules armées mais qui s'inscrit bien dans l'approche de défense nationale augure de l'orientation des travaux de la commission cette année sur les aspects de défense et de résilience nationale. C'est une excellente manière de rentrer dans cette phase.

S'agissant de la gouvernance, je salue vos objectifs pour améliorer la lisibilité et l'approche globale de la cybersécurité et de la cyberdéfense. Sur le partage des savoir-faire des armées, jugez-vous que les armées ont des marges de manœuvre, notamment en termes d'effectifs et de temps, pour partager ces savoir-faire vers le civil ?

Vous évoquez les effectifs du CERT de l'ANSSI. Avez-vous une idée du nombre d'ETP supplémentaires nécessaires ?

Enfin, vous évoquez votre souhait de créer une commission parlementaire sur la cyberdéfense. Est-ce que vous jugez que la DPR ne s'intéresse pas assez à ces questions de cyberdéfense ? Vous avez évoqué l'importance du rôle des services de renseignement dans ces questions. Comme vous le savez, les Parlementaires de la DPR sont habilités ès qualités et ont produit des travaux sur la cyberdéfense. Où est la marge de progrès ? Est-ce que la création d'une commission supplémentaire se justifie pour compléter les travaux de la DPR ?

Mme Anne Le Hénanff, rapporteure. S'agissant de la gouvernance et du partage des savoir-faire des armées, il faut avoir à l'esprit que les militaires sont vraiment des acteurs d'excellence en France sur le sujet de la prévention, de la sensibilisation, jusqu'à la gestion de crise et la remédiation. L'idée n'est pas de faire intervenir les militaires dans le civil, à la demande, lors d'actions ou de crise cyber. Mais nous trouvons dommage qu'il n'y ait pas davantage de partage de pratiques, de feuille de route, de mode d'emploi de leurs capacités et de leur savoir-faire. Il faut un intermédiaire entre les militaires et le secteur civil pour diffuser et mettre en œuvre ces bonnes pratiques. Prenons l'exemple d'un exercice cyber. Comment une commune de plusieurs dizaines de milliers d'habitants doit réagir pour éviter la

diffusion d'une cyberattaque ? La conduite d'exercices peut y aider, et dans ce domaine, les militaires sont les plus compétents.

M. Frédéric Mathieu, rapporteur. S'agissant de la spécificité d'une commission, tout le renseignement n'est pas contenu dans le cyber et tout le cyber n'est pas contenu dans le renseignement. La DPR est une commission ad hoc sur la politique de renseignement, mais même si les domaines peuvent se superposer, ils ne se confondent pas totalement. Après, si, dans plusieurs années, après avoir mis en place cette commission, on estime qu'il faudra mettre en place une commission plus large, en plus de la DPR et de la CNCTR, on pourra avoir ce débat. À notre sens, le sujet est celui de la visibilité et de la transparence. En termes de fonctions de contrôle parlementaire, il faut pouvoir être tenu informé des opérations conduites dans le cyberespace et dans le champ informationnel.

S'agissant du CERT de l'ANSSI, nous ne sommes pas en mesure de donner une estimation précise du nombre d'ETP nécessaires pour, par exemple, armer l'ANSSI pour garantir la cybersécurité des DROM-COM. Mais cela pourrait être le cas dans le cadre de futurs travaux parlementaires.

M. José Gonzalez (RN). Je vous remercie pour votre travail. Le CEMAT indiquait récemment que l'IA ne changera pas la nature de la guerre. Or, l'usage de l'IA dans le domaine de la cyberdéfense s'intensifie. Le conflit actuel en Ukraine l'a bien mis en lumière. Les Ukrainiens utilisent les moyens cyber pour rattraper leur retard sur les Russes. Le général Grégoire de Saint-Quentin, ancien commandant des forces spéciales, semble adopter la même ligne que le CEMAT. Au regard des auditions que vous avez menées, partagez-vous cet avis ? Ou pensez-vous au contraire que l'IA bouleversera la nature des conflits modernes ? Est-ce simplement un outil complémentaire aux outils existants ? Enfin, quelle stratégie la France doit-elle adopter pour s'adapter aux nouveaux défis de l'IA et l'intégrer pleinement à notre stratégie de défense ?

Mme Murielle Lepvraud (LFI). Pensez-vous que la montée en compétences progressive de l'ANSSI pourrait amener à combler le recours au secteur privé ? Si oui, à quelle échéance ? Les protocoles de contrôle assurent-ils la protection des données auxquelles ces entreprises privées ont accès dans le cadre de leurs missions ?

Mme Anne Le Hénanff, rapporteure. L'IA ne va pas modifier la forme des conflits. Mais la maîtrise et l'indépendance de l'IA nous conféreraient une supériorité opérationnelle. L'IA n'est qu'un moyen pour mieux anticiper et mieux connaître nos adversaires, et s'agissant de la L2I, de mettre en œuvre des actions qui nous positionneraient dans une situation de maîtrise et d'avance par rapport à nos adversaires.

M. Frédéric Mathieu, rapporteur. S'agissant des entreprises privées, l'ANSSI intervient en propre lorsque les crises cyber sont suffisamment critiques. La plupart des temps, en effet, elle a recours à des prestataires privés agréés. La

question de la confidentialité des données auxquelles peuvent avoir accès ces entreprises privées se pose en effet. Mais nous estimons que le droit pénal suffit à encadrer ce risque. La question qui peut se poser en revanche est celle de la nature très diverse des interventions qui peuvent avoir lieu. On est bien obligés d'agréer des entreprises privées selon un cahier des charges, mais cela ne nous dit rien de la rigueur du cahier des charges, tout comme cela ne nous dit rien des contrôles mis en œuvre au long cours pour s'assurer du respect du cahier des charges. Je ne remets pas en cause la rigueur de l'ANSSI pour effectuer ces contrôles, mais il y a un défi capacitaire : il faut bien avoir des entreprises qui puissent intervenir sur place en cas de besoin. On se doute bien qu'il faut s'adapter aux réalités du terrain : on ne peut pas placer un niveau d'exigence trop élevé, sinon, on n'agrée personne. C'est davantage sur cette mécanique que les préoccupations doivent porter.

M. le président Jean-Pierre Cubertafon. Bravo à nouveau à nos deux collègues pour la très grande qualité de leur travail. Nous allons donc désormais procéder au vote pour autoriser la publication du rapport.

*La commission **autorise** le dépôt du rapport d'information sur les défis de la cyberdéfense.*

ANNEXE N° 1 :
LISTE DES PERSONNES AUDITIONNÉES PAR LES RAPPORTEURS

➢ **M. Vincent TEJEDOR,** directeur général du numérique et des systèmes d'information et de communication du ministère des Armées ;

➢ **M. Thibaut de VANSSAY**, directeur des ressources humaines du ministère des Armées ;

➢ **M. le général de corps d'armée Didier TISSEYRE**, directeur central de la direction interarmées des réseaux d'infrastructure et des systèmes d'information de l'état-major des armées ;

➢ **M. l'ingénieur général de l'armement Bruno MARESCAUX**, chargé de mission « cyber » auprès du délégué général pour l'armement ;

➢ **M. Vincent STRUBEL**, directeur général de l'Agence nationale de la sécurité des systèmes d'information ;

➢ **Représentants de la Marine nationale** ;

➢ **M. le général de division Aymeric BONNEMAISON**, commandant de la cyberdéfense de l'état-major des armées, et **M. le capitaine de vaisseau Grégory DOUILLOT**, officier de cohérence opérationnelle en charge du domaine cyber au sein de la division « cohérence capacitaire » de l'état-major des armées ;

➢ **M. le vice-amiral Denis BERTRAND**, directeur de la protection des installations, moyens et activités de la Défense, et **Mme l'ingénieure en cheffe de l'armement Sophie GRIFFE**, fonctionnaire de sécurité des systèmes d'information du ministère des Armées ;

➢ **M. Édouard GEFFRAY**, directeur général de l'enseignement scolaire au ministère de l'Éducation nationale ;

➢ **M. Pierre-Yves JOLIVET**, vice-président « solutions de cyberdéfense » chez Thales ;

➢ **M. Philippe DULUC**, directeur de la technologie au sein de la division « Big Data & Security » d'Atos, et **M. Frédéric POLYCARPE**, vice-président et directeur des affaires publiques d'Atos ;

➢ **Représentants de la DGSE** ;

➢ **M. le général de corps d'armée Philippe SUSNJARA**, directeur du renseignement et de la sécurité de la défense ;

➢ **Mme Laura CHAUBARD**, directrice générale et présidente par intérim de l'École Polytechnique, et **M. Thomas DELOEIL,** directeur de cabinet de la présidente ;

➢ **M. le général de brigade Hervé GUILLERAULT**, officier général « numérique » au sein de l'état-major de l'armée de l'Air et de l'Espace ;

➢ **M. le général Jean-René COUANAU**, officier général « numérisation » au sein de l'état-major de l'armée de Terre ;

➢ **M. le général de brigade aérienne Bertrand JARDIN**, attaché de défense à l'ambassade de France à Washington ;

➢ **M. Patrick AUFORT**, directeur de l'Agence de l'innovation de défense ;

➢ **M. Stéphane BOUILLON**, secrétaire général de la défense et de la sécurité nationale ;

➢ **M. Yann PHILIPPIN**, journaliste à Mediapart, **M. Laurent RICHARD**, journaliste, fondateur et directeur du collectif Forbidden Stories, **et Mme Katia ROUX**, chargée de plaidoyer au sein d'Amnesty International ;

➢ **Représentants du ministère chargé de l'Enseignement supérieur et de la Recherche** ;

➢ **Mme Léa BENASSEM**, chargée de la cyber-résilience au sein du GICAT, et **M. Pierre BOUQUET**, Président du Comité Richelieu.

ANNEXE 2 : DÉPLACEMENTS

1. Sur le territoire national

➢ **27 juillet 2023, Bruz et Saint-Jacques-de-la-Lande** : visite des locaux de la DGA-MI et du groupement de la cyberdéfense des armées

➢ **27 novembre 2023, Cesson-Sévigné et Saint-Jacques-de-la-Lande** : visite du commandement des systèmes d'information et de la communication et de la 807e compagnie de transmissions de l'armée de Terre

➢ **29 novembre 2023, Issy-les-Moulineaux** : entretien avec des représentants du commandement de la Gendarmerie nationale dans le cyberespace

➢ **14 décembre 2023, Brest** : visite du Centre Support Cyberdéfense de la Marine nationale, de l'École navale et de France Cyber Maritime

2. À l'étranger

➢ **Du 17 au 20 décembre 2023** : déplacement en Finlande et en Estonie

ANNEXE 3 : GLOSSAIRE DES PRINCIPAUX ACRONYMES

ADS : armées, directions et services

AID : agence de l'innovation de défense

AMSN : autorité ministérielle de sécurité numérique

ANSSI : Agence nationale de la sécurité des systèmes d'information

BARC : bureau d'appui au recrutement cyber

BITD : base industrielle et technologique de défense

C2PO : centre cyber de préparation opérationnelle

C4 : centre de coordination des crises cyber

CALID : centre d'analyse en lutte informatique défensive

CASSI : centre d'audits de la sécurité des systèmes d'information

CECNum : comité exécutif du conseil du numérique et des SIC

CEMA : chef d'état-major des armées

CERT : *Computer Emergency Response Team*

CGFP : code général de la fonction publique

CHPI : centre des homologations principales interarmées

CIE : contre-ingérence économique

CIF : contre-ingérence des forces

CIRFA : centre d'information et de recrutement des forces armées

CNCTR : commission nationale de contrôle des techniques de renseignement

CNRLT : coordination nationale du renseignement et de la lutte contre le terrorisme

COMCYBER : commandement de la cyberdéfense

COMCyberGEND : commandement de la Gendarmerie dans le cyberespace

COMEX : comité exécutif

CSI : code de la sécurité intérieure

CSR : comité de suivi de la ressource cyber

DGA : direction générale de l'armement

DGA-MI : direction générale de l'armement - maitrise de l'information

DGNUM : direction générale du numérique et de des systèmes d'information et de la communication

DGSE : direction générale de la sécurité extérieure

DGSI : direction générale de la sécurité intérieure

DICOD : délégation à l'information et à la communication de la défense

DINUM : direction interministérielle du numérique et de des systèmes d'information et de la communication

DIRISI : direction interarmées des réseaux d'infrastructures et des systèmes d'information

DPID : direction de la protection des installations, moyens et activités de la Défense

DRH-MD : direction des ressources humaines du ministère des Armées

DROM-COM : départements et régions d'outre-mer

DRM : direction du renseignement militaire

DRSD : direction du renseignement et de la sécurité de la Défense

EMDS : états-majors, directions et services

ETP : équivalent temps plein

FSSI : fonctionnaire de la sécurité des systèmes d'information

GCA : groupement de la cyberdéfense des armées

GIP : groupement d'intérêt public

GPEEC : gestion prévisionnelle des emplois, des effectifs et des compétences

HFCDS : haut fonctionnaire correspondant défense sécurité

IA : intelligence artificielle

L2I : lutte informatique d'influence

LID : lutte informatique défensive

LIO : lutte informatique offensive

LPM : loi de programmation militaire

NPRM : nouvelle politique de rémunération des militaires

OIV : opérateur d'importance vitale

OPEX : opération extérieure

OSE : opérateur de services essentiels

PC : poste de commandement

PEM : programme à effets majeurs

PIV : points d'importance vitale

PNOR : plan national d'orientation du renseignement

PPC : posture permanente de cyberdéfense

PSTN : potentiel scientifique et technique de la Nation

S2IE : service des affaires industrielles et de l'intelligence économique

SGA : secrétariat général pour l'administration

SGDSN : secrétariat général de la Défense et de la sécurité nationale

SIC : système d'information et de communication

SOC : *Security Operation Center*

StratCom : communication stratégique

TESSCo : terrorisme, espionnage, sabotage, subversion, criminalité organisée

TRR : technique de recueil du renseignement